VendRisk360
ASSESS · MONITOR · STAY AHEAD

WHITEPAPER

# Beyond the Fourth Party: Mapping Concentration, Systemic Risk and the Real Blast Radius

A practitioner and auditor guide to discovering nth-party dependencies, measuring concentration and testing what really fails when a shared provider goes down.

**Published** 25 September 2026

**Written for** Heads of TPRM, CROs, CISOs, operational resilience leads, internal audit and compliance officers

**Online** www.vendrisk360.com/resources/whitepapers/beyond-the-fourth-party/

# Contents



How to discover fourth and nth parties, build a dependency graph, measure concentration, run blast radius and severe-but-plausible scenarios, track CUECs from SOC reports and meet DORA, PRA, CPS 230, RBI, OSFI and US expectations.

Most third-party risk programs are built around a list: the vendors you pay, each with a contract, an owner, a tier and an assessment date. That list is necessary, but it describes the edges of your organization, not the shape of your dependencies. Your payment processor runs on a cloud provider. Your core banking vendor uses a managed database service, a content delivery network and an offshore support subcontractor. Your claims platform, your CRM and your fraud engine may all resolve to the same hyperscale region. When that region fails, the incident will not respect your tiering spreadsheet.

Regulators have noticed. DORA, the PRA and FCA operational resilience framework, APRA CPS 230, OSFI Guideline B-10, the RBI Master Direction on IT outsourcing and the US interagency guidance all ask firms to look past the direct vendor to the subcontractors that support critical services, and to understand where risk concentrates. This paper sets out a practical, auditable method for doing that: discovering nth parties, modeling them as a graph, measuring concentration, and running blast radius scenarios that connect a single provider failure to the critical operations and impact tolerances your board has approved.

**KEY TAKEAWAYS**

- A direct-vendor inventory cannot show concentration. You need a relationship graph that includes subcontractors, subservice organizations and shared infrastructure.
- Discovery sources vary widely in reliability. Rate every nth-party record by source and confirm critical paths through contracts and SOC reports, not inference alone.
- Concentration has several dimensions: single-provider dependence, substitutability, share of critical services, geography and jurisdiction, and overlap across vendors. Measure each separately.
- Blast radius analysis turns a dependency map into a decision: pick a node, trace dependents, map to critical operations, and compare estimated impact with tolerance.
- CUECs in SOC reports are controls you own. Track them in your control library and test them like any other control.
- Boards need concentration reported as a small set of stable metrics with thresholds, trends and named actions, not a network diagram.

## Why direct-vendor views miss risk

A traditional vendor inventory answers "who do we contract with?" It does not answer "what do we depend on?" The gap matters for three reasons.

First, **hidden shared dependencies**. Ten vendors that appear independent in your register may rely on the same cloud region, identity provider, payment rail or offshore service center. Each looks moderate on its own; together they represent a single point of failure.

Second, **risk transfer without visibility**. When a vendor subcontracts a function that supports your critical service, the control environment you assessed may no longer be the one that operates. A SOC 2 report that carves out the hosting provider says nothing about the hosting provider's controls. Your due diligence is only as deep as the vendor's own oversight of its supply chain.

Third, **correlated failure**. Third-party incidents often cascade: an outage at a shared provider degrades multiple vendors at once, which overwhelms your incident response, your manual workarounds and your communications capacity simultaneously. Business continuity plans written per vendor assume one failure at a time. Concentration analysis tests whether that assumption holds.

## Definitions that matter

Terms are used loosely across frameworks. Agreeing on definitions in policy avoids inconsistent registers and confused reporting.

CORE TERMS FOR NTH-PARTY RISK

| Term | Working definition | Where you see it |
|---|---|---|
| **Fourth party** | A provider to your third party, used in delivering the service you receive | Common TPRM usage; APRA CPS 230 refers to fourth parties relied on by material service providers |
| **Nth party** | Any provider further down the chain (fifth, sixth and beyond) | TPRM practice, supply chain risk (NIST SP 800-161r1) |
| **Subcontractor** | A party engaged by your vendor to perform part of the contracted service | US interagency guidance, OSFI B-10, DORA |
| **Sub-outsourcing** | Onward outsourcing of an outsourced function, or part of it | EBA outsourcing guidelines, PRA SS2/21 |
| **Subprocessor** | A processor engaged by a processor to process personal data | GDPR Article 28, many DPAs |
| **Subservice organization** | A service organization used by the service organization whose controls are relevant to user entities | SOC 1 and SOC 2 reports |

The distinctions matter: a subprocessor list omits providers that never touch personal data, and a SOC report names only subservice organizations relevant to its scope. No single source gives the full picture.

