VendRisk360
ASSESS · MONITOR · STAY AHEAD

WHITEPAPER

Risk-Tiered Due Diligence: Scaling Assessments for Critical, Material and Low-Risk Vendors

How to scope, tier, assess, sign off and reassess third parties so that diligence effort follows risk and stands up to audit and examination.

Published 25 September 2026

Written for Heads of TPRM, CROs, CISOs, compliance officers, internal auditors

Online www.vendrisk360.com/resources/whitepapers/risk-tiered-due-diligence/

Contents

A practitioner guide to risk-tiered vendor due diligence: intake scoping, inherent risk versus criticality, tier criteria, evidence by tier, SOC report review, residual risk, sign-off, reassessment cadence and how internal audit tests the program.

Most third-party risk programs do not fail because they lack a questionnaire. They fail because they apply the same questionnaire to every vendor, drown the team in low-value reviews, and then run out of time for the handful of relationships that could actually hurt the organization. Regulators across jurisdictions have converged on the same expectation: due diligence and oversight should be commensurate with the risk and criticality of the relationship, and the organization should be able to show how it decided what "commensurate" means.

This paper sets out a working model for risk-tiered due diligence. It covers how to scope a new relationship at intake, how to separate inherent risk from criticality, how to define tiers that map to regulatory concepts, what evidence to require at each tier, how to evaluate that evidence and derive residual risk, who signs off, how often to reassess, and how internal audit should test the whole thing. It is written for practitioners who have to run the program and for auditors who have to form an opinion on it.

KEY TAKEAWAYS

- Inherent risk and criticality answer different questions. Score both, and let the higher of the two drive the tier.
- Intake scoping by business case, data types and services is the control that makes every later step proportionate. Get it wrong and the whole assessment is mis-sized.
- Evidence beats attestation. Define a minimum evidence set per tier and evaluate scope, period, opinion and exceptions, not just the presence of a report.
- Residual risk ratings should be defensible and repeatable, not precise. A simple, documented method outperforms a weighted formula nobody can explain.
- Sign-off needs segregation of duties: the preparer, reviewer and approver should be different people, and conflicts should be recorded.
- Internal audit will re-perform tiering, sample assessments and test timeliness. Design the program so that the evidence of review exists by default.

Why one-size-fits-all fails

A single, uniform assessment process produces two predictable failures. The first is waste: a catering supplier or a subscription to an industry newsletter receives the same several-hundred-question security assessment as a core banking processor. Vendors resent it, business owners route around it, and capacity is spent where risk is lowest. The second failure is shallowness at the top: because the process is standardized, the critical vendors receive no more scrutiny than the trivial ones. Nobody reads the SOC 2 exceptions, nobody tests the business continuity claims, and the concentration of operational dependency goes unexamined.

Supervisory guidance is explicit that this is not acceptable. The US Interagency Guidance on Third-Party Relationships: Risk Management (June 2023) expects a risk-based approach, with more comprehensive and rigorous oversight for relationships that support higher-risk activities, including critical activities. OSFI Guideline B-10 frames third-party risk management as proportionate to the risk and criticality of the arrangement. DORA requires financial entities to distinguish contractual arrangements that support critical or important functions. PRA SS2/21 distinguishes material outsourcing. APRA CPS 230 introduces material service providers. The RBI Master Direction on Outsourcing of IT Services requires a materiality assessment. The common thread is that proportionality must be designed, documented and applied consistently.

Tiering is the mechanism: deep effort on the few relationships that matter, and a complete, defensible inventory of everyone else.

Inherent risk versus criticality

Many programs collapse two distinct questions into one score. Separate them.

Inherent risk asks: if this vendor's controls failed, how much harm could it cause to our data, customers, compliance position or reputation? It is driven by what the vendor touches: the types and volume of data, the level of system access, whether it interacts with customers, whether it performs a regulated activity on your behalf, and where it operates.

Criticality asks: if this vendor stopped performing tomorrow, how badly would our operations be disrupted, and how quickly could we recover or replace it? It is driven by dependency: whether the service supports a critical operation or important business service, substitutability, time to exit, the impact on customers and the market, and concentration across the vendor base.

The two are independent. A payroll bureau processing employee bank details may carry high inherent risk but be replaceable within a quarter. A market data feed may hold no personal data at all yet be impossible to operate without for more than a few hours. A cloud provider hosting a core platform scores high on both.

