COMPLIANCE REPORT · MINDSHINE CORTEX

SOC 2 Audit Findings Report Cortex

Description of the Cortex system, the controls in operation to meet the SOC 2 Trust Services Criteria, the testing performed on those controls, and the matters open at the report date.

REPORT DATE	REVIEW PERIOD	SYSTEM IN SCOPE	CRITERIA
12 August 2026	12 July – 12 August 2026	Cortex data-governance platform — application & runtime infrastructure	AICPA Trust Services Criteria — Security, Availability, Confidentiality, Processing Integrity, Privacy

REPORT TYPE	PREPARED FOR
Management-prepared readiness assessment	Internal governance & prospective independent examination

I Report of the internal assessment function

We have assessed the controls of the **Cortex data-governance platform** operated by Mindshine — the application software, its runtime infrastructure, and the supporting operational procedures described in Section III — against the applicable Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy.

Management's responsibility. Management is responsible for designing, implementing, operating, and maintaining effective controls to meet the service commitments and system requirements described in Section III, and for the completeness and accuracy of the system description and the assertion in Section II.

Assessment responsibility. The assessment function is responsible for expressing a conclusion on whether the controls were suitably designed and operating as of the report date. Testing combined continuous automated scanning of the code base and infrastructure, structured control reviews closed with written evidence, live verification of enforcement mechanisms under the constrained identities they govern, and an independent adversarial review by a reviewer with no prior context who was instructed to refute each control claim.

Inherent limitations. Controls, however well designed and operated, provide reasonable but not absolute assurance. Projections of any evaluation to future periods are subject to the risk that controls may become inadequate because of changes in conditions.

Conclusion. In our assessment, as of 12 August 2026, the controls described in Section IV were suitably designed and operating to meet the applicable Trust Services Criteria, **except for the open matters described in Section V**, each of which is disclosed with management's remediation plan and target rather than omitted.

II Management's assertion

Mindshine management asserts that the description in Section III fairly presents the Cortex system as designed and implemented as of 12 August 2026; that the controls stated in Section IV were implemented as of that date; and that, except for the matters disclosed in Section V, those controls were operating with sufficient effectiveness to provide reasonable assurance that the service commitments and system requirements were met, based on the applicable Trust Services Criteria.

Management further asserts that the evidence supporting this report — control test results, configuration state, and review records — is maintained on a tamper-evident system of record and is available in full to an independent examiner.

Asserted by
Mindshine platform operations
12 August 2026

Evidence base
Cortex continuous-audit engine
& versioned evidence pack (`docs/soc2/`)

III Description of the system

Services provided

Cortex is a data-governance platform. Customer organizations use it to define governed data pipelines (sources, typed data elements, mappings, processing rules, targets), run business workflows with human and AI participants, operate project-scoped AI agents, publish governed applications, and train models on governed data. Every element of a customer's configuration is versioned data; the platform executes it on a managed Kubernetes runtime.

Principal service commitments and system requirements

- **Security & tenant isolation.** Customer configuration and data are accessible only to authorized members of the owning organization, enforced by a single central authorization policy.
- **Traceability.** Every configuration change, pipeline run, and administrative action is attributable and preserved on a versioned or append-only record.
- **Processing integrity.** Pipelines process data according to their declared, machine-readable contract; run results are reconcilable per stage.
- **Availability.** The platform and deployed customer applications remain available consistent with the capacity and recovery objectives stated in the evidence pack.
- **Confidentiality & privacy.** Customer data is used only for the project's stated purpose; personal data is inventoried, access-controlled, and disposable on request.