## Sources for discovering nth parties

Discovery is an evidence exercise. Each source has a characteristic blind spot, and your register should record which source produced each relationship and how reliable it is.

NTH-PARTY DISCOVERY SOURCES AND RELIABILITY

| Source | What it reveals | Reliability |
|---|---|---|
| **SOC report system description and subservice organizations section** | Named subservice organizations, services provided, carve-out or inclusive method, CSOCs | High for in-scope services; silent on out-of-scope providers |
| **Subprocessor lists and DPAs** | Providers processing personal data, locations, purpose | High for personal data; incomplete for resilience |
| **Contracts and sub-outsourcing notifications** | Approved subcontractors, notification and objection rights, changes over time | High where flow-down clauses exist and are enforced |
| **Due diligence questionnaires (SIG, CAIQ, custom)** | Self-declared critical suppliers, hosting, support locations | Medium; depends on vendor diligence and question design |
| **Public sources (filings, status pages, trust centers, press)** | Hosting providers, partnerships, acquisitions, outages | Medium; often current, rarely complete |
| **DNS, hosting and technology fingerprinting** | Cloud, CDN, email, DNS and certificate providers from internet-facing assets | Medium to low; shows public infrastructure, not back-office dependencies |

Two practical rules follow. First, do not treat inferred relationships (fingerprinting, press) as confirmed until a contractual or attested source supports them, particularly for critical services. Second, record a confidence level on each edge so that reporting can distinguish "confirmed dependency" from "probable dependency". Concentration metrics built on unconfirmed edges should be labeled as such.

## Building a relationship graph

A spreadsheet of vendors with a "fourth parties" column cannot answer questions like "which critical operations depend on this provider, through any path?" A graph can. The model does not need to be elaborate, but it does need to be consistent.

MINIMUM DATA MODEL FOR AN NTH-PARTY RELATIONSHIP GRAPH

| Element | Key attributes | Why it matters |
|---|---|---|
| **Node: your organization and business units** | Critical operations or important business services, impact tolerances | Anchors every path to something the board cares about |

| Element | Key attributes | Why it matters |
|---|---|---|
| **Node: third, fourth and nth parties** | Legal entity, parent group, country, regulatory status, designated critical provider status | Deduplication by parent group reveals true concentration |
| **Node: service or asset** | Service type (hosting, payments, identity, support), region, data center | Distinguishes one provider's distinct services and regions |
| **Edge: depends on** | Service provided, data types accessed, criticality, substitutability, source and confidence, last verified date | Enables path tracing, filtering and quality reporting |

Several design choices determine whether the graph is useful:

- **Resolve entities to parent groups.** Two subsidiaries of the same cloud provider are one concentration point for most failure modes, although distinct regions may be separate for others. Keep both levels.
- **Model services, not only companies.** "Provider X" is less useful than "Provider X, managed database, region A". Many resilience events are regional or service specific.
- **Share nodes across vendors.** When three vendors name the same subservice organization, they must point to one node, not three text strings. This is what makes overlap counting possible.
- **Carry the edge attributes.** Data types and criticality on each edge let you ask different questions: a confidentiality question (which providers can see customer account data?) and an availability question (which providers can stop payment processing?) follow different paths.
- **Date every edge.** Dependencies change. An edge last verified two years ago should be flagged in reporting.

## Measuring concentration risk

Concentration is not a single number. Regulators describe it in two ways: dependence on a provider that is not easily substitutable, and multiple arrangements with the same or closely connected providers. Measure the dimensions separately and then combine them in judgment, not in a single opaque score.

