Finexusinc.ai Integrated Governance, Risk, Compliance & AI Oversight Framework

Prepared to Address Due Diligence/Audit Questions

Prepared for: Executive Management, Product/Engineering, InfoSec, Compliance, and Bank Vendor Due Diligence Reviewers

Date: May 22, 2026

Confidential

Note: This framework synthesizes industry best practices (SOC 2 Trust Services Criteria, NIST Cybersecurity Framework, NIST AI Risk Management Framework, GLBA Safeguards Rule, and U.S. banking third-party risk management guidance) and integrates existing Finexus policies into a single, bank-ready management framework.

1. Executive Summary

Finexus delivers compliant, security-first AI fintech solutions for community banks and equipment finance lenders. This document defines Finexus's integrated Governance, Risk, and Compliance (GRC) management framework, including data protection/privacy, information security, application security, incident response, disaster recovery, third-party risk management, and AI governance/model risk management. The framework is designed to be audit-ready and to meet expectations commonly used in bank vendor due diligence and SOC 2 examinations.

Scope includes:

- Corporate governance, ethics, and compliance management
- Enterprise risk management (ERM) and risk register practices
- Data protection, privacy, and data governance
- Identity and access management (IAM) and acceptable use
- Secure engineering, change management, and web application security
- Security incident response, data breach response, and communications
- Business continuity and disaster recovery (BC/DR)
- Third-party/subprocessor risk management (TPRM) across the lifecycle
- AI governance aligned to trustworthy AI principles and model risk management

2. Framework Objectives & Principles

Objectives:

- Protect the confidentiality, integrity, and availability of customer and company information.
- Demonstrate bank-grade governance for AI systems, including inventories, monitoring, and human oversight.
- Provide an auditable control environment aligned to SOC 2 Trust Services Criteria and bank examiner expectations.
- Support consistent, secure delivery of Finexus services and products through documented processes and evidence.

Design principles: risk-based, least-privilege/need-to-know, lifecycle governance, and continuous improvement.

3. Audit and Due Diligence Coverage (Required Disclosures)

3.1 Most Recent SOC 2 Certification, Security Program Overview

- SOC 2: Most recent status available for sharing is reflected in Finexus due diligence materials (SOC 2 indicated as completed in April 2025, SOC2 audit in progress for 2026, will update when completed).

- Security program overview: Finexus maintains a security program spanning access controls, encryption, monitoring/logging, secure SDLC, vulnerability management, incident response, disaster recovery, and third-party oversight.

3.2 Current Incident Response & Escalation Procedures

Finexus maintains incident response and escalation procedures that include detection, triage, containment, investigation, remediation, and executive escalation. Security Response Plans (SRPs) are maintained for services/products and define escalation paths, contacts, and severity-based remediation timelines. For suspected theft/breach/exposure events involving protected or sensitive data, personnel must promptly report the event through established channels for investigation and response.

3.3 Notification Timelines Following Confirmation of Unauthorized Access or Data Exposure

Finexus expected notification timeline (client-facing standard):

- Finexus will notify affected clients within 72 hours of confirming unauthorized access to, or exposure of, hosted customer data, or sooner where required by contract or law.

3.4 Significant Cybersecurity Incidents or Investigations (Past 12 Months)

Disclosure statement:

- No significant cybersecurity incidents or investigations affecting hosted customer data are identified within the provided materials. If required, Finexus can provide an incident attestation for the prior 12 months.

3.5 Most Recent Penetration Test / Vulnerability Assessment / Third-Party Security Review

Testing and validation posture:

- Penetration test: Most recent date/vendor in progress as of May 2026, will provide latest test summary when available.
- Vulnerability assessments: Web application security assessments are performed based on release type and risk, aligned to OWASP testing guidance and risk rating concepts.
- Third-party security review: Performed as part of vendor/platform risk management for contract employees and vendor providers. Background checks/employee verification ongoing and current list can be provided upon request.

3.6 Material Changes in Past 12 Months Impacting Cybersecurity or Resiliency

Material change disclosure statement:

- No material infrastructure, hosting, staffing, or operational changes impacting cybersecurity or platform resiliency are identified within the provided materials. If applicable, Finexus can provide a change summary for the prior 12 months.

3.7 Outsourced Service Providers Supporting Platform or Hosted Data

Third-party/subprocessor support statement:

- Yes. Finexus uses outsourced service providers/subprocessors to materially support platform operations (e.g., development, DevOps, QA, operational tooling). These providers are subject to due diligence, contractual security obligations, least-privilege access controls, and ongoing monitoring/oversight.