Components

COMPONENT	DESCRIPTION
Infrastructure	Amazon EKS (us-east-1); per-environment namespaces plus an isolated namespace per deployed customer application; EBS-backed persistent volumes; S3 object storage; ECR image registry. Images are built exclusively by CI.
Software	Cortex application services (API backend, assistant/agent surfaces, web frontend); a versioned configuration store (Dolt) holding each project's governance recipe with full history; operational PostgreSQL stores (identity, organizations, jobs, application registry); the Flow execution engine running pipeline, workflow, and application endpoints; a separate audit portal with an append-only, hash-chained activity log.
People	Platform operations (infrastructure & release), engineering (application code via reviewed CI), and customer-organization members acting under per-organization roles. No direct human access to production data stores; administrative cluster access flows through a single audited jumpbox.
Procedures	Documented change management (versioned infrastructure overlays, CI verify gate), access provisioning and revocation, security-incident reporting (published security policy with severity-based SLAs), risk and vendor review on a quarterly cadence, and a data-subject access/correction runbook with a 30-day SLA.

COMPONENT	DESCRIPTION
Data	Staff identity data (name, email, credential hashes); organization membership and roles; customer project configuration (schemas, mappings, rules — column names, not values); customer datasets ingested by projects (may contain personal data, held in per-project stores); append-only audit records. A maintained data map records location, purpose, and encryption status per class.

Subservice organizations (carve-out method)

The following subservice organizations' controls are excluded from this assessment; each is monitored through the vendor register and relied upon under its own compliance program.

SUBSERVICE ORGANIZATION	SERVICE	DATA THAT REACHES IT	VENDOR POSTURE
Amazon Web Services	Cloud infrastructure (EKS, EC2, EBS, S3, ECR)	All platform data	SOC 1/2/3, ISO 27001; DPA with SCCs
Anthropic	LLM API for assistant and enrichment features	Configuration metadata; sampled rows during mapping/enrichment (excludable per project)	SOC 2 Type II; DPA in progress (Section V)
Atlassian (Bitbucket)	Source hosting & CI	Source code; scoped CI credentials	SOC 2, ISO 27001; DPA
Google	Workspace identity for staff; OAuth for the audit portal	Staff identity claims only	SOC 1/2/3, ISO 27001

Complementary user-entity controls

Cortex's controls assume that customer organizations: (a) manage their own membership and role assignments and remove leavers promptly; (b) hold a lawful basis for the personal data their projects ingest; (c) set the project data-sensitivity flag where regulated data must not appear in LLM enrichment samples; and (d) protect the credentials of data-source connections they configure.

IV Trust Services Criteria, controls & tests

Controls are stated as implemented and operating; the testing column records how each was verified. Testing is continuous — the automated portions re-run on every audit cycle and every code change, so results reflect the state at the report date, not a sampled moment. A

result of SEE §V means the control area is partially open and carries a disclosed remediation plan.

5	76	0	13
TSC categories in scope	Controls in the mapped catalog	Open security findings at report date — application & in-boundary platform	Open matters disclosed in Section V, each with a plan

CRITERIA	CONTROL ACTIVITY	TESTING PERFORMED	RESULT
CONTROL ENVIRONMENT, RISK & COMMUNICATION (CC1 – CC3, CC9)			
CC3.2	A risk register is maintained with likelihood/impact scoring, current mitigations, and residual actions; reviewed quarterly and on architecture change.	Register inspected; review cadence and per-risk mitigations verified against implemented controls.	NO EXCEPTIONS
CC9.2	A vendor & subprocessor register records every third party, the data that flows to it, agreements, and compliance posture; new vendors receiving customer data require a DPA before integration.	Register inspected against actual data flows; agreement status verified per vendor.	SEE §V
CC2.1	Deficiencies are tracked as issues with an append-only lifecycle; closure is mechanical — an issue auto-resolves only when its control re-detects as passing.	Issue lifecycle sampled end-to-end; auto-resolution behavior verified by re-scan.	NO EXCEPTIONS
CC1.x	Organizational governance policies (ethics, oversight, competence, accountability) are being formalized as a policy pack with recorded attestations.	Attestation status enumerated from the control catalog.	SEE §V
LOGICAL & PHYSICAL ACCESS (CC6)			
CC6.1	Staff authentication is federated to Google Workspace via OpenID Connect with verified-email and workspace-domain claims; MFA is enforced at the identity provider. Product credentials are stored as bcrypt hashes.	Authentication flow exercised end-to-end in a real browser; hashing library and configuration inspected; automated checks re-verify on every cycle.	NO EXCEPTIONS
CC6.1	Authorization is centralized in a single access policy evaluated on every project operation; organization scoping applies to all queries.	Policy unit-tested across every branch in CI; multitenant isolation reviewed periodically by structured RBAC review.	NO EXCEPTIONS