CONCENTRATION MEASURES AND METHODOLOGY

| Measure | How to calculate | Interpretation |
|---|---|---|
| **Single-provider dependence** | Count of critical operations with a path to each provider (direct or indirect) | Providers reaching several critical operations are candidates for scenario testing |

| Measure | How to calculate | Interpretation |
|---|---|---|
| **Substitutability** | Rated per edge: easily replaceable, replaceable with effort, not practicably replaceable, with an estimated switch time | Low substitutability plus high dependence is the core concentration concern |
| **Share of critical services** | Critical services supported by a provider divided by all critical services | Expressed as a percentage; trend it quarterly |
| **Geographic and jurisdictional concentration** | Share of critical services delivered from each country or region, and share subject to each legal regime | Captures regional outage, sanctions, data localization and legal access risk |
| **Overlap across vendors** | Number of distinct direct vendors that depend on the same nth party | Reveals hidden shared dependencies invisible in the direct register |
| **HHI-style index** | Sum of squared shares of critical services by provider group | Summarizes how evenly dependency is spread |

## A simple HHI-style index

The Herfindahl-Hirschman Index is a general concentration measure: sum the squares of each participant's share. Applied to vendor dependency, calculate each provider group's share of your critical services (using a consistent unit, such as number of critical services or weighted service value), square each share, and add them. With shares expressed as whole percentages, the result ranges from near zero (dependency spread across many providers) to 10,000 (every critical service depends on one provider).

Use it as a trend indicator for a defined category, such as cloud hosting or payment processing, rather than as an absolute rating. Thresholds are yours to set and justify in your risk appetite. Two cautions: an index computed from direct vendors alone will understate concentration if those vendors share an nth party, so compute it on the resolved graph; and it ignores substitutability, so always pair it with that measure.

### HYPOTHETICAL EXAMPLE: HHI-STYLE INDEX FOR CLOUD HOSTING

A mid-sized bank has 20 critical services. Resolving the graph shows 12 depend on provider group A, 5 on group B and 3 on group C. Shares are 60, 25 and 15. The index is 3,600 plus 625 plus 225, which equals 4,450. The direct register showed 14 different hosting arrangements and suggested diversity; the resolved view shows heavy reliance on one group. The bank sets an appetite threshold for this category, reports the index quarterly, and runs a blast radius scenario on group A.

### Systemic risk and correlated failure

Concentration in your own portfolio is one lens. Systemic concentration, where many firms in a sector depend on the same few providers, is another. It explains why regulators have created direct oversight of critical providers: under DORA the European Supervisory Authorities designate critical ICT third-party service providers (CTPPs) and a Lead Overseer supervises them, and in the UK HM Treasury can designate critical third parties under the Financial Services and Markets Act 2023, with PRA and FCA rules applying from 1 January 2025.

Direct oversight of a provider does not reduce your obligations, and supervisors will ask how you considered a provider's systemic importance in your own resilience planning.

Correlated failure modes worth modeling include:

- **Shared infrastructure outage**: cloud region, DNS, CDN, identity provider.
- **Shared software supply chain**: a compromised or defective update in a widely used component or security agent.
- **Shared service center**: a regional event affecting an offshore operations hub used by several vendors.
- **Shared legal exposure**: sanctions, data localization changes or legal access requests affecting all providers in one jurisdiction.
- **Market-wide stress**: a financial failure at a provider group, or a rapid consolidation that removes substitutes.

The practical question for each mode is not probability alone but whether your response capacity (people, manual workarounds, communications, alternate providers) can cope with several vendors failing at once.

## Blast radius analysis

Blast radius analysis asks: if this node fails or is compromised, what stops, what leaks, and for how long? It is the bridge between a dependency map and the impact tolerances you set under operational resilience rules.

### The scenario method

1. **Pick a node.** Start with providers that score highest on dependence and lowest on substitutability, then any node that appears in several vendors' supply chains.
2. **Define the failure.** Availability loss (full or regional), integrity failure (corrupted data or a malicious update) or confidentiality breach. Each follows different edges.
3. **Trace dependents.** Walk the graph upward from the node to every vendor and service with a path to it, noting edge confidence.

4. **Map to critical operations.** For each affected service, identify the critical operation or important business service it supports, and the customers or processes behind it.
5. **Estimate impact against tolerance.** Using recovery objectives, workaround capacity and substitution time, estimate time to restore each operation and compare with its tolerance. Include data exposure where the failure is a breach.
6. **Identify gaps and actions.** Where estimated impact exceeds tolerance, record a finding with an owner: an alternate provider, a manual workaround, contract changes or a risk acceptance at the right level.

