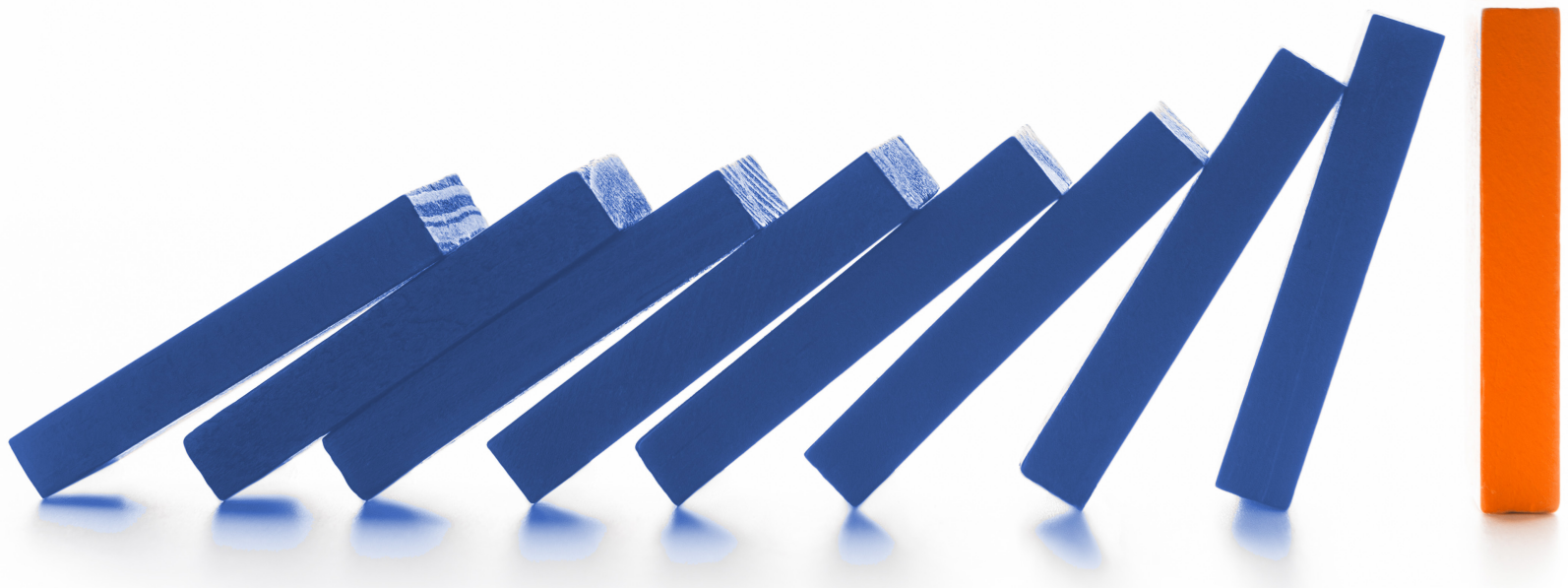
Insights for Effective Third-Party Risk Management:

PROTECT YOUR BRAND AND YOUR BOTTOM LINE



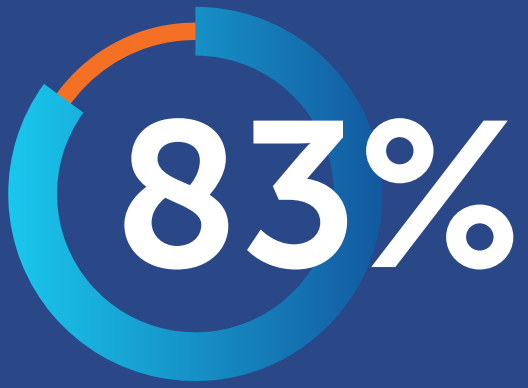
Introduction

Companies frequently use third-party suppliers, distribution partners, and free agents to accelerate growth, bring in expertise, or cut costs. While third parties can be beneficial, they can also present risks to organizations depending on what kind of services they provide and the company resources they have access to.

