The Big Picture: Develop a 360-Degree View of Third-Party Business Partners

Scanmarket

A 16-Point Checklist that Supports Your Organization's GRC Objectives

Historically, Governance, Risk Management, and Compliance frameworks have applied only to highly regulated industries like finance or within government and public sector procurement. But today, businesses manage complex and interconnected supply chains, which requires the ability to source, procure, and manage services and materials from all parts of the world.

Oversight has expanded into industries that previously flew under the radar of regulators, who now dole out large fines and increasingly targeting senior-level individuals for prosecution because of misconduct or lack effective controls within the business.

Tightening regulations also mean that businesses, in addition to managing ethical conduct within their own organizations, are also responsible for monitoring and addressing misconduct that originates from their third-party business partners.

But the ability to detect, measure, and manage risk remains a challenge for many CPOs. Few are formally tracking risks in their direct supplier base and even less have visibility beyond tier 1 suppliers (Deloitte, 2021). As the arbiter of essential business relationships, procurement leaders need a scalable, process-oriented way to detect, measure, and manage risk among business partners.

We've developed a 16-point checklist that uses a sourcing-centric approach to get a 360-degree view of third-party business partners. But first, let's dive into the basic concepts of how Governance, Risk Management, and Compliance work in conjunction with third-party risk management.

Zoom In: Understanding Governance, Risk Management, and Compliance

Collectively, the discipline of Governance, Risk Management, and Compliance, known as GRC, holds an organization to a set of ethical standards that increases organizational effectiveness, safeguards business continuity, and protects the company's reputation. Below are the basic concepts of each component:

- **Governance** is the combination of processes established and executed by the board of directors, reflected in the organization's structure and how it is managed and led toward achieving goals.

- **Risk Management** is predicting and managing risks that could hinder the organization from achieving its objectives.

- **Compliance** is adherence to the company's policies and procedures, laws and regulations, strong and efficient governance are considered key to an organization's success.

In most organizations, compliance and legal are the primary owners of managing risk, but these activities are often siloed from other business units, which duplicates efforts and wastes resources. Conducting the appropriate due diligence of a third-party relies heavily on access to data from internal and external sources. Similarly, building an effective GRC framework requires an efficient and effective set of third-party risk management tools.

Zoom Out: How Third-Party Risk Management Bolsters GRC

Third-party risk management is an umbrella term that refers to all contracting, governance, risk, and compliance activities related to your third parties.

Organizations need to strategically merge their methodology, framework, and use cases with technology to build a GRC program that is effective. Ignoring the risks associated with third parties has far-reaching consequences that may negatively influence both reputation and revenue.

Third-party governance and risk management software simplifies the process of identifying and vetting business partners. It automates time-consuming processes, triggers alerts, monitors external sources of information, and integrates with other technologies like Contract Lifecycle Management software and Supply Base Management tools.
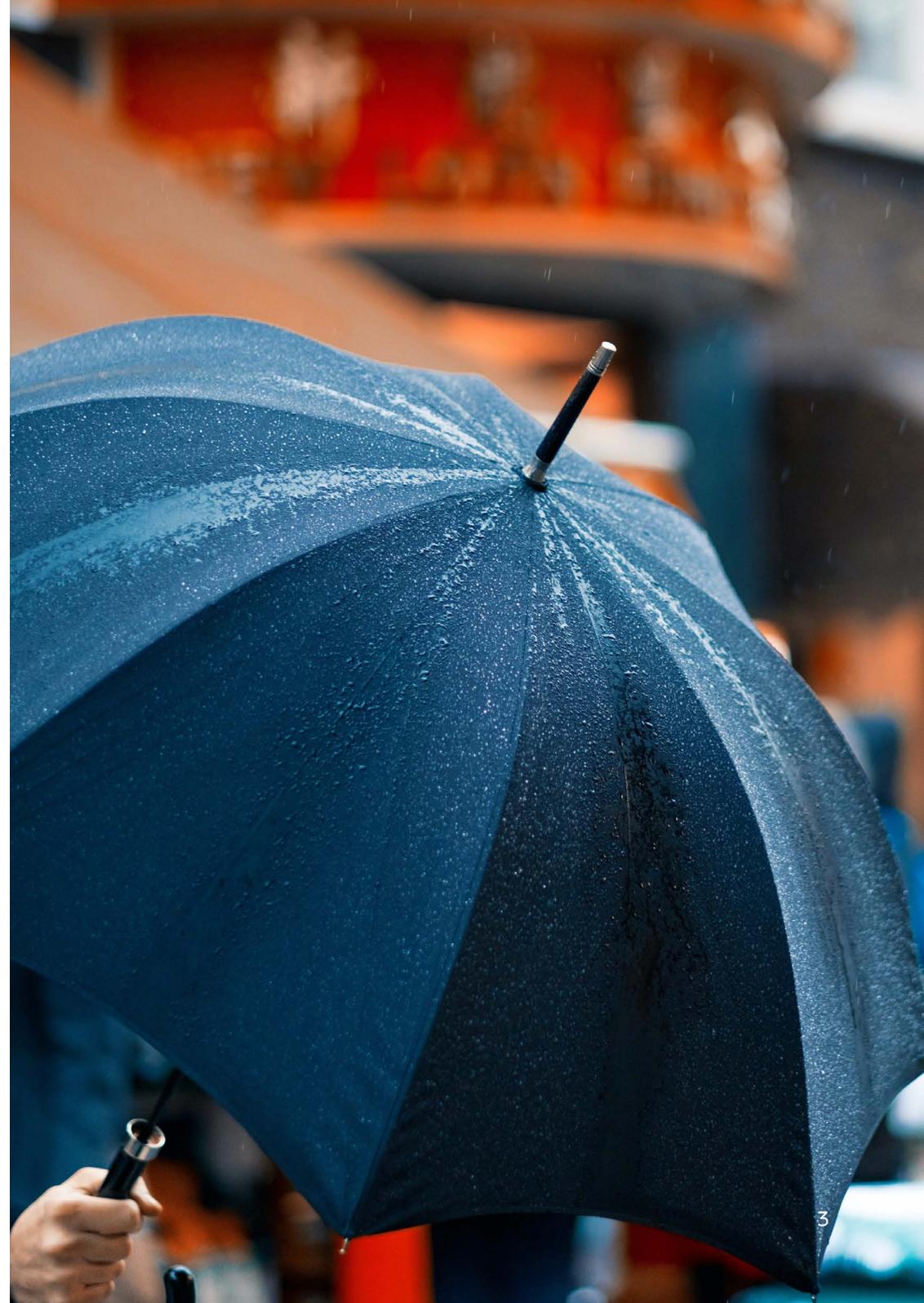
The 16-Point Checklist for a 360-Degree View