**HYPOTHETICAL EXAMPLE: BLAST RADIUS FOR A REGIONAL CLOUD OUTAGE**

A payments firm selects a managed database service in one cloud region used by three vendors: its card processing platform, its fraud scoring service and its customer notification provider. Tracing the graph shows card authorization (tolerance 2 hours), fraud screening (tolerance 4 hours) and customer alerts (tolerance 24 hours) are affected. The processing vendor fails over to a second region in about 1 hour. The fraud vendor has no multi-region design; its estimated restore time is 8 hours, and without fraud scoring the firm's policy is to decline high-value transactions, which degrades card authorization as well. The analysis produces two findings: the fraud dependency breaches tolerance, and the fallback rule creates a second-order impact on card authorization. Actions include a contractual resilience commitment, a rules-based fallback scoring mode and a quarterly failover test with evidence.

## Scenario analysis and severe-but-plausible testing

UK operational resilience rules, APRA CPS 230 and DORA all expect testing against severe but plausible scenarios. Concentration and blast radius analysis supply the scenarios; testing supplies the evidence.

Good scenario libraries include at least one of each: a shared provider outage, a supply chain compromise affecting multiple vendors, the insolvency or sudden exit of a provider with low substitutability, and a jurisdictional event affecting a concentration of services. For each, document the assumptions (duration, scope, what still works), the data used, the participants, results against tolerance and actions.

**TESTING APPROACH FOR CONCENTRATION SCENARIOS**

| Test type | What it demonstrates | Evidence to retain |
|---|---|---|
| **Tabletop exercise** | Decision making, communications, escalation across multiple vendor failures | Scenario pack, attendance, decisions log, actions |
| **Technical failover test** | Vendor or internal ability to switch region or provider | Vendor test report or joint test results, timings versus objectives |

| Test type | What it demonstrates | Evidence to retain |
|---|---|---|
| **Exit or substitution rehearsal** | Feasibility of the exit plan within the assumed time | Walkthrough of plan, data export test, alternate provider readiness |
| **Reverse stress test** | Which combination of failures would breach tolerance | Analysis, board or committee discussion, resulting actions |

### How an auditor tests the process

Internal audit typically tests design by reviewing the methodology (sources, confidence ratings, measures, thresholds) and walking through one critical operation end to end: from the register entry, through the graph, to a completed scenario and resulting actions. Operating effectiveness testing samples critical vendors and checks that nth-party data was refreshed on the stated cadence, that subcontractor change notifications were logged and assessed, that scenarios were run as scheduled, and that findings were tracked to closure. A common exception is a graph that was built once for a regulatory submission and never updated.

**WHAT EXAMINERS AND AUDITORS ASK**

- Show us your register and how it identifies subcontractors supporting critical or important functions.
- How do you identify providers that several of your vendors rely on? Show a current example.
- What concentration measures do you use, what thresholds apply, and who approved them?
- Walk us through a scenario test involving a shared provider, including results against impact tolerance.
- How are subcontractor change notifications received, assessed and escalated?
- How are CUECs from SOC reports assigned, implemented and tested?
- What did the board receive on concentration risk in the last year, and what did it decide?

## Regulatory expectations across jurisdictions

Expectations converge on four themes: know the chain for critical services, control changes to it, assess concentration, and plan for exit. Confirm the obligations that apply to your entity with counsel or your regulator, and check the current texts, since several of these frameworks are supplemented by technical standards and guidance that continue to evolve.

REGULATORY EXPECTATIONS FOR SUBCONTRACTING AND CONCENTRATION

| Instrument | Nth-party and subcontracting | Concentration |
|---|---|---|
| **DORA, Regulation (EU) 2022/2554 (from 17 January 2025)** | Register of information on ICT contractual arrangements, with technical standards covering the supply chain for services supporting critical or important functions; technical standards on subcontracting | Article 29 preliminary assessment of ICT concentration risk before contracting; CTPP oversight framework |
| **EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)** | Conditions for sub-outsourcing of critical or important functions, notification, flow-down | Consider concentration in risk assessment and exit planning |
| **PRA SS2/21; UK critical third parties regime** | Sub-outsourcing controls for material outsourcing; register | Concentration assessment at firm level; direct oversight of designated CTPs |
| **APRA CPS 230 (from 1 July 2025)** | Manage risks from fourth parties that material service providers rely on | Material service provider register; concentration considered in managing arrangements |
| **RBI Master Direction on Outsourcing of IT Services (2023)** | Sub-contracting controls, audit and access rights | Explicit expectation to assess and manage concentration risk |
| **OSFI Guideline B-10 (effective May 1, 2024)** | Subcontracting risk management, including notification | Monitor concentration at the individual provider and portfolio level |
| **US Interagency Guidance (June 2023)** | Subcontractor due diligence and contractual provisions | Consider concentration of third-party relationships |
| **MAS Guidelines on Outsourcing** | Sub-contracting controls for material arrangements | Consider concentration risk across arrangements |

