SCHNEIDER DOWNS

Big Thinking. Personal Focus.

The Third-Party Risk Management Concentration Risk Playbook

Concentration Risk and DORA

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

The Third-Party Risk Management Concentration Risk Playbook

Concentration Risk and DORA

Ever struggle to concentrate on mundane tasks after a long day sifting through 100+ emails? Now scale that to the daily oversight of a vendor portfolio of 1,000+. Overwhelming? Absolutely.

For third-party risk management (TPRM) practitioners, it often feels like a constant game of cat and mouse. Managing concentration risk helps slow that cycle and allows programs to focus on what matters most. TPRM safeguards operations, data, and reputation whenever organizations depend on external vendors.

Concentration risk crops up when too much dependence accumulates around a single provider, location, or service line. This turns routine incidents into enterprise problems. As organizations lean harder on cloud, software, and specialized services, concentration risk now touches operational, compliance, reputational, and cybersecurity exposure across organizations of all sizes.

This guide reviews the three primary types of concentration risk: vendor, geographic, and service. It also examines how the Digital Operational Resilience Act (DORA) requires firms to identify, assess, and mitigate each. By connecting core TPRM practices with evolving regulations, organizations can better understand dependencies and strengthen resilience.

The Three Faces of Concentration Risk and Real-World Examples

1) **Vendor Concentration:** Over-reliance on one provider increases single-point-of-failure risk.

- One cloud for everything (AWS *or* Azure *or* GCP)
- One law firm for all jurisdictions
- One supplier for a critical component (e.g., lithium for EV batteries)

2) **Geographic Concentration:** Vendors and operations clustered in one region magnify exposure to natural disasters, conflict, or political shifts.

- All customer support in the Philippines (typhoons, unrest)
- Data centers concentrated in a single corridor (e.g., Northern Virginia; flood/fire risk elsewhere)
- IT services centralized in one geopolitical hotspot

3) Service Concentration: Multiple critical functions sourced from the same provider create "blast radius" risk.

- One vendor for both payroll and benefits
- A single partner managing cybersecurity, compliance, and privacy
- One logistics firm for warehousing, shipping, and returns

How to Quickly Spot It Fast

- Heatmap your vendors by criticality × data sensitivity × substitutability
- Stack-rank exposure: % of spend, % of transactions, or % of critical processes tied to one vendor/region/service
- Map fourth parties (where practical) to see hidden clusters

How to Reduce It... Without Inflating Costs

- Segment and diversify: a primary + secondary model for crown-jewel services
- Contract for resilience: exit rights, data portability, RTO/RPO targets, tested failover
- Architect for portability: multi-AZ/region designs; avoid hard platform lock-in; standardize interfaces
- Stagger dependencies: separate hosting from security monitoring, payroll from benefits, warehousing from shipping
- Run scenarios: "If Vendor X is down for 72 hours, what breaks? What's plan B?"
- Measure & report: set thresholds (e.g., "no single vendor >40% of critical process X") and track exceptions

The Payoff

Treating concentration risk as a design constraint, not an afterthought, yields a vendor ecosystem that's diverse, flexible, and audit ready. It won't eliminate incidents, but it keeps local problems from becoming enterprise crises, and it gives you leverage at the negotiating table.

5 Ways DORA Targets Concentration Risk

Digital Operational Resilience Act (DORA), strengthens TPRM by targeting five key ways to identify, assess, and reduce concentration risk.

In the previous section, we explored the three core types of concentration risk Third Party Risk Management (TPRM) programs must manage: vendor, geographic, and service. Building on that, let's look at how DORA, the EU regulation for financial entities, pushes firms to identify, assess, and reduce each of those risks.

Who Does DORA Apply To?

DORA applies to EU financial entities (and certain ICT providers that support them). It requires a register of critical third parties, limits over-reliance on a small number of providers, and elevates expectations for contracts, monitoring, and exit.

