Security & Trust Evidence Pack (Template)

Version: 1.0
Date: 2026-02-26
Organization: FinCo (Example)

Purpose

This document is a template evidence pack designed for testing security-questionnaire autofill systems. Statements below are written to be directly citable.

1) Identity & Access Management

MFA/2FA: Multi-factor authentication (MFA) is required for privileged accounts (admins, SRE, DBAs) and administrative consoles.

SSO: Single Sign-On is supported for corporate users via SAML 2.0.

Least privilege: Production access is restricted to authorized personnel and granted using least privilege principles.

Access reviews: Access recertification is performed quarterly (every 90 days) by system owners and Security.

2) Encryption

In transit: All external endpoints require encryption in transit using TLS 1.2 or higher (TLS 1.2+). Public APIs terminate SSL/TLS at the edge with a minimum TLS version of 1.2.

Internal services: Internal services use mTLS where supported; otherwise traffic is restricted to private networks.

At rest: Databases and object storage are encrypted at rest using AES-256 with cloud-provider managed keys via a centralized KMS.

Backups: Backup snapshots and archives are encrypted at rest using AES-256 and stored with KMS-managed keys.

3) Logging & Monitoring

Centralized logging: Production systems send logs to a centralized logging platform with searchable indices for on-call engineers.

Authentication events: Authentication attempts (success and failure) are logged.

Privileged/admin actions: Role changes and administrative console actions are logged and monitored.

Alerting: Alerting rules include excessive failed logins, unusual admin actions, and elevated error-rate spikes.

4) Vulnerability Management & Secure SDLC

Code review: Code changes require peer review and CI checks prior to deployment.

Dependency scanning: Automated dependency scanning runs in CI on each pull request.

Infrastructure scanning: Infrastructure vulnerability scanning is performed monthly.

Emergency changes: Emergency changes follow an expedited approval process and are reviewed post-deployment.

5) Incident Response

IR plan: A documented incident response process is maintained.

Severity levels: Security incidents are triaged using severity classification: Sev1, Sev2, Sev3.

On-call: An on-call rotation is used for incident response.

Post-incident reviews: Post-incident reviews are required for Sev1 and Sev2 incidents.

6) Business Continuity & Disaster Recovery

Backups: Critical databases are backed up daily.

RPO: Recovery Point Objective (RPO) is 24 hours for critical systems.

RTO: Recovery Time Objective (RTO) is 24 hours for critical systems.

DR tests: Disaster recovery testing is performed annually.

7) Data Lifecycle & Deletion

Log retention: Standard log retention is approximately 2 months.

Deletion requests: Data deletion requests follow open ticket -> verify requestor -> execute deletion workflow -> confirm completion.

Deletion SLA: Requests are fulfilled within 30 days.

8) Compliance & Regulatory

SOC 2: A SOC 2 Type II report is available covering the Trust Services Criteria: Security, Availability, Confidentiality.

GLBA: For U.S. financial services data, customer nonpublic personal information (NPI) is handled in alignment with GLBA requirements.

PCI DSS: PCI DSS is not applicable because FinCo does not store, process, or transmit payment card data.

Appendix: Quick Controls Matrix

MFA: MFA required for privileged/admin access.

TLS: Minimum TLS version is 1.2 (TLS 1.2+).

At-rest encryption: AES-256 with KMS-managed keys for databases, object storage, and backups.

Logging: Centralized logging with auth events and admin actions.

Vulnerability scanning: Dependency scanning in CI and monthly infrastructure scans.