INHERENT RISK AND CRITICALITY COMPARED

Dimension	Inherent risk	Criticality
Core question	What harm if controls fail?	What disruption if service stops?
Main drivers	Data types, access, regulated activity	Dependency, substitutability, exit time
Typical owner	TPRM, information security, privacy	Business owner, operational resilience
Primary diligence focus	Security, privacy, compliance controls	Resilience, financial health, exit planning

A practical rule: rate each on its own scale, then set the tier to the higher of the two. That prevents a vendor with modest data exposure but severe operational dependency from being waved through as low risk, which is exactly the gap that operational resilience regimes such as the PRA and FCA rules on important business services and APRA CPS 230 were designed to close.

Intake scoping: business case, data and services

The intake questionnaire is the most important control in the program, because it determines everything that follows. It should be completed by the business owner, not the vendor, and it should be short enough to be completed accurately.

The business case

Capture what the organization is buying and why: the service description, the business process it supports, the expected contract value and term, whether it replaces an existing vendor, and whether it supports a critical operation or important business service. Ask whether the vendor will act on the organization's behalf toward customers, perform a regulated function, or make or support decisions using models or AI.

Data types

Data type selection drives much of the inherent risk score. Use a fixed taxonomy so that business owners pick from a list rather than describe data in free text.

DATA TYPE TAXONOMY FOR INTAKE SCOPING

Data type	Examples	Typical inherent risk driver
Customer PII	Names, addresses, national IDs, account numbers	Privacy law, breach notification, conduct
Cardholder data	PAN, cardholder name with PAN, sensitive authentication data	PCI DSS scope, requirement 12.8 obligations
PHI	Claims, diagnoses, member records	HIPAA business associate obligations
Credentials	Passwords, API keys, privileged or federated access	Direct path into your environment
Confidential business data	Financials, strategy, source code, M&A	Competitive and market harm
None	Facilities, office supplies, public data only	Operational and financial risk only

Ask for approximate volume (record counts or bands), whether data leaves the organization's environment, the countries where it will be stored, processed or accessed, and whether the vendor will use sub-processors. Cross-border handling matters under GDPR, the UK GDPR, India's DPDP Act 2023, Saudi and UAE PDPL, Singapore's PDPA and the Philippines Data Privacy Act of 2012.

Services and access

Capture the delivery model (SaaS, on-premises software, managed service, professional services, hardware, physical), the level of network or application access, whether access is privileged, whether the vendor connects to production, and whether the vendor hosts or processes on your behalf. A consultant with read-only access to a sandbox and a managed security provider with domain administrator rights are both "IT services" but sit at opposite ends of the risk range.

DESIGN THE INTAKE FOR ACCURACY, NOT COMPLETENESS

Every question on the intake form should change either the tier or the scope of the assessment. If an answer never changes anything, remove the question. Business owners complete short, consequential forms more carefully, and the TPRM team should still challenge answers that look inconsistent with the contract or statement of work.

Tier criteria and evidence

Three tiers are enough for most organizations. More tiers invite debate about boundaries and rarely change the assessment approach. Define each tier by criteria that can be applied consistently, and map them to the regulatory vocabulary your supervisors use.

TIER CRITERIA WITH REGULATORY ANALOGUES

Tier	Typical criteria	Regulatory analogues
Critical	Supports a critical operation; hard to substitute; sensitive data at scale or privileged access; significant customer impact on failure	US critical activities; DORA critical or important functions; PRA material outsourcing; APRA material service providers
Material	Sensitive data or meaningful access but substitutable; moderate operational impact; regulated activity with limited scale	Higher-risk arrangements under OSFI B-10; RBI material IT outsourcing depending on facts
Low risk	No sensitive data or access; readily substitutable; negligible customer or operational impact	Relationships subject to baseline oversight only

Mapping to the regulatory analogues is not always one to one. DORA's concept of critical or important functions, the PRA's material outsourcing, APRA's material service providers and the US notion of critical activities each have their own definitions and tests. Record, in the tiering

methodology, how each tier corresponds to each regime that applies to you, and confirm the mapping with counsel or your supervisor where it matters. A vendor can be Material in your internal scheme but still require inclusion in a DORA register or a CPS 230 register of material arrangements.

Tiering should also carry overrides. Allow the TPRM function to raise a tier with justification, and require second-line approval to lower one. Record the calculated tier, override, rationale and approver.

Minimum evidence by tier

Once the tier is set, define the minimum evidence set. The table below is a common starting point; adjust it for the service type (a professional services firm with no data access will not have a SOC 2 report, and should not be penalized for it).

