ThirdNexa

Financial-Services Third-Party Risk Compliance Checklist

A practical review tool for vendor governance, due diligence, contracts, Regulation S-P incident readiness, ongoing monitoring, evidence retention, and examiner preparation.

Version 1.0 — September 24, 2026
Use this checklist to structure an internal review with your compliance and legal advisers. Check the box only after your firm has confirmed the item and retained appropriate evidence.

1. Governance and accountability

☐	Program ownership Name the executive sponsor, operational owner, reviewers, and final approver for third-party risk decisions.	Owner: _____ Evidence / notes: _____
☐	Written process Document how vendors are inventoried, risk-classified, reviewed, monitored, escalated, renewed, and terminated.	Owner: _____ Evidence / notes: _____
☐	Regulatory scope List the registrations, jurisdictions, data types, and business activities that may affect vendor oversight obligations.	Owner: _____ Evidence / notes: _____
☐	Decision authority Define who may accept risk, approve a vendor, impose conditions, or require remediation. Keep the decision with the firm.	Owner: _____ Evidence / notes: _____

2. Complete vendor inventory

☐	Relationship record Capture legal name, service provided, business owner, contacts, status, geography, and material subcontractors where relevant.	Owner: _____ Evidence / notes: _____
☐	Access profile Record whether the vendor handles customer information, personal data, payment data, confidential records, or critical systems.	Owner: _____ Evidence / notes: _____

☐	Criticality Document operational dependency, substitutability, concentration risk, and impact if the service is unavailable.	Owner: _____ Evidence / notes: _____
☐	Source and changes Keep source evidence and an activity history showing who added or changed the record and when.	Owner: _____ Evidence / notes: _____

3. Risk classification and due diligence

☐	Inherent risk rationale Record the factors behind the firm-selected risk tier. Treat automated suggestions as prompts only.	Owner: _____ Evidence / notes: _____
☐	Proportionate review Match diligence depth and review frequency to data access, systems access, criticality, jurisdiction, and service type.	Owner: _____ Evidence / notes: _____
☐	Evidence Collect current security, privacy, resilience, insurance, financial, audit, and control evidence appropriate to the relationship.	Owner: _____ Evidence / notes: _____
☐	Questionnaires Use a consistent questionnaire or an internal evidence-based review, and preserve the exact responses and attachments reviewed.	Owner: _____ Evidence / notes: _____

4. Contracts and required terms

☐	Scope and accountability Confirm services, responsibilities, performance expectations, subcontracting, audit rights, and regulator access where applicable.	Owner: _____ Evidence / notes: _____
☐	Information safeguards Review confidentiality, security, data-use, data-return, deletion, and incident-notification provisions.	Owner: _____ Evidence / notes: _____
☐	Regulation S-P readiness For relevant contracts, record whether a 72-hour service-provider notification clause has been verified and where it appears.	Owner: _____ Evidence / notes: _____
☐	Lifecycle dates Track effective date, term, renewal, notice window, cancel-by date, and termination or transition requirements.	Owner: _____ Evidence / notes: _____

5. Incident and notification readiness

☐	Escalation path Document how a vendor reports an incident, who receives it, and who evaluates legal, customer, regulator, and insurer notifications.	Owner: _____ Evidence / notes: _____
☐	Dated incident record Capture occurred, discovered, vendor-notified, firm-notified, contained, and resolved dates without overwriting earlier facts.	Owner: _____ Evidence / notes: _____
☐	Customer information Record whether customer information may be involved, the basis for that assessment, and supporting vendor communications.	Owner: _____ Evidence / notes: _____
☐	Regulation S-P timing Covered institutions should be prepared to evaluate the service-provider notification and customer-notification timelines in the final rule.	Owner: _____ Evidence / notes: _____

6. Ongoing monitoring and findings

☐	Review calendar Set and monitor risk-based review dates, document expirations, contract notices, questionnaire deadlines, and assigned tasks.	Owner: _____ Evidence / notes: _____
☐	Findings Record the issue, severity, owner, due date, remediation, evidence, and independent verification before closure.	Owner: _____ Evidence / notes: _____
☐	Performance and change Reassess when services, data access, ownership, subcontractors, incidents, performance, or business criticality change.	Owner: _____ Evidence / notes: _____
☐	Renewal decision Bring open findings, incidents, performance, evidence, and notice dates into renewal or termination decisions.	Owner: _____ Evidence / notes: _____

7. Evidence retention and examiner preparation

☐	Reproducible package Be able to produce the inventory, assessments, contracts, document index, reviews, findings, incidents, decisions, and activity history.	Owner: _____ Evidence / notes: _____
☐	Actor attribution Show who performed each review or action, including client staff, consultants, and authorized platform support.	Owner: _____ Evidence / notes: _____

☐	Exceptions Explain missing evidence, overdue work, accepted risk, and compensating controls instead of presenting an unexplained blank.	Owner: _____ Evidence / notes: _____
☐	Test before the exam Generate and read the evidence package periodically; confirm names, dates, page breaks, empty sections, and export quality.	Owner: _____ Evidence / notes: _____

Official sources and review notes

These sources are starting points. Confirm the current text, effective dates, scope, exceptions, and regulator-specific interpretation before relying on them.

SEC Regulation S-P amendments (2024)
https://www.sec.gov/files/rules/final/2024/34-100155.pdf

Interagency Guidance on Third-Party Relationships (2023)
https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

FINRA Regulatory Notice 21-29
https://www.finra.org/rules-guidance/notices/21-29

FTC Safeguards Rule, 16 CFR Part 314
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

EU Digital Operational Resilience Act (DORA)
https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

GDPR Article 28
https://eur-lex.europa.eu/eli/reg/2016/679/art_28/oj

NIST Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework

Important limitation

This checklist is educational information, not legal, compliance, regulatory, cybersecurity, or accounting advice. It is not exhaustive and does not determine whether any law, rule, guidance, framework, contract term, or standard applies to your organization. ThirdNexa is software that helps firms organize workflow and records. The firm remains responsible for its policies, supervision, controls, oversight, risk decisions, regulatory interpretations, and books-and-records obligations. Consult qualified professionals for advice specific to your organization.