CRITERIA	CONTROL ACTIVITY	TESTING PERFORMED	RESULT
CC6.1	API access uses OAuth 2.1 bearer tokens with ~1-hour expiry, scoped per project; the engine integration surface is restricted to a read-only allowlist. Per-application deployment credentials are hash-stored, auto-rotated on redeploy, and individually revocable.	Token scoping and expiry inspected; allowlist contents verified against the served tool surface.	NO EXCEPTIONS
CC6.1	Secrets are injected from the platform secret store and access fails closed — services refuse to boot without their secrets; no fallback values exist in code. A CI gate blocks tracked secret material from entering the repository.	Continuous secret-hygiene scanning (private keys, env files, hardcoded fallbacks, cloud keys) on every cycle; CI gate verified active on both branches.	NO EXCEPTIONS
CC6.3	Workload identities follow least privilege: the application-deployment service account holds a minimal cluster role, per-application privileges are granted namespace-locally, and a Kubernetes ValidatingAdmissionPolicy constrains privilege-granting operations to the application namespaces and the designated role — enforced at the API server, keyed to the acting identity.	Enforcement tested live by attempting the constrained operations *as the governed identity* (server-side dry-run creates), including in restricted namespaces; effective permissions enumerated; independently re-tested by an adversarial reviewer probing for bypass paths.	NO EXCEPTIONS
CC6.5	Disposal paths exist per asset class: per-record, per-source, per-project, and per-user deletion cascade through configuration, object storage, and identity stores; volume disposal relies on encrypted-volume key destruction.	Deletion paths inspected per class; cascade semantics verified against schema constraints.	SEE §V
CC6.6	Network boundary controls: origin allowlist (no wildcard CORS), global rate limiting, and security-headers middleware on the API surface; TLS certificate verification is the enforced default on all outbound connections.	Automated configuration checks re-verify all four on every cycle.	NO EXCEPTIONS
CC6.7 / CC6.8	Runtime hardening: all container images declare a non-root user; platform- and engine-generated pods run with read-only root filesystems (scoped writable mounts only), `RuntimeDefault` seccomp, resource requests/limits, and digest-pinned data-store images. The few workloads requiring writable filesystems are individually named acceptances with recorded rationale.	CIS Kubernetes benchmark scanning (weekly plus on-demand); pod specs verified live after deployment; a headed browser round-trip confirms the product serves under the hardened runtime.	NO EXCEPTIONS
SYSTEM OPERATIONS (CC7)			

CRITERIA	CONTROL ACTIVITY	TESTING PERFORMED	RESULT
CC7.1	Continuous vulnerability management: dependency advisories gate CI at the critical level and are tracked continuously below it; lockfiles pin every package tree; the infrastructure scanner itself is version- and digest-pinned.	Dependency audits re-run per cycle across all package trees; CI gate configuration verified.	NO EXCEPTIONS
CC7.2	The platform and its infrastructure are scanned continuously (application checks per audit cycle; CIS Kubernetes benchmarks weekly; AWS account scans weekly under a dedicated read-only SecurityAudit role); every failing control becomes a tracked issue with an append-only lifecycle and recorded disposition rationale.	Scan cadence verified from the system of record; disposition records inspected for completeness.	NO EXCEPTIONS
CC7.1 / CC6.1	AWS account hardening baseline: EBS encryption-by-default, EBS snapshot public-access block, IAM account password policy (14+ characters, full complexity, 24-password reuse prevention, 90-day maximum age), and dedicated read-only SecurityAudit + Support IAM roles.	Applied 12 Aug 2026 via a reviewed declarative change (plan inspected before apply); post-change re-scan confirms each check passes; every remaining account-level finding carries a recorded disposition (owner-assigned or accepted with boundary rationale) — zero undispositioned.	NO EXCEPTIONS
CC7.2	An append-only, hash-chained audit log records administrative and security-relevant events; chain integrity is verified on every dashboard read. Failed logins are durably logged with reasons.	Chain verification exercised; log completeness sampled against known events.	SEE §V
CC7.3	A published security policy defines the reporting channel, acknowledgement, and severity-based remediation SLAs.	Policy presence and content verified per cycle.	NO EXCEPTIONS
CHANGE MANAGEMENT (CC8)			
CC8.1	Every build passes a CI verify gate — unit tests, dependency audit, tracked-secret scan — before images are produced; images are built only by CI. Code ownership routes review on sensitive surfaces.	Pipeline configuration verified on both branches per cycle; gate behavior confirmed on real builds.	SEE §V
CC8.1	Infrastructure changes flow exclusively through versioned overlay files and declarative apply; ad-hoc cluster edits are prohibited by policy. Customer configuration changes are individually versioned commits with full history — who, what, when — by construction.	Overlay-only policy verified against cluster state; configuration history inspected for attributability.	NO EXCEPTIONS
AVAILABILITY (A1)			