MINIMUM EVIDENCE BY TIER

Evidence	Critical	Material	Low risk
SOC 2 Type II (or equivalent)	Required	Required if data or access	Not required
SOC 1 Type II	Required if ICFR relevant	If ICFR relevant	Not required
Penetration test summary	Required, within 12 months	Requested	Not required
BCP/DR plan and test results	Required, with test results	Plan required	Not required
Financial statements	Audited, annual	Summary or credit check	Not required
Insurance certificates	Required (cyber, E&O)	Required	If contractually needed
Information security policies	Required	Required	Not required
ISO 27001 certificate and SoA	Accepted with scope review	Accepted with scope review	Not required
PCI DSS AOC	Required if cardholder data	Required if cardholder data	Not applicable
Privacy program and DPA	Required if personal data	Required if personal data	If personal data
Sanctions and adverse media screening	Required	Required	Required

An ISO/IEC 27001 certificate is only as useful as its scope: check the Statement of Applicability and certified scope against the service, locations and teams you rely on. Similarly, a PCI DSS Attestation of Compliance should be matched to the services you receive; PCI DSS v4.0 requirement 12.8 expects you to maintain a list of third-party service providers, understand which requirements each manages, and monitor compliance status at least annually.

Sanctions screening applies to every tier: it is cheap, and a sanctions breach is a breach regardless of tier.

Questionnaires and control coverage

Questionnaires remain useful, but only when they are scoped, non-duplicative and tied to controls.

- **Use scoping logic.** Only show questions relevant to the tier, data types and services captured at intake. A vendor that does not host data should not be asked about database encryption at rest.
- **Avoid duplicate asks.** If the SOC 2 report covers logical access, do not ask the vendor to describe logical access again. Ask only about gaps the report does not address, or controls outside its scope.
- **Accept standard formats.** Allow vendors to submit a completed Shared Assessments SIG or a CSA CAIQ where one exists, and map it to your control set rather than forcing re-entry.
- **Prefer evidence over attestation.** For each high-value question, request the artifact that proves the answer: a policy, a configuration screenshot, a test report, a certificate.
- **Map every question to a control.** Each question should be traceable to a control objective in your framework, which in turn maps to the standards you report against (for example NIST CSF 2.0, ISO/IEC 27001:2022 Annex A, or a regulator's framework).

Control domain coverage

Define the control domains your assessments cover and state which apply at each tier. A comprehensive framework typically spans 30 or more domains; a Critical assessment evaluates all applicable ones, a Material assessment a defined core set, and a Low-risk review a baseline.

ILLUSTRATIVE CONTROL DOMAIN COVERAGE BY TIER

Domain group	Critical	Material	Low risk
Governance, policies, risk management	Full	Core	Baseline
Identity and access management	Full	Full	Not assessed
Data protection, encryption, privacy	Full	Full	If personal data
Vulnerability, patching, pen testing	Full	Core	Not assessed
Logging, monitoring, incident response	Full	Core	Not assessed

Domain group	Critical	Material	Low risk
Business continuity and resilience	Full, with test evidence	Plan review	Not assessed
Subcontractor and fourth-party management	Full	Core	Not assessed
Financial condition, insurance	Full	Core	Baseline
Compliance, legal, sanctions	Full	Core	Screening
AI and model use (where applicable)	Full	Core	Disclosure only

Fourth-party coverage deserves attention at the Critical tier. DORA, EBA outsourcing guidelines, PRA SS2/21, APRA CPS 230 and the RBI IT outsourcing direction all address sub-outsourcing or fourth parties in some form. At minimum, identify the subservice organizations a critical vendor depends on and understand whether its SOC report includes or carves them out.

Evaluating evidence

Receiving a SOC 2 report is not the same as reviewing it. A reviewer should work through the same questions every time and record the answers.

Scope

Does the report cover the service you receive, the systems and locations involved, and the Trust Services Criteria you care about? A SOC 2 covering only the security criterion tells you nothing about availability or confidentiality commitments. Check whether subservice organizations are handled using the inclusive or carve-out method; with carve-out, their controls are excluded and you need separate assurance for material ones, along with the complementary subservice organization controls (CSOCs) the vendor expects them to perform.

Period and currency

A Type II report covers a period; a Type I report covers a point in time and says nothing about operating effectiveness. Note the period end date. If the gap between period end and your review is material (commonly more than three months), request a bridge letter covering the gap and confirming no significant changes. A bridge letter is management's representation, not auditor assurance, so treat it accordingly.