Several details matter operationally. DORA's register uses standardized templates set out in implementing technical standards, and supervisors have collected registers from in-scope entities, so data quality issues become visible to supervisors quickly. Article 29 requires a preliminary assessment of concentration risk before entering an arrangement for critical or important functions, which means concentration data must be available at intake, not only in annual reporting. CPS 230 extends the view explicitly to fourth parties of material service providers. Regulators in the Middle East, the Philippines and New Zealand address subcontracting within their outsourcing rules, and the direction of travel is consistent.

# SOC reports in depth

SOC reports are the richest attested source of nth-party information and the most commonly under-used. Reading them properly is a core TPRM and IT audit skill.

## Carve-out and inclusive methods

Under the **inclusive method**, the subservice organization's relevant controls are included in the description and tested by the service auditor. Under the **carve-out method**, the subservice organization's controls are excluded; the description identifies the subservice organization and the services it provides, and states which controls the service organization expects it to have. Most cloud-hosted vendors use the carve-out method for their hosting provider.

A carve-out is not a deficiency, but it transfers work to you. You need assurance on the carved-out provider, usually by obtaining its own SOC report and checking that its scope, period and results cover the services your vendor uses.

## CSOCs and CUECs

**Complementary subservice organization controls (CSOCs)** are the controls the service organization assumes the carved-out subservice organization operates. Check that the subservice organization's own report covers them. If it does not, the assurance chain has a gap.

**Complementary user entity controls (CUECs)** are controls the service organization assumes you, the user entity, operate. Typical examples: reviewing user access to the vendor application, protecting credentials and API keys, reconciling transaction outputs, notifying the vendor of terminated users, and reviewing reports the vendor provides. If you do not operate them, the control objectives in the report may not be achieved for your organization, regardless of the auditor's opinion.

## Tracking CUECs as your own controls

Treat CUECs as entries in your control library, not as notes on a vendor file.

- [ ] Extract every CUEC from each in-scope SOC report on receipt.
- [ ] Map each CUEC to an existing internal control, or create a new one.
- [ ] Assign a control owner in the business or IT function that uses the service.
- [ ] Record evidence expectations and frequency.
- [ ] Re-extract on each new report and flag new, changed or removed CUECs.
- [ ] Report unmapped or unowned CUECs as open findings.

### Testing CUECs as an auditor

An auditor tests CUECs like any key control. For design, confirm that the mapped internal control actually addresses the CUEC as written (a generic access review may not cover the vendor application's privileged roles). For operating effectiveness, select a sample across the period, commonly scaled to control frequency (for example, a few instances for a quarterly control, more for a monthly or daily control), and inspect evidence: access review sign-offs, reconciliations, termination notifications. A walkthrough typically follows one instance end to end, from the trigger to the evidence retained. Exceptions should be evaluated for their effect on reliance on the vendor's report.

Also check the report period, the opinion, exceptions noted and management responses, and obtain a bridge letter where the report period does not reach your assessment date.

## Contract levers

Contracts are where discovery becomes control. For critical services, negotiate the following, and flow them down to subcontractors that support those services.

CONTRACT LEVERS FOR NTH-PARTY RISK

| Lever | What to seek | Purpose |
|---|---|---|
| **Flow-down** | Equivalent security, confidentiality, resilience and audit obligations imposed on subcontractors | Keeps your control expectations intact down the chain |
| **Notification and approval** | Advance notice of new or changed material subcontractors, with a right to object or terminate | Lets you assess before a change takes effect |
| **Transparency** | Maintained list of material subcontractors, locations and services | Supports register accuracy and concentration measurement |
| **Audit and access rights** | Rights for you and your regulators, extending to relevant subcontractors or satisfied by their assurance reports | Meets supervisory expectations and supports testing |
| **Resilience commitments** | Recovery objectives, multi-region design, participation in your testing | Aligns vendor capability with your tolerances |
| **Exit and transition** | Data return in usable formats, transition assistance, reasonable notice periods | Makes substitution feasible within assumed timelines |

Where a large provider will not negotiate, document the gap, the compensating measures (such as reliance on its assurance reports and your own architecture choices) and the risk acceptance at the appropriate authority level.