Verifying third-party business partners is of strategic significance to protect business operations, control costs, and ensure supply continuity. Use the checklist below to develop a standardized process that supports your organization's GRC objectives.

Source: 59% of organizations report having experienced a data breach due to a third party. (Gartner, 2021)

01 Strategy and Planning

Third-party risk strategy is developed and the cost and benefits are considered while the risk appetite is incorporated into the process.

02 Due Diligence and Third-Party Selection

Risk is identified, assessed, and prioritized. During this stage, due diligence and related enhanced activities are performed and recorded yielding which third parties are acceptable for a relationship.

03 Third-Party Portal/Registration

Provides a self-service option for third parties that automates and standardizes the registration process to ensure that all required information is gathered and kept up to date on an ongoing basis.

04 Qualification

Ensures that all third parties and trading partners meet or exceed regulatory standards.

05 On-boarding

Ensures that the required third-party processes, including due diligence, risk management, compliance, sourcing, procurement, and performance are delivered in an automated, centralized, and consistent fashion that can be easily tracked and audited.

06 Due Diligence

Automates initial and ongoing due diligence with a systematic approach. This facilitates credit checks, beneficial ownership checks, sanctions and watch-list screening, information security audits, sustainability audits, conduct risk assessments, and the collection of appropriate documentation and certification.

07 Risk Scoring, Assessment, and Management

Automates and continuously scores and assesses the risk originating from third parties. Integrates risk data (sourcing and management) from past events, externally provided third-party information and effective screening processes. Manages and controls risks through contract management and mitigation programs.

08 Contracting

Risk, compliance, and performance requirements are incorporated into contracts and reporting capabilities. At this stage contracts, including those for segmented expiration, are managed against SLA's and/or other contractual identifiers.

09 Contract Management

A single repository inextricably linked to the due diligence/on-boarding process that fully manages the initiation, authoring, approving, and post-execution management of contractual terms and obligations.

10 Regulatory Compliance

Manages both corporate and industry-specific regulatory compliance, including anti-bribery, anti-corruption, the Foreign Corrupt Practices Act (FCPA), data security and privacy (EU GDPR), anti-slavery, conflict minerals, and other trade compliance programs.

11 Compliance Management

Ensures third parties are adhering to compliance programs for code of conduct, information security, environmental, health and safety standards, and responsible sourcing.

12 Manage and Monitor

Risk is reported and monitored against key performance indicators and risk assessments are conducted across all risk profiles. Further, issues are documented and escalated as required and third-party reviews are scheduled for full remediation. This stage provides real-time risk reporting, management reports, dashboards, and visualization. Ongoing monitoring throughout the relationship is also provided here.

13 Master Data Management

Provides a single source of truth for third party and supplier information, providing an enterprise-wide view. The data model allows many-to-many relationships and full integration/synchronization with ERP/CRM systems.

14 Visibility

User dashboards, reporting, and drill-down capabilities, and provides continuous monitoring and flagging of risk and performance issues.

15 Termination and Off-boarding

At this stage users can determine whether they need to stop using a third party. This stage also enables users to manage the off-boarding process and block payments, orders, or contracts.

16 Audit

Provides evidence of compliance with full audit traceability.

To stay ahead of disruptions, procurement leaders need to prioritize embedding risk, resilience, and agility metrics across the organization. A cloud platform that digitizes the 16 processes listed above will help you conserve resources so your team can focus on mission-critical activities.

Are Governance, Risk Management, and Compliance at the top of your business agenda? Learn more about Scanmarket's acquisition of Symfact, which specifically addresses the trend of GRC and provides solutions across the full spectrum of risk assessment and monitoring.

Scanmarket

Scanmarket is a source-to-contract software provider that develops advanced functionalities in an effortless design. Originating from the needs of the end user, Scanmarket's S2C solution is attuned to meet the needs of the procurement professional. We take ownership of customer success with experts at your fingertips to drive user adoption. Digitalize your upstream procurement functions with technology that is built to be used.