Opinion and exceptions

Read the auditor's opinion. A qualified opinion means one or more control objectives or criteria were not met. Then read the exceptions in the testing section, even in an unqualified report. For each exception, record whether it affects controls relevant to your use, what management's response says, and whether it was remediated.

Complementary user entity controls

CUECs are controls the vendor assumes you perform. If you do not perform them, the vendor's controls may not achieve their objectives for you. Extract the CUECs, assign each to an internal owner, and confirm they are in place. This is one of the most frequently missed steps and one of the most commonly questioned by auditors.

HYPOTHETICAL EXAMPLE: A CLEAN OPINION WITH A RELEVANT EXCEPTION

A reviewer receives an unqualified SOC 2 Type II report for a Critical payments vendor. The testing section records an exception: in 3 of 25 sampled terminations, access was removed after the vendor's stated five-day window. Management states the process was automated mid-period. The reviewer records a finding on timely deprovisioning, requests evidence of the automation and a sample of post-change terminations, and notes that the organization's own CUEC for notifying the vendor of departing users must also be confirmed.

Rating results and deriving residual risk

Residual risk is inherent risk after considering the effectiveness of the vendor's controls and any compensating measures on your side. The rating method should be simple enough that two reviewers reach the same answer and a reviewer can explain it to an examiner.

A DEFENSIBLE RESIDUAL RISK METHOD

Step	What the reviewer does	Output
1. Rate controls	For each domain: effective, partially effective, ineffective, not evidenced	Domain ratings
2. Weight by relevance	Flag domains most relevant to the data types and services in scope	Key domains
3. Apply rules	Any ineffective key domain caps residual at High; any not evidenced key domain requires a finding	Rule-based floor
4. Consider compensating controls	Contract terms, your own monitoring, encryption you control	Documented adjustments
5. Assign residual	High, Medium or Low with a written rationale	Residual rating and narrative

Avoid false precision. A residual risk score of 67.4 out of 100 implies a measurement accuracy the underlying evidence cannot support, and invites challenge on the weighting rather than the substance. Qualitative ratings driven by explicit rules, supported by narrative, are more defensible.

If you do use numeric scores internally, publish the formula, calibrate it against reviewer judgement, and report bands rather than decimals.

"Not evidenced" should be its own rating. It is different from "ineffective" and different from "effective". It usually means the vendor has not provided proof, and it should generate a finding rather than a silent assumption either way.

Findings, risk acceptance and sign-off

Every control gap that matters should become a finding with an owner, a severity, a remediation plan agreed with the vendor, and a target date. Track findings to closure and require evidence of closure rather than a vendor's email saying it is done.

Where a finding cannot be remediated before contract signature or within an acceptable time, the organization must decide whether to accept the risk. Risk acceptance is a formal decision with an owner, a rationale, compensating controls, an expiry date and an approver whose authority matches the severity.

ILLUSTRATIVE RISK ACCEPTANCE AUTHORITY

Residual severity	Who can accept	Maximum duration
Low	Business owner with TPRM concurrence	Until next reassessment
Medium	Business unit head and second-line risk	12 months, then re-approval
High	Senior executive (for example CRO) and CISO for security risks	6 months, with board or committee reporting
Critical or regulatory breach	Executive committee or board risk committee	Time-bound, with remediation plan

Risk acceptances should expire. An open-ended acceptance is, in practice, a permanent exception that nobody revisits. Report open acceptances and their expiry dates to the risk committee.

Sign-off and segregation of duties

The final assessment is a decision, and decisions need independent review. Define roles and keep them separate.

PREPARER, REVIEWER AND APPROVER MATRIX

Role	Responsibility	Cannot also be
Preparer	Collects evidence, evaluates controls, drafts findings and rating	Reviewer or approver of the same assessment

Role	Responsibility	Cannot also be
Reviewer	Challenges evidence, ratings and findings; confirms method was followed	Preparer or approver of the same assessment
Approver	Accepts residual risk and approves the relationship at the tier	Preparer; ideally not the business owner for Critical

Record conflicts of interest. A reviewer who previously worked at the vendor, holds a personal relationship with its staff, or championed its selection should declare it, and the assessment should be reassigned. For Critical vendors, require that the approver is not the business sponsor who wants the contract signed. The sign-off record should show who did each step, when, and what they reviewed, so that the evidence of review exists without anyone reconstructing it later.

