Mastering global supplier risk: A procurement checklist

Introduction

Effective supplier risk management doesn't happen overnight—it evolves alongside your business.

As your organisation grows, so does vendor complexity, regulatory pressure, and exposure to risk. This checklist is a three-party strategy designed to help you build, strengthen, and scale your company's supplier risk management over time, ensuring global compliance as your business matures.

Phase 1: Establishing the Foundation

Who this is for

Companies just starting to formalise supplier risk management. Compliance is a concern, but risk management is mostly reactive and manual at this stage.

Key outcome

Basic supplier risk awareness and controls are in place, reducing exposure to major compliance or operational failures.

- [ ] Standardise supplier onboarding with a **single intake process** to collect key details (legal entity, contract owner, purpose of engagement).
- [ ] Conduct **basic sanction screening** during onboarding – perform TIN/VAT checks and require suppliers to disclose financials.
- [ ] Implement **manual risk approvals** for high-risk suppliers (e.g., those handling sensitive data or processing payments).
- [ ] Create a **simple supplier risk repository** (even in a spreadsheet) to log suppliers, risk levels, and key documents.
- [ ] Review **contract renewals** on an ad-hoc basis, ensuring suppliers with known risks are reassessed before extending agreements.
- [ ] Assign **risk owners** – designate someone in Legal, Compliance, or Procurement to oversee supplier risk, even if part-time.

Phase 2: Strengthening Compliance & Automating Risk Workflows

Who this is for

Organisations managing a growing supplier base and facing increasing regulatory requirements. Risk management moves from reactive to structured and proactive at this stage.

Key outcome

Risk management becomes automated and embedded into the entire supplier lifecycle, reducing manual work and improving compliance.

- [ ] Automate **supplier intake workflows** with structured approval flows for IT, Security, Finance, and Compliance teams.
- [ ] Expand **supplier risk screening** – integrate automated checks (OFAC, D&B, ESG, cybersecurity ratings) to flag potential risks in real time.
- [ ] Enforce **risk-based supplier assessments** – classify suppliers into tiers (low/medium/high risk) based on their access to sensitive data, business impact, and regulatory requirements.
- [ ] Define and document **organisational risk appetite** – establish clear, measurable criteria for acceptable supplier risk levels across various categories, integrating these criteria into automated risk assessments and supplier onboarding decisions.
- [ ] Implement **scheduled supplier risk reviews** (quarterly/annually) for critical suppliers to monitor financial stability, security controls, and ongoing compliance.
- [ ] Establish a **contract renewal risk review** – ensure suppliers are reassessed before renewal, especially those with expired certifications or compliance gaps.
- [ ] Implement **risk-based offboarding** to remove suppliers that no longer meet security, financial, or compliance standards.

Phase 3: Scaling with Full Risk Orchestration

Who this is for

Organisations in highly regulated industries or with complex supplier ecosystems. Compliance and risk management are mission-critical, and supplier risk is continuously monitored and optimised.