Third-party risk management grows more challenging as government regulations—such as the EU's General Data Protection Regulation (GDPR)—proliferate. These regulations hold companies responsible not only for their own actions but also for the actions of any party doing business on their behalf. Risk can come from third-party service providers and even IT platform providers that those service providers use to run their businesses. The cost of poor third-party risk management can be very high—up to 4% of revenue for violations of GDPR.

Information security risk, bribery and corruption, Corporate Social Responsibility, operational resilience, and other concerns with third parties must be carefully managed to avoid non-compliance, penalties from regulators, and damage to the brand.

When companies are trying to evaluate third-party risks during an unprecedented global event like COVID-19, having multiple siloed systems means delays that companies and suppliers can ill afford in a time of crisis. The performance and risk of each supplier relationship can significantly impact a company's success, especially during uncertain times.



of organizations experienced a third-party incident in the past 3 years,

11% of them with a severe impact and 35% with a moderate impact on customer service, financial position, reputation, or regulatory compliance.

Deloitte Third Party Governance and Risk Management Extended Enterprise Report

Digital Initiatives Can Leave Companies Exposed

Digital transformation initiatives have allowed many companies to shift non-core activities to service providers and digital platforms as they focus more deeply on their own core capabilities.

As they do so, compliance teams may struggle with the expansion in third-party providers if third-party management processes and technology are under-funded:

- **Excessive Manual Workload:** Compliance teams and Chief Information Security Officers (CISOs) find themselves bogged down with using spreadsheets or legacy tools to identify and manage third-party risk.
- **Constantly Changing Risks:** Third-party relationships with direct partner companies change with new business initiatives, while similar processes at partner companies are extremely difficult to monitor.
- **Complex Compliance Landscape:** Overlapping and changing regulations increase complexity, with extensive documentation and audit requirements.

For a complete list of all violations in the United States,
please visit goodjobsfirst.org/violation-tracker.

Industry Leaders Are Doing Things Differently

As many companies struggle with third-party risk management, others excel in this area. What are leaders doing to avoid costly and embarrassing incidents?

Leaders systematically ask a few crucial questions to avoid issues:

- Who are we doing business with?
- What subcontractors are they using that may expose us to risk?
- Do we understand the terms and clauses in our company's contracts?
- Which risks pose the greatest threats to our company?
- How are these risks being mitigated?

While implementing a strong risk management program may seem costly and daunting, looking to business leaders who've succeeded can be a great source of inspiration for those who want to improve their own programs.

Lapses in Third-Party Risk Management Damage a Major Brand

In 2019, a data breach at a billing contractor exposed the private data of nearly 12 million customers of a Fortune 500 company that provides clinical lab services. Investigators discovered that this massive data breach included personally identifiable information, credit card data, and health information. While the breach originated outside the lab services provider, the billing contractor's failure to secure customer data put the lab services provider's brand in the national spotlight with detrimental effects.

Leaders Use 10 Best Practices for Effectively Managing Third-Party Risk

One of the biggest challenges in risk management is that companies often experience different points of vulnerability as they work with large numbers of other companies, service providers, and contractors.

Here are a few tips for effectively managing third-party risk:

1. **Get Support from all Levels of Leadership:** Leading companies make sure their senior leaders and directors fully understand the importance of implementing a strong risk management program and are committed to doing so.

2. **Evaluate Every Third Party with a Minimum of Due Diligence:** Knowing who the partner is and how they operate is an important first step in detecting potential problems and reducing risk.

3. **Start with Provider Sourcing and Selection:** Third-party risk management should be incorporated into vetting and sourcing criteria when awarding new business. Vendors should be required to vet their own suppliers and third parties for security, compliance, and ethical concerns. Once awards are made, contracts should include the proper clauses to address risk.

4. **Understand How Company Resources are Managed:** It's good practice to track and analyze how third parties interact with company information and other resources, and how those resources are returned or destroyed when engagements are concluded.

5. **Provide Buyers with Visibility into Supplier Risk:** Properly assessing third-party risk is of limited value if employees buy from unvetted or risky suppliers.

6. **Continually Monitor Third-Party Behavior:** Annual or periodic assessments help companies detect risks, but continuous monitoring can help them detect problems and adapt to changes in technology and personnel.