Reassessment cadence and triggers

Tiering drives frequency as well as depth. Cadence is a policy choice: the program should set reassessment frequency, evidence depth and sign-off for each tier in its own policy, calibrated to its regulators and risk appetite. One common example:

- **Critical:** full reassessment annually, with continuous monitoring in between.
- **Material:** full reassessment every 24 months, with an annual refresh of key evidence such as SOC reports and insurance.
- **Low risk:** review at contract renewal, plus ongoing sanctions screening.

Calendar cadence is only half the design. Define trigger events that force an out-of-cycle reassessment or tier review:

- A security incident or data breach at the vendor, or credible reports of one.
- A change in services, data types or access that would change the intake answers.
- Merger, acquisition, change of control or significant restructuring at the vendor.
- Material adverse news, litigation, regulatory or enforcement action, or sanctions exposure.
- Deterioration in financial condition or credit indicators.
- A qualified SOC opinion or significant new exceptions.
- Service level failures that suggest control or capacity problems.
- A new fourth party supporting a critical service.

Critical vendors also need an exit strategy that is reviewed on cadence. DORA, EBA outsourcing guidelines, PRA SS2/21, APRA CPS 230 and the RBI direction all expect exit planning for critical or material arrangements.

Governance and how internal audit tests the program

A tiered program needs board-approved policy, a documented methodology, defined roles across the three lines, and management information that shows whether it is working. Useful program metrics include the inventory by tier, overdue assessments, open findings by severity and age, open risk acceptances and expiry dates, and the proportion of Critical vendors with a current exit plan.

Internal audit, or an independent review function as the US interagency guidance describes, will test both design and operating effectiveness. A walkthrough typically follows one new vendor from intake request to approval, inspecting each artifact and confirming the control operated as described. Then the auditor samples.

INTERNAL AUDIT TEST PLAN FOR A TIERED TPRM PROGRAM

Test area	Procedure	Evidence inspected
Population completeness	Reconcile vendor inventory to accounts payable, contracts and SSO app lists	Inventory, AP extract, reconciliation
Tier accuracy	Re-perform tiering for a sample using intake answers and the methodology	Intake forms, tier calculation, overrides
Assessment quality	For a sample by tier, confirm required evidence was obtained and evaluated	Evidence set, SOC review notes, ratings
Evidence of review	Confirm preparer, reviewer and approver were distinct and dated	Sign-off records, audit trail
Timeliness	Compare reassessment dates to cadence; test trigger events were acted on	Schedule, monitoring alerts, reassessment records
Findings and exceptions	Trace findings to closure evidence; test risk acceptances for authority and expiry	Findings log, acceptances, approvals
CUEC coverage	For Critical vendors, confirm CUECs were mapped and owners confirmed	CUEC register, owner attestations

Stratify samples by tier so Critical vendors are always represented. A common audit finding is not that assessments were bad, but that the program cannot produce evidence that the review happened, who did it, or what they looked at.

WHAT EXAMINERS AND AUDITORS ASK

- Show us the complete third-party inventory and how you know it is complete.
- Explain your tiering methodology and walk us through how a specific vendor was tiered.
- Which relationships support critical activities or critical or important functions, and how is that recorded?
- For this Critical vendor, show the due diligence evidence, the SOC report review, and how exceptions and CUECs were addressed.
- Who approved this relationship, and who reviewed the assessment before approval?
- List open findings and risk acceptances, their owners and expiry dates.
- How do you know reassessments are on schedule, and what triggered the last out-of-cycle review?
- What is your exit strategy for this vendor, and when was it last tested or reviewed?

Pitfalls and checklist

Common pitfalls

- **Vendor-completed intake.** The vendor describes its service optimistically; the business owner should describe what the organization is buying.
- **Tiering on spend.** Contract value is a poor proxy for risk. Low-cost SaaS tools often hold the most sensitive data.
- **Ignoring carve-outs and CUECs.** The most important controls are sometimes the ones excluded from the report.
- **Permanent risk acceptances.** Acceptances without expiry dates accumulate silently.
- **Self-approval.** The same person preparing and approving an assessment defeats the purpose of review.
- **Calendar-only reassessment.** A vendor breached in month two should not wait until month twelve.