## Governance and board reporting

Boards are accountable for third-party risk under every framework discussed here, and concentration is one of the few topics where only the board can make the trade-off between efficiency and resilience. Reporting should enable that decision.

A useful concentration report is short and stable from quarter to quarter:

- Top providers by number of critical operations supported, directly and indirectly, with substitutability.
- HHI-style index for key categories (hosting, payments, core processing), with trend and threshold.
- Geographic and jurisdictional distribution of critical services.
- Overlap: nth parties shared by several direct vendors.
- Scenario results since the last report, with any tolerance breaches and actions.
- Data quality: share of critical edges confirmed by contract or SOC report, and edges past their verification date.
- Decisions requested: risk acceptances, investment in alternates, changes to appetite thresholds.

Assign clear ownership: TPRM maintains the graph and measures, operational resilience owns critical operations and tolerances, the business owns substitution plans, and internal audit provides independent assurance.

## Practical checklist

- [ ] Define fourth party, nth party, subcontractor, subprocessor and subservice organization in policy.
- [ ] Record the source and confidence level for every nth-party relationship.
- [ ] Extract subservice organizations, CSOCs and CUECs from every in-scope SOC report.
- [ ] Resolve providers to parent groups and model services and regions as distinct nodes.
- [ ] Link every critical operation or important business service to its full dependency paths.
- [ ] Measure single-provider dependence, substitutability, share of critical services, geography, overlap and an HHI-style index.
- [ ] Set and approve concentration thresholds within risk appetite.
- [ ] Perform a preliminary concentration assessment at intake for critical arrangements.
- [ ] Run blast radius scenarios on the top concentration nodes at least annually.
- [ ] Include multi-vendor failure in severe-but-plausible testing.

- [ ] Map every CUEC to an owned internal control and test it.
- [ ] Negotiate flow-down, notification, audit, resilience and exit terms for critical services.
- [ ] Log and assess every subcontractor change notification.
- [ ] Report concentration metrics, scenario results and data quality to the board.
- [ ] Have internal audit review methodology and sample operating effectiveness.

## How VendRisk360 supports this

VendRisk360 is a third-party risk management platform designed to put these practices into daily operation for regulated organizations.

**Nth-party intelligence.** The platform maps fourth-party and nth-party relationships, and those relationships are shared across vendors, so a provider that three vendors depend on appears as one node. This supports overlap counting and a resolved view of dependency. See nth-party intelligence.

**Concentration, systemic risk and blast radius.** Concentration and systemic risk views highlight providers that support many vendors and services, and blast radius analysis traces the vendors and services affected when a node fails, helping teams choose which scenarios to test.

**SOC review and CUEC tracking.** SOC 1 and SOC 2 review covers exceptions, carve-outs, subservice organizations and CUECs. CUEC tracking keeps the controls you owe as a user entity visible and assigned, rather than buried in a report appendix. Your analysts perform the review on the platform, or VendRisk360 assessors perform it through Comprehensive Vendor Risk Assessment Services or a standalone SOC Report Review (with optional AI assistance); either way a named reviewer signs off and each decision is recorded in the audit trail.

**Findings and lifecycle.** Gaps from scenarios and SOC reviews become findings with remediation plans or formal risk acceptance, with multi-stage sign-off and segregation of duties. Criticality tiers drive assessment depth and a policy-configured reassessment cadence across the vendor lifecycle, and outside-in continuous monitoring covers attack surface, shadow infrastructure, indicators of compromise, breaches, adverse news, regulatory actions and sanctions between point-in-time reviews.

**Board reporting.** The Concentration Risk Briefing is one of nine board and executive decks, available as PDF and editable PowerPoint and schedulable, alongside executive dashboards, Excel exports of registers and findings, and an examiner package export with assessments, evidence, sign-offs and audit trail. See board and executive reporting.

**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.

To see how a dependency map, a blast radius scenario and a concentration briefing come together, 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.