7. **Include Performance in Risk Criteria:** Qualitative information on partner performance gathered from employees—preferably immediately after a service is rendered—adds to quantitative data on performance.

8. **Digitize Third-Party Risk Management Processes:** Moving from spreadsheets or legacy systems to a modern third-party risk management platform ensures that data collection and threat detection happen in real time, improving risk-management outcomes while also reducing costs.

9. **Conduct Periodic In-Depth Audits:** Engaging an expert, either from outside the company or from an internal audit team, provides an unbiased opinion on program performance. In-depth audits can identify problems missed by an automated process, as well as changes in the external environment that require process changes.

10. **Centralize Control of Risk Management Initiatives:** Having centralized control allows businesses to save on costs and avoid duplicating efforts when it comes to activities like vendor approval and vetting.

Risk is Relationship Specific

Leading companies make a distinction between risky third parties and risky third-party relationships. Foundational vetting may reveal that some organizations, such as restricted parties from government watch lists, shouldn't be engaged under any circumstances. Beyond that, relationships that require access to sensitive resources such as customer data as well as extensive relationships with the same third party (supplier concentration risk) call for increased scrutiny.

Integrating Risk Management with Business Spend Addresses Common Challenges

Successful companies integrate third-party risk management with a business spend management (BSM) solution. Third-party risk management should be part of the company's mindset and operational processes or systems, rather than an afterthought.

Here are some best practices:

- **Assess Supplier Relationships Comprehensively:** Gather information and analyze the risk a potential supplier relationship poses prior to starting a contract. Continue to evaluate the supplier throughout the lifecycle of the project.
- **Take a Multi-Tiered Approach:** Dig deep into the value chain by gathering information on contractors to direct suppliers, including fourth and fifth parties.
- **Manage Risk Proactively:** Inform decision makers about potential risks so that they can make effective spending and risk management decisions. This data allows them to work on action plans in order to remove risk from the supply chain.

Third-Party Risk Management Benchmarks

Best-practice companies combine an overall plan for managing third-party risk with operational Key Performance Indicators (KPIs) to measure efficiency so that they can improve. Efficient processes free up time to work with suppliers and business partners, letting companies become more effective in avoiding risk altogether. Benchmarks provide context that managers need to understand their current performance relative to leaders in third-party risk management.

This report features benchmarks drawn from Coupa Community Intelligence, an AI-powered analytics engine that monitors anonymized transaction data from across 1,000+ Coupa customers. These benchmarks represent top-quartile performance across Coupa customers.

1. External Risk Assessment Cycle Time: **81.1 hours**
   This KPI measures the time it takes for third parties to respond to risk assessments. Accelerated response by third parties improves service level to the business.

2. External Risk Assessment Completion Rate: **88.8%**
   This KPI measures the percentage of the assessments sent to third parties that are completed online. More assessments completed online reduce manual follow-up by compliance managers.

3. Internal Action Plan Cycle Time: **90.1 hours**
   This KPI measures the time it takes to put a risk mitigation plan in place. Accelerated risk planning improves service level to the business.

4. Suppliers Managed per Resource: **107 suppliers**
   This KPI measures the number of suppliers that can be managed by a single compliance resource. Organizations that have efficient digital processes will do less manual work, leaving more time for higher-value risk management activities.

Costs of Non-Compliance

When thinking about the return on investment in third-party risk management, consider that the total costs of non-compliance include not only damage to the brand, bottom line, and fines from regulators, but also investigation and monitoring costs associated with regulator action. Investigation costs typically equal about the cost of any fine, and monitoring costs post-fine are about half that. In areas such as bribery & corruption, total costs can be 2.5 times the fine amount.

Think Beyond the Governance, Risk Management, and Compliance (GRC) Approach

GRC is the capability to reliably achieve objectives (Governance) while addressing uncertainty (Risk Management) and acting with integrity (Compliance).[1] Today, a number of GRC software services are available to companies and practitioners. Successful GRC implementations present many benefits, including better decision-making and more efficient investing in IT resources.

