coupa

Retrofit Your Risk Strategy:

How to Develop a Risk-Aware Culture

Businesses face risk from all angles—and from every department and third-party relationship.

Today, with suppliers, distributors, and other business partners dispersed across the world, there has been an acceleration in the number and types of risks that companies must handle, including unexpected economic events.

"Changes in the environment and in the global economy are increasing the frequency and magnitude of negative impacts from third parties," notes McKinsey Research."[1]

While COVID-19 has disrupted supply chains, so too have more frequent extreme weather events, higher tariffs, and regional conflicts, due to the rising share of global trade conducted in countries ranking in the bottom half of the world for political stability (rising from 16 percent in 2000 to 29 percent in 2018 according to the World Bank[2].) As McKinsey notes, "This is more than just a run of bad luck."

Companies face concerns about supply chain and third-party viability and performance, supplier concentration risk, and fraud. At the same time, companies must monitor different types of risk to address an ever-growing list of global government regulations and business requirements—including data privacy, information security, money laundering, bribery and corruption, environmental, geo-political, and cyber risk.

Once an afterthought in organizations, these risks are now top-of-mind for executives and their boards.

Instead of waiting for the "big one" to hit, companies would be wise to focus on building a ***risk-aware culture*** *from the ground up.*

A ***risk-aware culture*** takes a proactive stance. Risk isn't an afterthought. Nor is it seen as the responsibility of risk and compliance teams alone. Instead, accountability for risk is shouldered across the business, the entire C-suite, and by every employee. In this type of culture, managing business continuity risks and compliance, and responding quickly to adverse events are part of decision-making at the strategic and day-to-day levels.

In this guide, you will uncover the benefits of a modern approach to risk management, understand why the the status quo of managing risk in silos doesn't work, and unlock nine steps to develop a modern risk-aware culture.

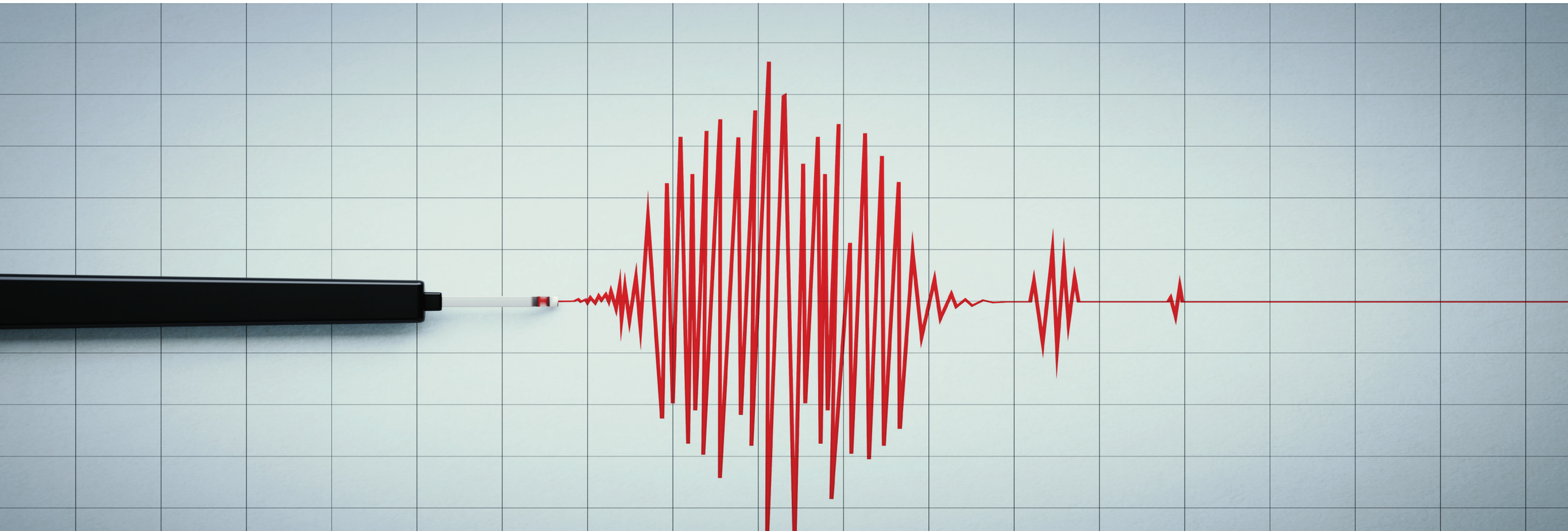
[1] https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains

[2] https://info.worldbank.org/governance/wgi/

Ignoring Foreshocks: Siloed Risk Management Approaches Fail

Minor tremors before a destructive seismic event are sometimes ignored or even undetected. So too go the warning signs of trouble with third-party relationships in organizations. While risk teams, often distributed across the company, may try to be proactive by setting rules and asking the business to comply, most resources end up being spent reacting to breakdowns in risk management, not proactively managing risk.

When risk and compliance teams operate in silos, it can be challenging to take a risk-aware approach. Many times, siloed teams find themselves with inefficient processes to identify and manage risk, which are often spreadsheet-based and riddled with inconsistency and error. As a result, risk mitigation is ineffective and unnecessarily costly. Initial assessments and ongoing monitoring are labor-intensive and time consuming, requiring excessive manual work to gather and analyze all of the relevant data from across the company. By the time the analysis is complete, it's often too late to act.



Three Faults of a Siloed Risk Management Approach

Surprises for Risk Teams and Delays for Business

When risk becomes a "hot potato" that gets tossed around, this is a sure sign that the company has not truly established a Risk-Aware Culture and needs to embrace change. Risk teams that are siloed don't get advance visibility into agreements with suppliers and other counterparties. They may be brought in to check the box for compliance just prior to contracting. Business partners may overlook better alternatives, and risk teams must scramble to avoid vetting delays that can be costly for the business.