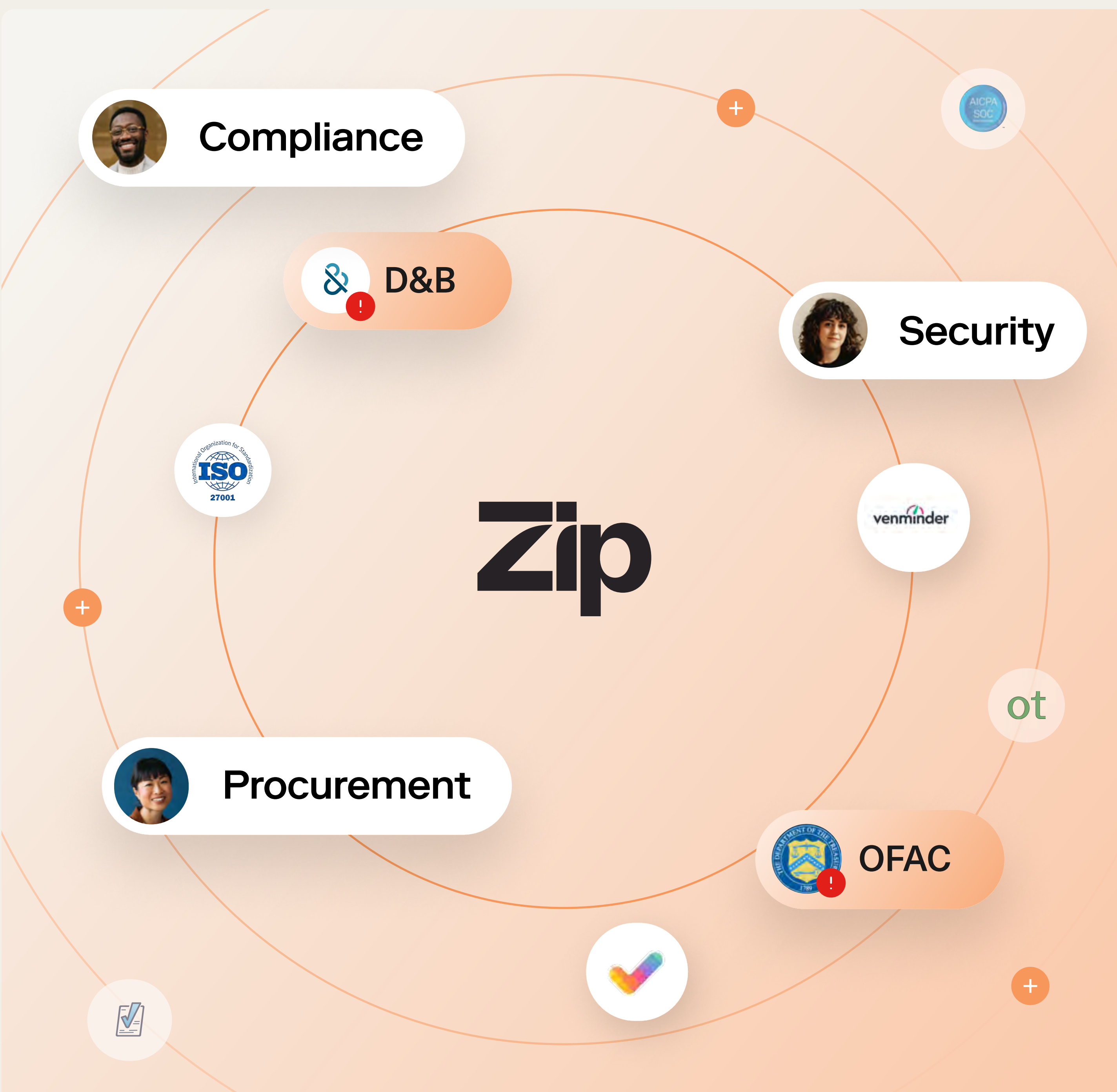
Key outcome

Risk management is fully integrated, automated, and continuously improving, allowing the business to scale while maintaining regulatory confidence.

- [ ] Build advanced **supplier risk reassessments** through AI-driven reviews (e.g., on contracts, supplier onboarding questionnaires).
- [ ] Establish **multi-tiered risk scoring** (supplier-level, service-level) to drive data-driven risk decisions.
- [ ] Implement **automated risk remediation workflows**, assigning corrective actions when a supplier fails a compliance check.
- [ ] Centralise **all supplier risk data in a single system**, ensuring full visibility across Procurement, Legal, Finance, and IT teams.
- [ ] Adopt multiple **specialised risk management tools** to address different regulatory and business needs (e.g., ESG compliance, operational resilience, data privacy).
- [ ] Develop **internal and external supplier scorecards** to evaluate supplier performance.
- [ ] Understand SLAs in the contract and **track supplier performance against SLAs**.
- [ ] Deploy **real-time risk monitoring** for key suppliers, tracking financial health, cybersecurity incidents, and regulatory compliance.
- [ ] Establish a **periodical evidence collection process**, a scheduled system for suppliers to provide evidence of control effectiveness (e.g., audit reports, penetration test results, policy documentation).
- [ ] Formalise **a structured supplier offboarding strategy** that includes compliance, security, and procurement teams to prevent operational disruptions.
- [ ] Create a **cross-functional risk committee** to align risk management strategies across different teams.

Zip for Risk Orchestration

Zip connects all the tools, teams, and data you need to confidently manage supplier risk–with smart automation built in where you need it.