However, stand alone GRC software solutions are often broad and very complex. They might not represent the shortest path to leader-level performance in third-party risk management KPIs. Integrating third-party risk management with BSM may be the right solution for many companies.

1 www.oceg.org/about/what-is-grc/

Telecom Giant Improves Risk Management Protocols After Getting Hit with $800 Million in Fines for Corruption

A multinational telecom company used local partners to secure needed frequencies in central Asia, exposing itself to bribery and corruption risk in the process. The company's third-party risk management program proved ineffective. A third party got involved in a bribery scheme and the company was subsequently fined almost $800 million.

After suffering significant embarrassment and changing its brand, the company turned to Coupa for a more reliable solution for managing risk and gaining transparency into third-party activities. Today, the company sees much greater participation from suppliers and is on track to emerge from increased regulatory scrutiny.

Effective Risk Management Plus BSM Offers Big Impact

With a comprehensive third-party risk management platform implemented in a modern digital platform, companies can gain advantage:

1. Reduce Reputation Risk: Lapses such as data breaches inflict long-lasting damage as customers defect to competitors. Digital platforms immediately surface risk flags to decision-makers across the company, letting them avoid risky suppliers and protect shareholder value.

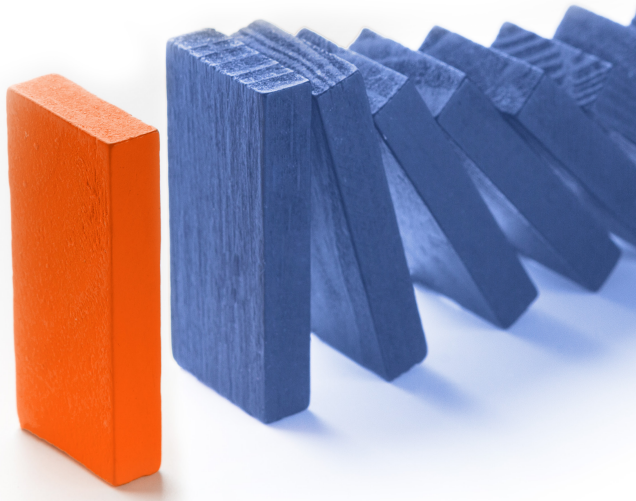
2. Avoid Regulatory Action: Fines can easily add up to millions of dollars, with total costs reaching much more. Digital risk and spend platforms increase effectiveness of risk controls while recording mitigation plans and activities, allowing businesses to stay compliant.

3. Manage Adverse Events: When mishaps do occur, companies using digital platforms will be better prepared to recover quickly. Properly designed systems let businesses immediately put relevant transactions on hold while suggesting alternative suppliers, minimizing the impact of adverse events.

4. Increase Supply Chain Agility: Automated, effective processes let companies vet suppliers more quickly, speeding time-to-market for new products and minimizing disruption if multiple suppliers need to be replaced quickly (e.g., in an economic downturn).

Conclusion

Executives and board members have a responsibility to ensure that their company utilizes necessary resources to protect the company's brand. Using the tips and best practices outlined here, organizations can be proactive in managing third-party risk and protecting themselves from damage to the brand as well as the bottom line. Uncertainties in times of global crisis make this all the more urgent.



Learn more about how Coupa can help your business.
Download our datasheet to learn more about how Coupa can help your company manage third-party risk. >

Want to see Coupa in action?
Attend a live demo about how Coupa can help your business achieve compliance and reduce third-party risk. >

With nearly $1.7 trillion of cumulative spend under management across its global customer base, Coupa offers all businesses—from Fortune 1000 companies to the world's fastest-growing organizations—the visibility and control needed to manage costs, mitigate risks, and scale for growth in one comprehensive and open cloud-based platform. With the extensive data flowing through Coupa, Community Intelligence uniquely offers real-time benchmarks and best-practice prescriptions that are tested against the measurable outcomes of companies around the world.

Coupa's Business Spend Management (BSM) Platform empowers finance and procurement leaders to spend smarter and tap into the collective wisdom of the Coupa Community. Join us to spend smarter today.

For more information, visit www.coupa.com.

coupa