VendRisk360
ASSESS · MONITOR · STAY AHEAD

WHITEPAPER

Board-Ready Third-Party Risk: What Directors and Executives Need to See

A practical guide to third-party risk appetite, KRIs, board packs, escalation triggers and the evidence examiners and auditors expect from board oversight.

Published 25 September 2026

Written for Board members, CROs, heads of TPRM, CISOs, compliance officers, internal audit

Online www.vendrisk360.com/resources/whitepapers/board-ready-third-party-risk/

Contents

How to design board and executive reporting on third-party risk: appetite statements, KRIs and KPIs, reporting cadence, escalation triggers, board pack anatomy, supervisory expectations across regimes, and how internal audit tests it.

Most boards now receive some form of third-party risk report. Far fewer receive one that lets directors do their job: set appetite, see whether the organization is inside it, challenge management where it is not, and record decisions. The typical pack is a count of assessments completed, a pie chart of vendors by tier and a list of overdue items with no indication of whether any of it matters.

This paper sets out what a board-ready third-party risk report looks like. It covers what the board is and is not accountable for, the questions directors should be able to answer from the pack, how to express appetite as measurable tolerances, how to select key risk and performance indicators, cadence and escalation, the anatomy of the pack itself, what supervisors across major regimes expect, and how internal audit tests the whole chain from source data to minutes. Obligations differ by jurisdiction and charter, so confirm specifics with counsel and your supervisors.

KEY TAKEAWAYS

- The board owns oversight and appetite, not operations. Reporting should be built to support approval, challenge and decisions, not to prove activity.
- Express third-party risk appetite as a small set of measurable tolerances with clear owners and breach consequences.
- Pair lagging indicators with leading ones, and show trend over at least four periods rather than a single snapshot.
- Define out-of-cycle escalation triggers in advance so a breach at a critical vendor reaches directors in days, not at the next quarterly meeting.
- Minutes must evidence challenge and decisions. Examiners read them, and so does internal audit.
- Every number in the pack should be traceable to a system of record and re-performable by an auditor.

The board's oversight role

Across regimes the pattern is consistent: the board (or management body) remains accountable for risk arising from third-party relationships even when the activity is performed by someone else. Outsourcing an activity does not outsource the responsibility. What differs by jurisdiction is how explicitly the regulator assigns specific approvals to the board.

What the board is accountable for

- Approving the third-party risk management policy (or the outsourcing or ICT third-party policy, depending on the regime) and reviewing it periodically.
- Setting risk appetite for third-party risk and confirming that it is consistent with the enterprise risk appetite framework.

- Approving, or delegating with clear criteria, entry into arrangements that support critical activities, critical operations or critical or important functions.
- Holding management accountable for operating the program within appetite, and ensuring management has adequate resources and expertise.
- Receiving sufficient, timely information to oversee material relationships, concentration, incidents and remediation.
- Ensuring independent assurance over the program, usually through internal audit reporting to the audit committee.

What the board is not accountable for

The board does not review individual SOC 2 reports, score questionnaires or chase vendors for evidence; pulling directors into that detail blurs accountability and hides the portfolio view. A useful test is whether an item in the pack requires a board decision, informs a board decision, or confirms that delegated authority is operating as intended. If it does none of these, it belongs in a management report.

DELEGATION NEEDS A PAPER TRAIL

Where the board delegates approval of critical arrangements to a committee or executive, the delegation should be written into the policy or committee charter, with the limits of the delegation and the reporting that flows back. Examiners commonly ask to see this chain: board resolution, charter, and the reports that evidence delegated authority is being used within its limits.

Questions directors should ask

Directors do not need to be TPRM specialists, but they should be able to answer a small set of questions from the pack without asking management to go away and find out. If the pack cannot answer them, the pack is the problem.