CRITERIA	CONTROL ACTIVITY	TESTING PERFORMED	RESULT
A1.1	Capacity is governed by per-workload resource requests/limits; a resilience assessment inventories single points of failure with mitigations and is revisited quarterly.	Limits enforcement verified by benchmark scan; assessment inspected.	SEE §V
A1.2	A backup & disaster-recovery inventory documents durability and restore path per data store; recovery objectives are set (RPO 24h / RTO 8h); all infrastructure is rebuildable from code and versioned configuration.	Inventory verified against the live estate; restore paths reviewed.	SEE §V
CONFIDENTIALITY (C1)			
C1.1	A data map records where confidential and personal data lives, why it is collected, and its encryption-at-rest status; access to detected PII columns must be governed by access-policy rows, enforced by a per-project audit check with closed-loop fix requests.	Data map verified against the estate; the PII-policy check runs on every project audit.	SEE §V
C1.2	Retention and deletion are documented per data class, including where copies persist (version history, future backups) and for how long.	Documentation reviewed against actual deletion paths.	SEE §V
PROCESSING INTEGRITY (PI1)			
PI1.1 / PI1.2	A project's processing contract is explicit, machine-readable data: source schemas are captured and pinned at connect time, governed columns are typed elements, transformations are typed with domain/codomain compatibility enforced — malformed pipelines cannot be wired. Unmapped columns never reach targets; rejects are visible records, not silent drops.	Contract enforcement exercised through the product; per-project audit checks verify rule coverage.	NO EXCEPTIONS
PI1.4 / PI1.5	Every pipeline run records per-stage record counts as its reconciliation surface; failures surface as failed jobs, never partial-silent. Stored integrity relies on transactional constraints, versioned configuration, and rebuildable derived stores with pinned lineage.	Run records inspected; constraint and lineage behavior verified through the product.	NO EXCEPTIONS
PRIVACY (P)			
P3.1	Personal data is inventoried by class with source, purpose, and location; collection is limited to the project's stated pipeline purpose.	Inventory verified against the estate.	NO EXCEPTIONS

CRITERIA	CONTROL ACTIVITY	TESTING PERFORMED	RESULT
P4.1 / P5.1	A data-subject access, correction, and deletion runbook operates on a 30-day SLA; corrections propagate by re-running pipelines from the corrected source — lineage makes propagation structural.	Runbook reviewed; deletion and correction paths verified per class.	SEE §V

Verification basis. "No exceptions" reflects the state re-detected by the continuous testing described above as of the report date. Enforcement controls are tested *as the identity they constrain* — permission listings alone are not accepted as evidence of admission-level enforcement — and the full control-by-control results, including every disposition and its recorded rationale, are preserved on the tamper-evident system of record for independent re-examination.

V Open matters & management's remediation plans

The following matters are open at the report date. None is an identified breach of the criteria in operation; each is a control whose implementation, verification, or formalization is not yet complete. All are tracked to closure with the owner and target stated.