Practical checklist

- [ ] Board-approved TPRM policy with a documented tiering methodology
- [ ] Intake completed by the business owner using a fixed data type taxonomy
- [ ] Inherent risk and criticality scored separately; tier set to the higher
- [ ] Tier mapping to each applicable regulatory regime documented

- [ ] Minimum evidence set defined per tier and service type
- [ ] Questionnaires scoped, de-duplicated and mapped to controls
- [ ] SOC reports reviewed for scope, period, opinion, exceptions, subservice method and CUECs
- [ ] Residual risk derived using a documented, rule-based method
- [ ] Findings tracked to evidenced closure
- [ ] Risk acceptances approved at the right authority, with expiry dates
- [ ] Preparer, reviewer and approver separated, with conflicts recorded
- [ ] Reassessment cadence scheduled by tier, with trigger events defined
- [ ] Exit strategies in place and reviewed for Critical vendors
- [ ] Obligations confirmed with counsel or regulators for each jurisdiction

How VendRisk360 supports this

VendRisk360 is built around the tiered model described in this paper. The platform's vendor lifecycle management begins with intake scoped by business case and data types, so the business owner's answers drive the assessment rather than a generic questionnaire. Each vendor is assigned a criticality tier of Critical, Material or Low risk, and the tier drives the depth of the assessment, the sign-off chain and the reassessment cadence. Cadence is configurable to your own policy (for example, Critical annually, Material every 24 months and Low risk at renewal), not a fixed rule.

Vendor risk assessments are artifact-based and span more than 30 control domains. Your analysts review the evidence, record ratings, findings and notes, and sign off, or VendRisk360 assessors do so through Comprehensive Vendor Risk Assessment Services. Every decision is recorded in the audit trail with a named reviewer, which supports the evidence-over-attestation principle while keeping accountability with people.

SOC 1 and SOC 2 review covers exceptions, carve-outs, subservice organizations and complementary user entity controls, so the review steps described above are captured in a consistent structure. Findings flow into remediation plans, and formal risk acceptance is recorded with its rationale and approver.

Multi-stage sign-off enforces segregation of duties between preparer, reviewer and approver, and produces a sign-off certificate for each assessment. Vendors respond through a vendor portal with one-time-code access, and each vendor sees only its own requests.

Between assessments, continuous monitoring adds the outside-in view: the vendor's external attack surface, shadow infrastructure, indicators of compromise, breaches and security incidents, adverse news and litigation, regulatory and enforcement actions and sanctions, routing confirmed-

only alerts to the vendor owner so trigger events can prompt reassessment. Nth-party intelligence maps fourth-party relationships across vendors and tracks CUECs.

How to work with VendRisk360. On the Vendor Lifecycle Management Platform, your team manages vendors, sends due diligence and evidence requests through the vendor portal, performs the review, records it and signs off, with every step tracked in a full audit trail. With Comprehensive Vendor Risk Assessment Services, you onboard the vendor and VendRisk360's certified assessors collect the evidence and follow up with the vendor, perform the risk assessment scaled to the vendor's tier with a second-expert quality review, and follow findings through remediation. You see each vendor's progress on the platform in near real time and keep final approval, as regulators expect. Continuous Monitoring Services add the outside-in view between assessments, and Report-Specific Reviews (SOC Report Review, Information Security Program Review and Business Continuity Program Review) are available standalone or alongside either. Assessors hold certifications such as CISSP, CISA, CISM, CRISC and ISO/IEC 27001 Lead Auditor and Lead Implementer, with PCI DSS implementation experience. AI is optional: where a customer opts in, it assists only with completeness checks and key-date extraction on vendor evidence and with an AI-assisted first pass on SOC reports that the expert assessor verifies. Every review, rating and sign-off is performed by an expert assessor or by the customer's own reviewers.

For governance and audit, the platform provides board and executive reporting, including an Audit Committee / Examiner Readiness deck and an Annual TPRM Program Review, Excel exports of registers and findings, and an examiner package export containing assessments, evidence, sign-offs and the audit trail. See the platform overview or book a demo.

About VendRisk360

VendRisk360 is an independent company providing a third-party risk management platform and expert services for regulated organizations: banks, credit unions, fintech and payments, healthcare and SaaS. The platform runs vendor lifecycle management, risk-tiered assessments, continuous monitoring, nth-party intelligence and board-ready reporting from one governed record per vendor, combining point-in-time, evidence-based review with continuous outside-in monitoring. Customers run it themselves on the Vendor Lifecycle Management Platform, or add Comprehensive Vendor Risk Assessment Services, Continuous Monitoring Services and Report-Specific Reviews delivered by certified VendRisk360 assessors.

Learn more at **vendrisk360.com** or write to **info@vendrisk360.com**.

This paper is general guidance for practitioners, not legal advice. Regulatory requirements change and vary by jurisdiction and institution; confirm your obligations with counsel and your supervisors.