QUESTIONS A BOARD PACK SHOULD ANSWER

Question	What good looks like in the pack
Which third parties could cause us serious harm if they failed tomorrow?	A named critical vendor watchlist with the service each supports and its current status
Are we inside our third-party risk appetite?	Tolerances with current value, trend and a clear red/amber/green against the threshold
Where are we concentrated?	Concentration by provider, by fourth party and by geography for critical services

Question	What good looks like in the pack
What has gone wrong since we last met?	Incidents and breaches at vendors, impact on us, and actions taken
What risk have we knowingly accepted, and is it expiring?	Open risk acceptances with owner, rationale, expiry and compensating controls
Could we actually exit a critical vendor?	Status of exit plans and whether any have been tested
What is coming that will change our obligations?	A short regulatory horizon with dates and readiness status
What do you need from us?	Explicit decisions requested, with options and a recommendation

Questions directors often fail to ask, and should, include: which critical vendors have not been reassessed within policy cadence, how many vendors are in use but not in the inventory, which fourth parties sit underneath multiple critical vendors, and whether any risk acceptance has been renewed more than once.

WHAT EXAMINERS AND AUDITORS ASK ABOUT BOARD ENGAGEMENT

- How does the board define and measure appetite for third-party risk?
- Provide the last four board or committee packs covering third-party risk, with minutes.
- Where in the minutes did directors challenge management, and what changed as a result?
- How was the board informed of the most recent significant incident at a third party, and how quickly?

Risk appetite and tolerances

A third-party risk appetite statement has two layers. The qualitative statement says what the organization will and will not accept. The quantitative tolerances translate that into measurable limits, each with an owner and a defined consequence when breached.

Writing the qualitative statement

A usable statement is short and specific. It typically covers: low appetite for critical services depending on vendors without an assessed and tested exit or continuity plan; very low appetite for customer data held by third parties without contractual security, breach notification and audit rights; low appetite for concentration where a single provider or fourth party supports multiple critical services; and moderate appetite for innovation through non-critical vendors, provided they are inventoried and tiered.

Translating appetite into tolerances

Each tolerance should use data you already hold, be calculable the same way every period, and have green, amber and red bands. Amber is an early warning that triggers management action. Red is a breach that is reported to the board or risk committee with a remediation plan.

WORKED EXAMPLE TOLERANCES (ILLUSTRATIVE THRESHOLDS ONLY)

Tolerance metric	Green	Amber	Red
Critical vendors with assessment older than policy cadence	0	1 to 2	3 or more, or any over 90 days late
Critical vendors without a documented exit plan	0	1	2 or more
High-severity findings open past due date at critical vendors	0 to 2	3 to 5	6 or more
Active risk acceptances past expiry	0	1	2 or more
Critical services dependent on a single fourth party	0 to 1	2	3 or more
Vendors in use but not in inventory (discovered in period)	0 to 2	3 to 10	More than 10

HYPOTHETICAL EXAMPLE: APPETITE BREACH AND BOARD RESPONSE

A hypothetical mid-size bank sets a tolerance of zero critical vendors without a documented exit plan. The quarterly pack shows two critical vendors (a core processor and a card platform) in red. The CRO presents the breach with a remediation plan: exit plans drafted within 60 days, a tabletop test for the core processor within the next two quarters, and a request that the risk committee accept the interim position. The committee approves the plan, asks for monthly updates until green, and the minutes record the decision, the owner and the date by which the tolerance will be back within appetite.

Avoid tolerances that measure only activity, such as number of assessments completed. They say nothing about exposure. Also avoid setting thresholds so loose that they are never breached; a tolerance that has been green for three years with no change in the portfolio is probably not calibrated.

KRIs, KPIs, leading and lagging

Key risk indicators (KRIs) measure exposure: how much risk the organization carries. Key performance indicators (KPIs) measure how well the program operates. Boards need both, but in different proportions: the board pack leans toward KRIs, while the executive committee and

program management need more KPIs.