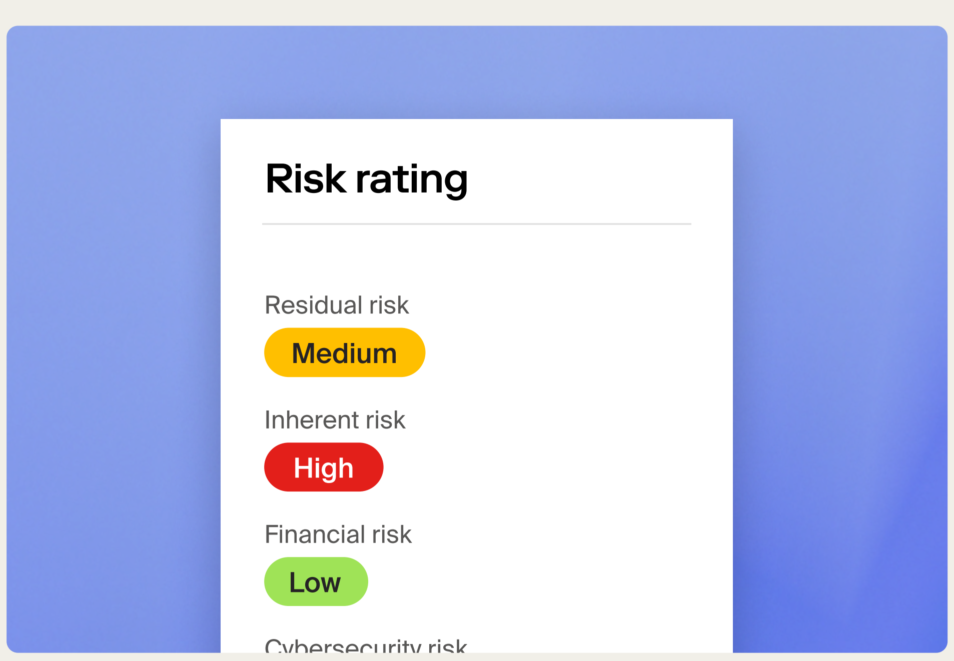
What is risk orchestration?

Risk orchestration is an approach to risk management that emphasises coordination across teams, tools, and data to streamline the entire process. Zip takes the headache out of supplier risk management. From supplier due diligence to risk monitoring and reporting, Zip orchestrates risk across the entire supplier lifecycle—so you can stay compliant without slowing down business.

Why change now?

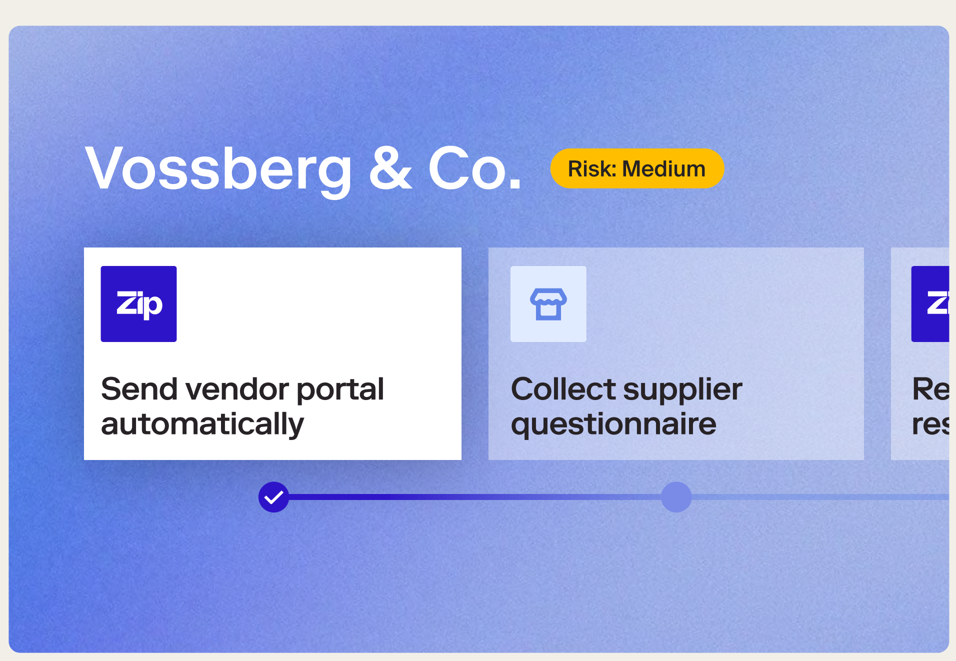
Regulations are evolving faster than ever, with stricter enforcement and higher penalties - sometimes up to 4% of global revenue.

Zip helps you stay ahead of evolving regulations like DORA, German Supply Chain Act, GDPR, ViDA, and the EU AI Act. Zip's configurable platform adapts to new requirements, ensuring you're always audit-ready.