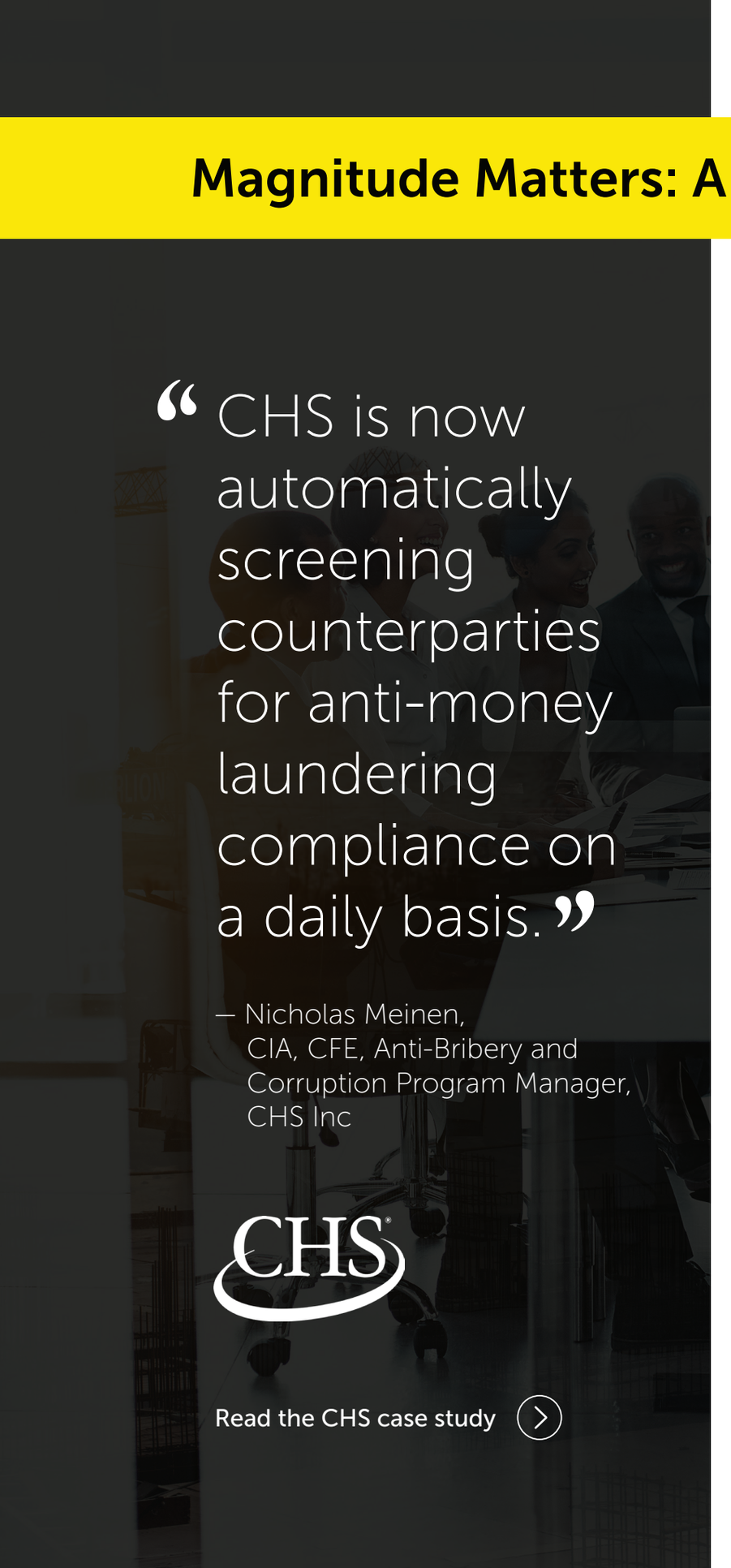
High-Risk Workarounds and Deliberate Non-Compliance by The Business

When employees are frustrated by the time needed for risk vetting or don't understand the process, they may start work with an unvetted vendor. This creates risk exposure on day one. The pressure and burden of identifying and managing risk is often forced on the line of business, which may not be well equipped or understand the value of vetting third parties to company standards. In a decentralized environment, some organizations focus only on the risk of a particular provider and service may not be understood before contracting, and in some cases, not until the invoice is presented.

Ineffective and Slow Risk Response

Risk signals from the immediate (like restricted-party list hits) to the longer term can't be acted on effectively. For example, if you find that a supplier has been flagged for a restricted-party list, then you need to stop spend, invoices, and payments immediately. But without a comprehensive risk-aware approach, it's challenging to share the right signals with the right people so that they act on them at the right time. Perhaps another company or another division has run into issues with a supplier but that information hasn't been shared effectively, and so it doesn't get acted upon until it's too late.

Magnitude Matters: A New Risk Management Approach



Risk leaders face significant issues with the change management needed to centralize and up-level their function. Now is the time to capitalize on the risk-concerned mindset of senior leaders to drive organization-wide change.

To build a risk-aware culture, start with the process used to engage and contract with business partners. Modern Business Spend Management (BSM) platforms manage all aspects of spend, from procurement to contracts to payments. By ensuring all spend goes through one platform, it’s much easier to rapidly identify third-party risks, such as information security, and ensure that all third parties are properly vetted before a contract is signed.

Benefits of an Integrated Approach for Risk Management

Avoid Surprises: Being proactive and embedding everyday processes used by the business, from contracting to purchasing, encourages business leaders to think about risk proactively and gives sufficient time for proper vetting.

Ensure Compliance: Collaborative processes act as guards against business leaders bringing on unvetted partners, either due to not understanding the process or intentionally working around it. Centralized processes streamline audits and make any required controls changes easier to manage.