EXAMPLE KEY RISK INDICATORS

Metric and definition	Formula and source	Threshold example	Owner
Critical vendor coverage: share of critical vendors with a current assessment	Current assessments divided by critical vendors; vendor inventory and assessment records	Below 100 percent is amber	Head of TPRM
Overdue high findings: high or critical findings past remediation date	Count of open findings where due date is before period end; findings register	More than 5 is red	Vendor owners, reported by TPRM
Concentration: critical services relying on one provider or fourth party	Count of shared dependencies across critical services; nth-party map	More than 2 is amber	CRO
Adverse monitoring signals: confirmed breach, sanctions or enforcement alerts at critical vendors	Confirmed alerts in period; continuous monitoring log	Any confirmed breach is red	CISO
Expired risk acceptances still in effect	Acceptances past expiry date without renewal; risk acceptance register	Any is amber	Risk owner
Contract gaps: critical contracts missing audit, notification or exit clauses	Contracts failing clause checklist; contract repository	Any is amber	Legal and procurement

EXAMPLE KEY PERFORMANCE INDICATORS

Metric and definition	Formula and source	Threshold example	Owner
Assessment cycle time: intake to sign-off	Median days per tier; workflow timestamps	Critical over 60 days is amber	Head of TPRM
Vendor evidence responsiveness	Median days from request to complete evidence; portal logs	Over 21 days is amber	TPRM analysts
Remediation closure rate	Findings closed on time divided by findings due in period; findings register	Below 80 percent is amber	Vendor owners
Pipeline backlog	Intake requests older than service level; intake queue	More than 10 is amber	TPRM operations
Offboarding completion	Exits with access revocation and data destruction evidence; offboarding records	Below 100 percent is amber	Vendor owners

Leading and lagging indicators

Lagging indicators tell you what already happened: incidents at vendors, findings that went overdue, breaches of tolerance. Leading indicators signal that risk is building before it materializes. In third-party risk, useful leading indicators include a rising vendor attack surface score, deteriorating financial or adverse media signals, repeated slippage on remediation dates, a growing share of critical vendors with qualified SOC opinions or unaddressed complementary user entity controls, key-person departures on the vendor side, and a growing backlog of unassessed intake requests. A pack made up only of lagging indicators tells the board what went wrong after it is too late to influence it.

Cadence, audiences and escalation

Different governance bodies have different jobs, so they need different reports on different cycles. The content should be layered: the same data, cut at different altitudes.

REPORTING CADENCE BY AUDIENCE

Audience	Typical cadence	Focus
Board of directors	Quarterly summary; annual program review	Appetite status, critical vendors, concentration, decisions requested
Board risk committee	Quarterly, with monthly updates when in breach	KRIs, tolerance breaches, risk acceptances, emerging risks, regulatory horizon
Audit committee	Quarterly or per audit cycle	Assurance results, audit findings on TPRM, examiner findings, remediation status
Executive committee	Monthly	KPIs, pipeline, overdue remediation, resourcing, incidents

Out-of-cycle escalation triggers

Waiting for the next scheduled meeting is not acceptable for some events. Define triggers in the policy, name who notifies whom, and set a time frame. Typical triggers include:

- A confirmed security incident or data breach at a critical vendor affecting the organization's data or services.
- An outage at a critical vendor that exceeds, or is likely to exceed, an impact tolerance for an important business service or critical operation.
- A material change in concentration, such as a critical vendor being acquired by another critical vendor, or a fourth party becoming a shared single point of failure.
- A regulatory or enforcement action, sanctions designation or insolvency event affecting a critical vendor.

- A red tolerance breach that cannot be remediated within the agreed time frame.
- A supervisor inquiry or notification obligation arising from a third-party event.

Escalation normally goes first to the CRO and relevant executive, then to the chair of the risk committee, with a written briefing within an agreed period and full committee or board discussion where the impact warrants it. Several regimes require regulatory notification of material outsourcing or incidents within set time frames, so the escalation path should be aligned with the incident reporting process rather than run in parallel.

Anatomy of a board pack

A board pack on third-party risk should read in the order a director thinks: am I okay, what changed, what do you need from me, then the supporting detail.