Definitions

- **ICT = Information and Communications Technology:** the systems and services (often third-party) that underpin your digital operations.
- **CTPP = Critical ICT Third-Party Provider:** an ICT vendor designated by European Supervisory Authorities (ESAs) for direct oversight due to systemic importance.

1) Enhanced Due Diligence & Risk Assessment: DORA raises the bar on what "good" due diligence looks like.

- Evaluate criticality of the ICT service and the single-point-of-failure risk (including fourth-/nth-party chains)
- Consider replaceability and realistic alternatives
- Factor in third-country and subcontracting exposures into the risk rating
- Align findings with your digital resilience strategy (not just a one-off checkbox)

What to update: Due Diligence Questionnaire (DDQ) content, risk-tiering logic, and inherent risk models to explicitly score concentration, substitutability, and chain risk.

2) Stronger ICT Contract Requirements: DORA expects contracts with ICT providers to be explicit and enforceable.

- Clear service scope, security obligations, and performance targets
- Incident reporting timelines and defined Recovery Time Objective/Recovery Point Objective (RTO/RPO)
- Audit, testing, and access rights (including pen testing where proportionate)
- Data location/processing terms and portability assurances
- Termination & exit clauses that work in practice (e.g., material breach, chronic under-performance)

Why this matters for concentration: When you're heavily reliant on a single provider, operable termination and exit rights are the safety valve that lets you move without chaos.

3) Ongoing Monitoring & Vendor Diversification: DORA leans into a multi-vendor mindset where feasible.

- Monitor performance, incidents, resilience metrics, and subcontractors—not just once a year
- Identify concentrations (by provider, region, service) and set thresholds that trigger remediation or diversification
- Use portfolio-level dashboards to show where risk clusters are forming

What to add: Portfolio heatmaps, trigger thresholds (e.g., "no single vendor >40% of X"), and remediation playbooks.

4) Oversight Framework for Critical ICT Third-Party Providers (CTPPs): DORA creates a regulatory oversight lane for ICT providers designated as "critical" by the European Supervisory Authorities (ESAs).

- ESAs can designate providers critical based on systemic impact and substitutability
- CTPPs face direct oversight, inspections, resilience testing, and corrective actions
- Lead Overseers can issue recommendations; non-compliance can lead to penalties and force financial entities to suspend or exit services

Practical takeaway: Monitor which of your vendors are or may become CTPPs—their status signals heightened scrutiny and elevated expectations for your program.

5) Exit Strategy & Termination Testing: DORA treats exit as a designed capability, not an afterthought.

- Maintain tested exit plans (data portability, transition support, knowledge transfer)
- Validate time-to-cutover, licensing contingencies, and access during wind-down
- Test exits periodically—beyond normal BCP/DR—to prove you can detach from a concentration in practice

What to test: Cloud/provider failover drills, escrow/portability of data and configs, role-based access during transition, and communications plans.

Putting It Into Practice

- Register: Maintain an up-to-date critical third-party register with concentration indicators.
- Score: Add concentration, substitutability, and chain risk to inherent/overall risk scoring.
- Contract: Standardize DORA-ready clauses (audit, RTO/RPO, reporting, data location, termination/exit).
- Monitor: Build portfolio heatmaps with thresholds that trigger diversification or remediation.
- Exit: Test your exit and cutover scenarios—treat them like fire drills.

The Bottom Line

DORA doesn't just ask you to document concentration risk, it expects you to design around it. If you operationalize these five areas, you'll reduce single-point-of-failure exposure, improve negotiating leverage, and be ready when regulators (or your board) ask the only question that matters: If this provider fails, can we carry on?

DORA's Approach to Exit Strategy and Termination

Lastly, we focus on how DORA addresses concentration risk during the exit strategy and termination process, ensuring organizations can move away from over-reliance on a single ICT or cloud provider without compromising operational resilience.

Although DORA is a very important regulation that includes new requirements for managing concentration risk, another unique framework exists in the area of financial organization governance known as Basel.