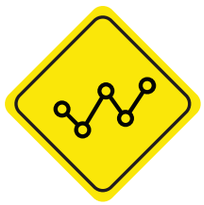
Respond Rapidly: Managing all types of third parties and all risk domains systematically, with a central process and platform, makes it much easier to respond to risk flags—as in immediately cutting off all in-flight transactions in case of a restricted-party list hit. A central process also makes it easier to track KPIs and compare them to benchmarks, ultimately moving towards best-in-class risk management.

Nine Steps to Develop a Risk-Aware Culture

To establish a Risk-Aware Culture, follow these nine steps:

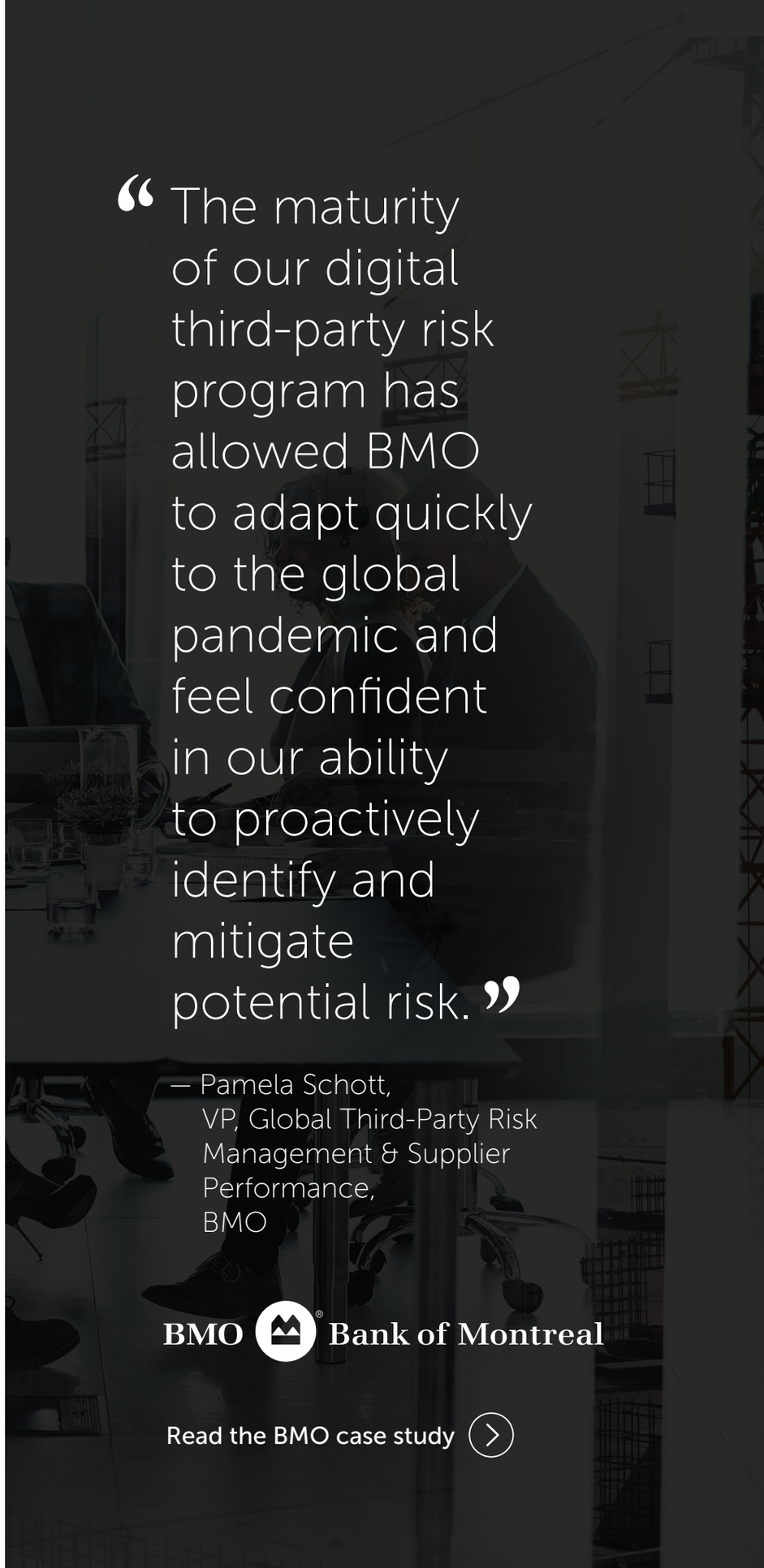
1. Best-Practice Template Approach
Your provider can give you templates to accelerate compliance in different risk domains, from GDPR to industry-specific needs such as OCC compliance in Financial Services.