Core components

- **One-page summary.** Overall position against appetite, the three to five things that changed, and decisions requested. If a director reads only this page, they should know whether to worry.
- **Heat map.** Critical and material vendors plotted by inherent risk and residual risk, or by likelihood and impact of disruption, with movement arrows since last period.
- **Critical vendor watchlist.** Named vendors, the service each supports, assessment status, open high findings, monitoring signals and exit plan status.
- **Concentration.** Shared providers and fourth parties beneath critical services, geographic concentration, and any change since last period.
- **Overdue findings and risk acceptances.** Aged findings by severity, and every active risk acceptance with owner, rationale, compensating controls and expiry.
- **Pipeline.** New critical or material arrangements in flight, with expected approval dates and any that will require board approval.
- **Incidents.** Third-party incidents in the period, impact, root cause where known, and follow-up actions.
- **Regulatory horizon.** New or changing requirements with effective dates and readiness.

Design principles

- **So-what first.** Every chart or table carries a one-line interpretation. "Overdue high findings rose from 3 to 7, driven by two vendors; both have remediation plans due next month" is more useful than a bar chart alone.
- **Trend, not snapshot.** Show at least four periods for each KRI. Direction and pace of change matter more than the point value.

- **Decisions requested.** State explicitly what the board is asked to approve, note or challenge, with options and management's recommendation.
- **Consistency.** Keep definitions, thresholds and layout stable across periods so changes reflect risk, not reformatting. When a definition changes, say so and restate prior periods.

SAMPLE BOARD PACK OUTLINE

Section	Content	Length
1. Summary and decisions	Appetite status, key changes, decisions requested	1 page
2. Appetite dashboard	KRIs with thresholds, RAG status and four-period trend	1 page
3. Critical vendor watchlist	Named critical vendors, status, signals, exit readiness	1 to 2 pages
4. Heat map and concentration	Residual risk plot; shared dependencies and fourth parties	1 page
5. Findings and risk acceptances	Aged overdue findings; active and expiring acceptances	1 page
6. Incidents	Third-party incidents, impact and actions	1 page
7. Pipeline	New critical and material arrangements in flight	Half page
8. Regulatory horizon	Changes, dates, readiness	Half page
Appendix	Full registers, definitions, methodology	As needed

Supervisory expectations across regimes

Supervisors differ in wording but converge on the same themes: board-approved policy, board-level appetite, oversight of critical arrangements, adequate information, and evidence that oversight actually occurred. The summaries below are a starting point; check the current text of each instrument.

- **United States.** The Interagency Guidance on Third-Party Relationships: Risk Management (June 2023; OCC Bulletin 2023-17, Federal Reserve SR 23-4, FDIC FIL-29-2023) places responsibility for oversight with the board, including approving policies, approving or delegating approval of contracts for critical activities, and receiving reports that allow it to oversee risk. Management is responsible for implementation. Oversight should be commensurate with the criticality and risk of each relationship.
- **NCUA.** NCUA supervisory letters, including Letter to Credit Unions 07-CU-13, expect credit union boards and management to oversee third-party relationships through due diligence and ongoing monitoring. Because NCUA lacks direct examination authority over credit union service vendors, examiners place heavy reliance on the credit union's own oversight and reporting.
- **Canada.** OSFI Guideline B-10 (final April 2023, effective May 1, 2024) expects a third-party risk management framework with clear accountability, with senior management responsible and the board overseeing, and scales expectations to the risk and criticality of each arrangement.

- **European Union.** Under DORA (Regulation (EU) 2022/2554, applying from 17 January 2025), the management body bears ultimate responsibility for ICT risk management. That includes approving the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, and reviewing the ICT third-party risk strategy.
- **United Kingdom.** PRA SS2/21 (effective 31 March 2022) expects boards to approve the outsourcing and third-party risk policy and to oversee material arrangements, alongside the PRA and FCA operational resilience framework, where the board approves important business services and impact tolerances.
- **India.** The RBI Master Direction on Outsourcing of IT Services (April 2023, effective 1 October 2023) requires a board-approved outsourcing policy, with the board responsible for oversight of material outsourcing.
- **Australia.** APRA CPS 230 (effective 1 July 2025) makes the board ultimately accountable for operational risk management, including oversight of material service providers, and requires tolerance levels for critical operations to be approved by the board.
- **Singapore.** MAS Guidelines on Outsourcing and the Technology Risk Management Guidelines expect the board and senior management to maintain oversight of outsourcing and third-party technology risk.
- **Middle East and Philippines.** SAMA's Rules on Outsourcing and Cyber Security Framework, the CBUAE Outsourcing Regulation and Standards, and BSP outsourcing and IT risk rules all assign governance responsibility to the board and senior management, with approval and reporting expectations for material arrangements.