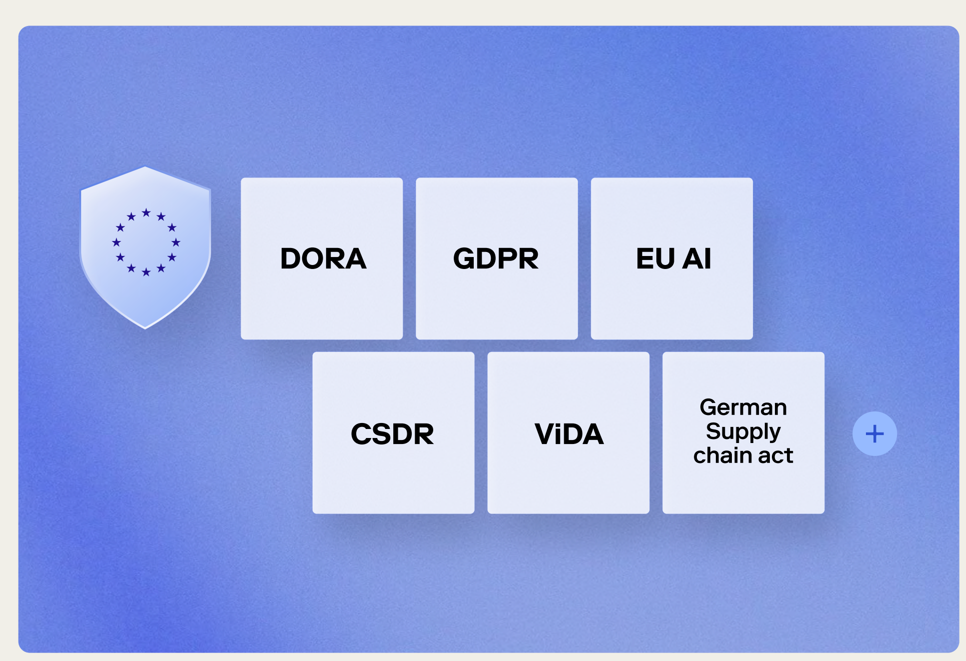
Gain full visibility into supplier risk

Automate risk approvals across Procurement, Legal, Finance, and IT—ensuring supplier risk decisions are consistent, audit-ready, and compliant.



Cut manual work, stay risk-ready

Managing risk doesn't have to be painful. Zip's intuitive, user-friendly platform makes it easy to reduce supplier risk.



Stay compliant in an evolving landscape

Easily adapt to new regulations and expand risk controls across ESG, data privacy, AI, and more—without slowing your business down.

Key features

Supplier due diligence

Assess supplier risk with standardised intake, external data checks, and a rigorous approval process.

Risk scoring & tiering

Automatically score suppliers, assign risk tiers, and flag high-risk suppliers for review.

Automated approval workflows

Route supplier approvals to the right stakeholders based on risk level, spend, and regulatory requirements.

Centralised risk repository

Maintain a single source of truth for supplier risk data, documents, and 3rd party screening history.

Scheduled risk reviews

Automatically trigger periodic supplier reassessments to ensure ongoing compliance.

Supplier audit & reporting

Easily generate audit packages and reports to meet regulatory requirements any time.

METRO BANK

> "Zip for Risk Orchestration represents the kind of intelligent automation that's essential as we balance innovation with security. We're fundamentally strengthening the foundation of trust that underpins everything we do."

James Morris
Senior Credit Officer, Metrobank

Frequently asked questions

How is Zip different from other GRC tools?

Most GRC tools are clunky and siloed—Zip is different. As the leader in risk orchestration, we don't just track risk—we connect teams, processes, and tools to make compliance seamless. Additionally, Zip's highly user-friendly platform leads to high adoption rates, which in turn shrinks compliance gaps.

I already have a TPRM tool—can I still use Zip?

Absolutely. Zip integrates with top risk platforms like Onetrust and Venminder, so you get the best of both worlds—powerful orchestration without disrupting your existing risk checks.

I haven't used any risk management tools—Is Zip the right fit?

Yes! Whether you're just getting started or scaling fast, Zip makes risk management effortless. Begin with supplier onboarding for instant efficiency gains, then seamlessly expand into advanced risk management as your business grows.

Seamlessly orchestrate any procurement request – without risk

Learn more at **ziphq.com**