4. Governance & Oversight

4.1 Executive Accountability

Executive management is ultimately accountable for compliance obligations, approvals of exceptions (where required), and oversight of operational and security practices.

4.2 Key Roles and Committees

AI Governance Committee / Steering Committee: Strategic oversight of AI initiatives, risk tolerance, and adherence to AI policy; supports lifecycle responsibilities.

InfoSec Team: Maintains security and data protection policy reviews, coordinates training, and reviews/approves third-party agreements that may handle sensitive data.

Information Security Administrator: Manages and monitors need to have system access for Finexus and client employees, breach reporting and coordinates investigations and procedures for reported incidents.

Data Owners: Assign classifications, approve access to sensitive data, and review access lists per schedule.

Business Unit Security Champion: Develops and maintains product/service Security Response Plans (SRPs) with InfoSec.

Engineering & Operations: Implements controls (change management, monitoring, remediation) and supports audits/evidence.

5. Enterprise Risk Management (ERM)

5.1 Risk Domains

- Information Security Risk
- Data Protection & Privacy Risk

- AI / Model Risk
- Third-Party / Subprocessor Risk
- Operational Risk (including change control and service reliability)
- Business Continuity & Disaster Recovery Risk

5.2 Risk Lifecycle

Finexus applies a lifecycle risk approach consistent with bank third-party risk expectations: planning, due diligence/selection, contracting, ongoing monitoring, and termination/exit planning.

5.3 Core ERM Artifacts (Operational Requirements)

- Centralized Risk Register linking: risks → controls → owners → evidence → review cadence.
- Risk scoring methodology (likelihood × impact; include customer/regulatory impact for AI and data risks).
- Issue management and remediation tracking for findings (security assessments, incidents, audits).
- Executive reporting (quarterly) covering KRIs/KPIs and major issues.

6. Compliance Management System (CMS)

6.1 Baseline Standards

Finexus aligns its controls and evidence to the following widely used baselines:

- SOC 2 Trust Services Criteria (Security required; Availability/Confidentiality/Privacy scoped as needed).
- NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).
- NIST AI Risk Management Framework (trustworthy AI; Govern/Map/Measure/Manage).
- GLBA Safeguards Rule expectations for safeguards and service provider oversight.
- U.S. banking interagency third-party risk management lifecycle guidance.

6.2 Policy Governance & Exceptions

Policies are reviewed at least annually (or as required by policy) and exceptions require documented approval by the responsible authority (InfoSec or executive leadership depending on the policy).

6.3 Audit Evidence Library

Finexus maintains an evidence repository organized by control domain (Access, Change Management, AppSec, Incident Response, DR Testing, Training, Vendor Oversight). Evidence is retained per contractual and regulatory expectations.

7. Data Protection, Privacy & Information Governance

7.1 Data Classification & Need-to-Know

Finexus classifies information (Restricted, Confidential, Public) and enforces need-to-know access with data owner approvals and periodic access reviews.

7.2 Personal Data Protection

Personal data is handled under a data protection standard that defines collection, storage, processing, encryption requirements for electronic transfer, and restrictions on informal sharing. Centralized sources of truth are preferred to local copies.

7.3 Data Transfer Controls

Restricted data transmissions over external networks must be encrypted and use approved secure mechanisms. Personal data is not sent via unsecured channels (e.g., standard email or chat).

7.4 Breach Response Integration

Breach reporting and response processes define mandatory reporting, investigation, containment, executive escalation, forensics, communications planning, and remediation.

8. Identity, Access & Acceptable Use

8.1 Acceptable Use

Company systems are for business use; monitoring and periodic audits are performed. Unacceptable activities are prohibited, and violations result in disciplinary action.

8.2 Minimum Access / Remote Access

Remote access requires encryption (VPN), strong credentials, endpoint protections (anti-virus), and InfoSec approval for use of external resources to conduct Finexus business.

9. Secure Engineering, Change Control & Application Security

9.1 Secure Development & Production Separation

Developers do not have permission to modify production program files; changes are deployed through operations and follow change management. Production data access is limited to read-only where applicable and routed through application interfaces when possible.

9.2 Web Application Security (OWASP-Aligned)

Web applications undergo security assessments based on release type (major, third-party, point/patch, emergency). Remediation requirements follow OWASP risk rating concepts and require validation testing for Medium risk or higher issues.