WHAT SUPERVISORS TYPICALLY REQUEST

- Board-approved third-party, outsourcing or ICT third-party risk policy and evidence of periodic review.
- Risk appetite statement and the tolerances that apply to third-party risk.
- The register of arrangements, showing which support critical activities or critical or important functions.
- Evidence of notification to the supervisor where required for material arrangements or incidents.

Minutes and evidence of challenge

Supervisors and auditors do not only read the pack; they read the minutes to see whether the board engaged with it. Minutes that say "the committee noted the report" suggest a board that received information without overseeing anything.

Good minutes record the questions directors asked, management's answers, any follow-up actions with owners and dates, and decisions taken with the rationale. Follow-up actions should appear in an action log that is reviewed at the next meeting, so the loop closes visibly.

HYPOTHETICAL EXAMPLE: MINUTES THAT EVIDENCE CHALLENGE

A hypothetical insurer's risk committee minutes read: "A director asked why the payments processor remained on the watchlist for a third quarter. The Head of TPRM explained that two high findings on access management were delayed pending the vendor's platform upgrade. The committee asked whether compensating controls were effective and requested a validation by second line before the next meeting. The CRO confirmed the risk acceptance expires in 45 days and will not be renewed without committee approval. Action: second-line validation, owner CRO, due before next meeting."

- [ ] Minutes record specific questions, not just "discussion".
- [ ] Decisions are distinguished from items noted.
- [ ] Actions carry an owner and a due date.
- [ ] The action log is reviewed at the next meeting.
- [ ] Risk acceptances above a defined level are explicitly approved and minuted.
- [ ] Out-of-cycle briefings are noted at the next scheduled meeting.

How internal audit tests board reporting

Internal audit typically treats board reporting as a control: the control objective is that the board receives complete, accurate and timely information on third-party risk sufficient to exercise oversight. Testing covers design and operating effectiveness.

Design effectiveness

The auditor reviews the policy, committee charters and reporting procedures to confirm that the required content, cadence and escalation triggers are defined, that KRI definitions and thresholds are documented, and that ownership of each metric is assigned. A walkthrough follows one reporting cycle end to end: extraction of data from source systems, calculation of metrics, review and sign-off by management, submission to the committee, and minuting of the discussion.

Operating effectiveness

- **Data lineage.** For each KRI, trace the reported number back to the system of record and document every transformation. Metrics compiled manually in spreadsheets with no

documented steps are a frequent finding.

- **Completeness of the inventory.** Reconcile the vendor inventory to accounts payable, procurement and contract records for the period. Payees not in the inventory indicate unmanaged relationships, and every percentage in the pack is only as good as its denominator.
- **Reconciliation to source.** Select a sample of reported items (for example, overdue findings or critical vendors) and agree them to the findings register and assessment records. Then sample from source to report to test for omissions.
- **KRI re-performance.** Independently recalculate a sample of KRIs using the documented definition and compare to the reported value. Differences should be explained.
- **Timeliness and escalation.** For events in the period that met an escalation trigger, confirm the briefing reached the right people within the defined time frame.
- **Evidence of review.** Confirm management review and sign-off of the pack before submission, and that minutes and action logs show follow-through.

WHAT INTERNAL AUDIT WILL ASK FOR

- KRI definitions, formulas, data sources and thresholds, with the date of last approval.
- Extracts from source systems as at each reporting date.
- Working files or queries used to calculate each metric.
- Evidence of management review before the pack was issued.
- Reconciliation of the vendor inventory to payments and contracts.
- Minutes and action logs for the committees that received the reports.