2. Continuous, Broad-Based Risk Monitoring
Use platforms that connect with data services to monitor restricted-party lists, financial viability risk, and so forth on a monthly or even daily basis across your broad base of suppliers and third parties.



3. Community-Powered Risk Data
Participate in a community to share resources with other risk professionals, benchmark KPIs, and systematically get risk signals based on third party behavior with other companies. As soon as a third party hits a risk tripwire, that information should be shared across a network of companies with access to that data.

4. Central Process and Tool for Multiple Risk Domains
You may have different SMEs to manage data privacy risk for tech vendors and bribery & corruption risk for distribution, but a single BSM platform delivers consistency and auditability. It also allows executives to see a more complete picture of risk.



> “The maturity of our digital third-party risk program has allowed BMO to adapt quickly to the global pandemic and feel confident in our ability to proactively identify and mitigate potential risk.”

— Pamela Schott,
VP, Global Third-Party Risk Management & Supplier Performance,
BMO

BMO Bank of Montreal

Read the BMO case study

5. Provide Software That is Easy to Use for Employees and Third Parties
The best time to ask suppliers for information (such as answering a risk questionnaire or updating their diversity status) is when they are submitting a PO or invoice. If all spend is managed through one easy-to-use (and frequently used) BSM platform, there are ample opportunities to collect this data.

6. Improve Decision-Making by Putting Risk in Context
Combine risk ratings with spend. Use platforms that capture a full picture of risk, and apply the insights generated when and where decisions are made. For example, steer employees to risk-vetted partners (from simple purchasing to planning sourcing events and more).

7. Improve Visibility for Risk Teams
Platforms can alert risk teams to purchase requests and in-flight contract approvals with risky or unvetted third parties, or to those that may change relationships so that additional vetting is needed.

8. Operationalize Risk Response
Use an integrated platform to quickly identify risk flags, understand all aspects of the third-party relationship, and respond immediately—from putting a risk mitigation plan in place to halting in-flight invoices and payments.

9. Select a Platform That's Configurable Without IT Support
When a requirement changes or when users are having issues with a question, you can update assessments as needed.

Preparing for the Unexpected: Managing Risk Through Constant Shifts

Today, many companies are stabilizing after their initial pandemic response and reflecting on lessons learned. Companies are evaluating what changes still need to be made their supply chains to build resilience, such as adding more redundancy and near-shoring. And they are examining their risk response to see how they fared.

Globalization, digitization, environmental conditions, and political shifts have brought risk management to the forefront. It's important to evolve your risk management programs and develop a risk-aware culture to get ahead of unanticipated events that require rapid response. Regardless of scale—whether minor tremors or major disruptions—preparation is key to supporting business continuity.

Now is the time for proactive procurement and risk leaders to make a change. Start by looking within the company to see where all of the different types of third parties are managed, how each risk domain is addressed, and what's the frequency of assessment.

Is there a truly cohesive and integrated third-party risk management process? Or are there many processes (and gaps in between)? If so, it's time for change across the people, processes, and technology decisions to retrofit your risk management and build a risk-aware culture, where risk is co-owned between the business and risk teams, not separated and managed inefficiently in silos.

Learn more about Third-Party Risk Management at coupa.com