10. Incident Response & Security Response Plans

10.1 Security Response Plans (SRPs)

Each business unit develops SRPs per product/service that include service description, data flows/architecture, contact information and escalation, triage steps, mitigations and testing, and severity-based remediation timelines. SRPs must be version controlled and reviewed annually.

10.2 Data Breach Response

The breach response process includes mandatory reporting, immediate access removal for affected resources, executive escalation for confirmed breaches, forensic investigation as required, and communications planning with legal and communications teams.

11. Business Continuity & Disaster Recovery

Finexus maintains baseline disaster recovery planning and requires creation of contingency sub-plans (emergency response, succession, data study, service criticality list, backup/restoration, equipment replacement, and media management). Annual tabletop exercises and annual reviews/updates are required.

12. Third-Party & Subprocessor Risk Management (TPRM)

12.1 Lifecycle Program

Finexus manages third-party risk through planning, due diligence, contracting, ongoing monitoring, and termination/exit activities consistent with bank examiner expectations.

12.2 Controls for Subprocessors

- Due diligence and risk assessment prior to engagement.
- Contractual confidentiality, data protection, and security obligations.
- Least-privilege access restrictions and monitoring/oversight of activities.
- Alignment to Finexus secure development, change management, and incident response requirements.
- Maintenance of a current subprocessor list available upon request.

13. AI Governance & Model Risk Management

13.1 Trustworthy AI

Finexus's AI policy embeds trustworthy AI characteristics including human oversight and control, robustness and safety, privacy and data governance, transparency and explainability, fairness and non-discrimination, and accountability.

13.2 AI Risk Monitoring & Review

AI systems in production are monitored for performance degradation, bias drift, and security vulnerabilities, with periodic reviews (at least annually) and defined roles for governance and compliance.

13.3 AI System Inventory

Finexus maintains an AI system inventory including system identifiers, purpose, owners, data sources and sensitivity, model type/architecture, performance metrics, risk classification, compliance obligations, and review/audit dates. New AI systems are registered via a standardized process and the inventory is kept current.

14. Metrics, Reporting & Continuous Improvement

14.1 Executive Reporting

- Access approvals and quarterly access review completion
- SRP coverage across products/services and annual review completion
- AppSec assessment coverage and remediation aging by severity
- Incidents/breaches: counts, time-to-contain, remediation completion
- DR testing completion and corrective actions

14.2 Continuous Improvement

Findings from assessments, incidents, audits, and vendor monitoring are used to update controls, policies, training, and risk register entries.

Appendix A — Reference Documents (Attached Separately)

- AI Policy (AI.pdf)
- Acceptable Use Policy (Acceptable_Use.pdf)
- Anti-Bribery and Corruption Policy (Anti-Bribery.pdf)
- Data Breach Response Policy (Data_Breach_Response.pdf)
- Data Protection Standard (Data_Protection.pdf)
- Minimum Access Policy (Minimum_Access.pdf)
- Security Response Plan Policy (Security_Response_Plan.pdf)
- Web Application Security Policy (Web_Application_Security.pdf)
- Disaster Recovery Plan Policy (Disaster_Recovery_Plan.pdf)
- Finexus Vendor Due Diligence Response (finexus_due_diligence_response_final 032426.docx)
- Finexus Due Diligence base policies 2019 052126

Appendix B — SOC 2 Control Alignment (Summary)

Finexus aligns its controls to the SOC 2 Trust Services Criteria (Common Criteria CC1–CC9). The following summary describes control alignment at a high level; detailed evidence is available upon request.

- CC1 – Control Environment: Governance, ethics, policy framework, and accountability.
- CC2 – Communication & Information: Security communication and training; policy dissemination and updates.
- CC3 – Risk Assessment: Enterprise risk assessment, including AI risk management and third-party risk evaluation.
- CC4 – Monitoring Activities: Monitoring/logging, periodic review and testing, and management oversight.
- CC5 – Control Activities: Operational controls, approvals, and enforcement mechanisms.
- CC6 – Logical & Physical Access Controls: Least privilege, remote access safeguards, RBAC/MFA posture, and access reviews.
- CC7 – System Operations: Vulnerability management, incident response, and operational monitoring.
- CC8 – Change Management: Secure SDLC, change control, release governance, and application security assessments.
- CC9 – Risk Mitigation: Incident/breach response, disaster recovery planning/testing, and remediation tracking.