Infrastructure & Architecture Overview

Version: 2.0
Last Updated: 1st September 2026
Classification: Public

Infrastructure & Architecture Overview

This document presents Concord's infrastructure and architecture in a structured Q&A/schedule format. For security reasons, it intentionally omits implementation detail that would increase operational risk if disclosed.

Architecture Principles

Cloud-native design, security and privacy by design, scalability, high availability, resilience, modularity, API-first integration, operational observability, and responsible AI.

Platform Layers

Layer	Contents
Client	Web application and API/CI-CD clients
Identity & Authentication	SSO (SAML 2.0, OAuth 2.0/OIDC), native MFA, session management
Application & Business Services	AI governance engine, workflow engine, policy management, risk management, AI inventory, reporting
AI Integration & Orchestration	Multi-provider AI connectors, prompt handling, output processing
Data & Storage	Relational database, object storage, append-only audit log, backups

Layer	Contents
Cloud Infrastructure	Google Cloud Platform

Cloud Infrastructure

Concord's application infrastructure runs on Google Cloud Platform, primarily in the Canada (Toronto) region, using managed compute, storage, networking, monitoring, identity, and encryption services. Deployment is containerized and centrally managed rather than per-instance-configured, keeping the fleet's configuration consistent. Discuss specific data-residency requirements with us during procurement.

Multi-Tenant Architecture

Concord is a multi-tenant SaaS platform. Tenant data is logically segregated: each customer's data lives in its own database schema, with no query path that spans schemas — isolation is structural, not a filtered view within shared tables. Application-level authorization and API-level checks provide a second layer on top of that structural separation.

AI Integration Architecture

Concord integrates with AI capabilities through a multi-provider abstraction layer rather than a single hardcoded model, primarily Google Gemini today, allowing the underlying model to change as the field evolves without customer-visible disruption to governance workflows.

API Architecture

Concord's APIs support authenticated, authorized integration with customer systems and CI/CD pipelines: encrypted communication, input validation, rate limiting, audit logging, and version management. API documentation is available to authorized customers.

Identity and Access Management

Role-based access control, multi-factor authentication, and SSO (SAML 2.0, or OAuth 2.0/OIDC via Okta, Google, or Microsoft) — either can be required exclusively at the tenant level, with MFA then delegated to the customer's own identity provider. See the IAM Overview.

Encryption

TLS 1.2+ in transit; encryption at rest via the underlying cloud platform, with an additional application-layer encryption pass for particularly sensitive fields such as MFA secrets. See the Section encryption of Security Overview.

Networking

Firewalled, segmented, private cloud networking with load balancing and DDoS mitigation provided by the underlying cloud infrastructure.

Monitoring and Observability

Infrastructure, application, performance, availability, and security-event monitoring, plus log aggregation and alerting. Application errors are tracked via cloud-native error reporting tied to the code version that produced them.

Backup and Recovery

Automated daily backups with integrity verification and periodic restoration testing. See the BCDR Summary for the operational detail, and the applicable Service Level Agreement for specific recovery commitments.

High Availability

Redundant, managed cloud services, automated health monitoring, load balancing, fault isolation, and elastic capacity scaling reduce single points of failure. Availability commitments are defined in the applicable Service Level Agreement.

Change Management

Production changes go through peer review, testing, deployment validation, and post-deployment monitoring, with rollback capability. Emergency changes follow an expedited but still-reviewed path.

Shared Responsibility

Concord is responsible for: cloud platform configuration, application security, infrastructure management, monitoring, backups, and service availability.

Customers are responsible for: user administration, identity provider configuration where applicable, endpoint security, customer-managed integrations, and governance of their own data and AI workflows.

Additional Information

Available on request, subject to confidentiality obligations: Security Overview, Data Processing Addendum, Information Security Schedule, Service Level Agreement, and Subprocessor & Data Residency Schedule.