AREA	CRITERIA	OPEN MATTER & PLANNED ACTION	TARGET
Production infrastructure baseline	CC6.3 / CC6.8	The hardened runtime baseline and admission-policy least-privilege model operating on the primary environment are scheduled to be applied to the production cluster, together with continuous benchmark scanning of production, in an announced change window.	Scheduled change window
Recovery rehearsal	A1.2	Backup and restore paths are documented per store with RPO 24h / RTO 8h targets; a full restore rehearsal with recorded results has not yet been performed. Scheduled backup jobs and a recorded drill are the closing actions.	Program Phase 2
Encryption-at-rest verification	C1.1 / CC6.5	**EBS encryption-by-default was enabled account-wide on 12 Aug 2026**, so every new volume is created encrypted. Remaining: per-volume verification of pre-existing volumes and S3 bucket-policy verification; asset disposal by key destruction closes with this verification.	Program Phase 2 (narrowed)

AREA	CRITERIA	OPEN MATTER & PLANNED ACTION	TARGET
Capacity alerting	A1.1	No automated alert on persistent-volume disk usage; a PV usage alert is the identified smallest closing action, scheduled.	Scheduled
Branch protection	CC8.1	Required pre-merge review must be verified/enabled in the git-host repository settings; code-ownership review routing is already in place.	Repo-settings change
Security-event alerting	CC7.3	Failed logins are durably logged; no push alert fires on bursts. A threshold alert on denial events in the audit portal is planned.	Program Phase 2
Retention enforcement	P4.1 / C1.2	Retention is documented per data class; time-to-live enforcement jobs are not yet running. Lands with the backup rollout; backup-copy retention (35 days) to be reflected in the DPA.	With backup rollout
LLM subprocessor DPA	CC9.2 / P	The data-processing agreement with the LLM provider is in progress. Until countersigned, projects with regulated data set the enrichment/sampling flag off so no row samples leave the platform.	In progress
Organizational policy attestations	CC1 / CC2 / P	Twenty governance controls (integrity & ethics, oversight, competence, incident-response and recovery-test formalization, privacy notice, choice & consent, disclosure) await formal policy-pack attestation with recorded owner and date.	Program Phase 2
Product-level MFA	CC6.1	MFA is enforced at the federated identity provider; a product-native second factor for non-federated accounts is on the roadmap.	Roadmap
Operator redundancy	CC1.4 / A1	Platform operations currently depend on a single credentialed operator; runbooks are documented and executable. Second-operator onboarding is tracked.	Tracked
Independent penetration test	CC4.1	A third-party penetration test is planned to complement continuous automated scanning.	Program Phase 2
Independent examination	—	A SOC 2 Type I examination by a licensed CPA firm, followed by a Type II observation window, is the scheduled path to attestation; the tamper-evident audit trail behind this report is intended as its evidence base.	Program Phase 3

Disclosure principle. Open matters are disclosed here with plans and targets rather than netted against completed work. Items marked "Program Phase 2/3" belong to the sequenced compliance program; phase completion is itself tracked on the system of record.

VI Basis of this report

This report follows the structure of an AICPA SOC 2 report — assessment report, management's assertion, system description, criteria-mapped controls with tests and results, and disclosed open matters — so that it can be read, challenged, and later examined on familiar terms.

Important — nature of this report. This is a rigorous, evidence-linked **management-prepared readiness assessment**, produced from Cortex's continuous-audit system of record and an independent adversarial review. It is **not** an examination or attestation performed by a licensed CPA firm, and it does not constitute a SOC 2 report under AICPA attestation standards. A SOC 2 Type I examination by an independent firm is the scheduled next step (Section V).

Evidence pack. Supporting documentation versioned with the platform (`docs/soc2/`): access matrix, risk register, vendor & subprocessor register, backup/DR inventory, data map & personal-data inventory, retention & disposal procedures, resilience assessment, and processing-integrity documentation. Control test results and issue lifecycles are preserved on the tamper-evident audit system of record.

Confidential — prepared for internal governance and prospective independent examination. Companion reports: repository tier and platform infrastructure tier (same evidence base, finding-level detail).