

# Architecture overview (sample)

Sanitized excerpt for buyer review • Evidence ID: ENC-002

## Scope

This excerpt is a demo sample intended to show structure and clarity. Replace it with your real architecture overview and captured exports where possible.

## System boundaries

Production environment includes application services, storage, and logging/monitoring.

Corporate/workforce systems (IdP, ticketing, CI/CD) are included as evidence sources for controls.

# Data flows (sample)

Sanitized trust boundaries and flows • Evidence ID: ENC-002

## Ingress and auth

Requests enter through a managed edge/load balancer. Workforce access to admin systems is authenticated through the identity provider with MFA enforcement. Customer auth may be customer-managed depending on deployment.

## Storage and processing

Data is stored in managed storage and databases. This sample avoids internal identifiers and focuses on the control model: access is role-restricted and audited.

## Egress and integrations

Outbound integrations are explicit and scoped. Exports (audit logs, evidence snapshots) are generated from systems of record and stored with capture dates and cadence.

# Encryption and access model (sample)

What reviewers usually ask about • Evidence ID: ENC-002

## Encryption model

Data in transit is protected via TLS. Data at rest is encrypted using managed storage encryption. Key management and rotation are handled by the underlying cloud KMS.

## Access model

Administrative and support access is restricted to authorized roles. Privileged actions are logged. Where sensitive artifacts exist, sharing is gated behind agreement and time windows.

## Reviewer notes

Reviewers want scope, capture dates, and citations. Prefer exports/logs over screenshots, and add a refresh cadence for evidence that becomes stale.