The Basel Framework is a set of international banking regulations that must be followed by banks that are members of the Basel Committee on Banking Supervision (BCBS). The BCBS is the primary global standard setter for the prudential regulation of banks. Member jurisdictions have agreed to fully implement these standards and apply them to internationally active banks in their regions. This alignment ensures that banks adhere to necessary regulatory adjustments and transitional arrangements, maintaining the stability and integrity of the global financial system.

Although the Basel Framework is not targeted at third-party risk specifically, all of the requirements below incorporate elements related to identifying concentration risk areas:

1. Pillar 2 Supervisory Review and Evaluation Process (SREP)

- Bank Responsibilities: Banks are expected to identify, measure, monitor, and manage all material risks, including concentration risk, under their internal capital adequacy assessment process (ICAAP).
- Supervisory Review: Under Pillar 2, supervisors review and evaluate a bank's ICAAP to ensure it appropriately assesses concentration risk and maintains adequate capital to cover it.
- Concentration Risk in Pillar 2: This includes evaluating the potential impact of credit exposures to single counterparties or groups of connected counterparties, geographical locations, industry sectors, specific products, or service providers, according to the Bank for International Settlements.

Understanding the Large Exposures Framework and Its Role in Managing Concentration Risk

The Large Exposures Framework complements Pillar 1 by limiting a bank's exposures to single or connected counterparties. A large exposure is defined as the sum of all exposures to a single counterparty (or connected group) that is 10% or more of a bank's Tier 1 capital. Generally, exposures to a single counterparty are limited to 25% of Tier 1 capital, with a tighter 15% limit for exposures between global systemically important banks (G-SIBs).

This framework applies to various exposures in both the banking and trading books. For interconnected counterparties that could cause cascading failures, the limit applies to the combined exposures of the group.

In conclusion, concentration risk is no longer a theoretical concern. It is a rapidly evolving and increasingly critical component of Third-Party Risk Management (TPRM). As organizations become more reliant on external vendors for essential services, the potential for operational, compliance, reputational, and cybersecurity disruptions due to over-reliance on a single provider, region, or service type becomes more pronounced.

Preparing Your TPRM Program for the Future of Concentration Risk

Looking ahead, we can expect continued development of regulatory frameworks such as DORA and Basel, along with new tools, controls, and best practices designed to help organizations identify, assess, and mitigate concentration risk more effectively. As this area matures, proactive engagement, diversified vendor strategies, and robust oversight mechanisms will be key to building a resilient and future-ready TPRM program.

If you are overseeing your own TPRM program, the list of questions below can help you begin identifying concentration risk:

1. How many specific vendors does our company leverage for data center / cloud hosting?
2. Have we confirmed the service locations / area of operations for all of our vendors?
    a. Are these information / locations tracked?
3. How many different solutions are used across the organization for meetings, calls, instant messages?
4. Do we have a centralized support team, or is support assistance decentralized?
5. How many different vendors do we use for staffing?
6. Which of our vendors support multiple business units or functions across the organization?
7. How many vendors within our population provide a service/product that is considered a sole provider with no backup options?
8. Are Concentration Risk questions or factors included in our IRQ / Due Diligence process?
9. Have we considered determining quantifiable characteristics for concentration risk by service type, business unit, or risk tier?

By understanding the three types of concentration risk and aligning with DORA requirements, organizations can reduce dependency, strengthen resilience, and build a more sustainable third-party risk management program.

If you have any questions regarding your third-party risk management program or where to get started, contact our team at **contactsd@schneiderdowns.com**.

How Can Schneider Downs Help?

Schneider Downs is a registered assessment firm with the Shared Assessments Group, the clear leader in third-party risk management guidance. Our personnel are experienced in all facets of vendor risk management, and have the credentials necessary (CTPRP, CISA, CISSP, etc.) to achieve meaningful results to help your organization effectively achieve new vendor risk management heights.

For more information visit **www.schneiderdowns.com/tprm**.