Common pitfalls

- **Activity reporting.** Counts of assessments completed tell the board how busy the team was, not how much risk the organization carries.
- **No appetite linkage.** Metrics shown without thresholds leave directors unable to judge whether a number is good or bad.
- **Snapshot only.** A single-period view hides deterioration and gives no sense of trajectory.
- **Incomplete inventory.** Coverage metrics look healthy because the denominator excludes vendors nobody registered.
- **Stale acceptances.** Risk acceptances that roll over quietly become permanent exceptions that the board never approved.
- **Missing concentration view.** Vendors are reported one by one, so shared fourth parties beneath several critical services stay invisible.

- **Manual compilation.** Numbers rebuilt by hand every quarter drift in definition, cannot be re-performed, and consume analyst time.
- **Late escalation.** Significant vendor incidents surface at the next scheduled meeting instead of within days.

A 90-day plan to upgrade board reporting

The plan below assumes an existing program with an inventory and assessment process, and a board pack that needs to mature.

Days 1 to 30: foundations

1. Review current packs and minutes for the last four periods and list what directors asked that the pack could not answer.
2. Draft or refresh the qualitative third-party risk appetite statement with the CRO.
3. Propose eight to twelve KRIs, each with definition, formula, source, threshold bands and owner.
4. Reconcile the vendor inventory to accounts payable and contracts, and fix the denominator.
5. Confirm the critical vendor list and the services each supports.

Days 31 to 60: build

1. Back-populate at least four periods of history for each KRI where data allows, and note gaps.
2. Build the concentration view: shared providers and fourth parties across critical services.
3. Consolidate the risk acceptance register with expiry dates and owners.
4. Write escalation triggers and notification paths into the policy, aligned with incident reporting.
5. Draft the new pack using the outline above and dry-run it with the CRO and risk committee chair.

Days 61 to 90: embed

1. Seek risk committee approval of the tolerances and board approval of the appetite statement.
2. Issue the first pack in the new format with an explanation of changes.
3. Introduce an action log and agree minute-taking expectations with the company secretary.
4. Document data lineage for each KRI and invite internal audit to review the design.
5. Automate extraction and scheduling where possible to remove manual compilation.

How VendRisk360 supports this

VendRisk360 is built so that board reporting falls out of the program's system of record rather than being rebuilt by hand each quarter. Assessments, findings, risk acceptances, monitoring alerts and nth-party relationships live in one place, so the numbers in a board pack trace back to the underlying records.

Nine board and executive decks. The platform generates the Monthly VRM Board Report, Vendor KPI and Performance Review, Executive Risk Briefing, Audit Committee / Examiner Readiness, Vendor Approval Pipeline, Vendor Incident / Breach Briefing, Concentration Risk Briefing, Annual TPRM Program Review, and Regulator / Examiner Meeting decks. These map directly to the audiences and cadence described above: the board and risk committee, the audit committee, the executive committee, out-of-cycle incident briefings and the annual program review. Each deck is produced as a PDF and as editable PowerPoint, so management can add commentary and decisions requested before issue.

Scheduling. Decks can be scheduled so that recurring packs are produced on a consistent cycle with consistent definitions, which supports trend reporting and reduces manual compilation.

Executive dashboards. Dashboards give executives a current view of criticality tiers, assessment status, overdue findings, risk acceptances and monitoring signals between formal meetings.

Concentration and incidents. Nth-party intelligence maps fourth-party and nth-party relationships across vendors to show concentration, systemic risk and blast radius. Outside-in continuous monitoring surfaces confirmed-only alerts for attack surface, shadow infrastructure, indicators of compromise, breaches and security incidents, adverse news and litigation, regulatory and enforcement actions and sanctions, routed to the vendor owner and available for escalation.

Evidence for examiners and auditors. Findings, remediation plans, formal risk acceptances and multi-stage sign-offs with segregation of duties are recorded with a full audit trail, and Excel exports of registers and findings support reconciliation and KRI re-performance. The examiner package export assembles assessments, evidence, sign-offs and the audit trail for supervisors and internal audit.

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.

See board and executive reporting and 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.