

# The Companies you keep

Global Supply Chain Management:  
Five Steps to Managing Third-Party Risk



# Letter from the Chair



As lawyers, it can be easy to fall into the habit of approaching every client issue from our particular area of expertise. We get used to viewing corporate challenges through our anti-bribery, antitrust, customs, sanctions, export controls, product regulatory or privacy lens—often in isolation of a client's business reality or even related legal issues outside of our own proficiencies.

When we started talking about doing this survey, however, we were beginning to realize that companies managing global supply chains need more than siloed, specialized advice. The cycle of designing, producing and distributing goods and services is a single process of interconnected steps. Where a company sources its raw materials and how it manufactures a particular product can have a profound effect on where it can sell that product and what kinds of requirements it is subject to down the line. There is a reason it's called a chain.

We also recognized that the increasing use of third parties in supply chains was creating some of the greatest challenges for our clients, not to mention major compliance risk. Historically, companies have rarely been held accountable for the actions of their business partners, largely because years ago, companies performed many of the processes they now outsource. It also stems from growing concerns about issues like terrorist funding and human rights that have brought the idea of holding people responsible for who they do business with into the limelight. As a result, governments around the world have been passing and enforcing an ever-expanding list of laws that have essentially forced companies to scrutinize and police those acting on their behalves. For this reason, third-party relationships are not only a source of cost-savings and greater efficiency, but also major stress.

Our purpose in undertaking this survey was to understand what companies perceive as their greatest third-party risks and apply our collective knowledge to better address their increasing legal responsibilities in this context. The results affirm what we have long suspected: that companies must take a coordinated, integrated approach to how they structure their supply chains and assess and manage their risk. We hope this report helps you in that pursuit.

**Nicholas Coward**

Global Trade & Commerce Practice



If you choose people who have a bad reputation, it can impact your operation and your company image.

Compliance Director

## Introduction

Nearly 50 years ago, Warren Buffett warned his young son, Howard, “It takes 20 years to build a reputation and five minutes to lose it. If you think about that, you will do things differently.” The Berkshire Hathaway CEO wasn’t talking about global supply chain management, but he may as well have been.

Companies are more concerned than ever about the reputations of the third parties that source, manufacture, transport, distribute, market and sell their products around the world. When assessing whether to hire a third-party supplier or partner, reputation is even more important than cost, according to our survey of 100 global supply chain executives.

Recent news headlines will tell you why: major retailers face public scrutiny after a series of factory fires and a building collapse in Bangladesh kill hundreds of workers making clothing for their subcontractors. UK food inspectors discover horsemeat in Findus beef lasagna sourced from a subcontractor that passed off Romanian horsemeat as beef. Billabong falls victim to hackers who steal the user names and passwords of 35,000 customers who registered online for a promotional event through the surfwear company’s marketing firm.

“The reputation of third-party suppliers and partners is very important because it reflects on yours,” said one compliance director interviewed in our survey. “If you choose people who have a bad reputation, it can impact your operation and your company image.”

The increased focus on reputation also stems from the fact that governments are imposing more and more regulations on companies holding them accountable not only for their own actions, but those of their third-party suppliers and partners on everything from money laundering and data protection to using forced labor and sourcing conflict minerals from the Congo.

As a result, corruption and general compliance issues such as antitrust, data protection, export control and trade sanctions have risen to the top of the list of things companies worry about in their third-party relationships, surpassing even product quality and timely delivery.

“My biggest focus is making sure that we’re selecting partners that don’t put us at undue bribery risk,” said another compliance manager interviewed in our survey.

The **key findings** from our survey of 100 senior executives who oversee their companies' supply chains include:

- **Corruption and general compliance top the list of third-party concerns.** When asked what they worry about most when working with suppliers/partners, our respondents said corruption (24%), general compliance (19%) and product quality (15%). They also listed insolvency of third parties and data/cyber security as significant areas of risk.
- **Compliance with rapidly developing laws in emerging markets, international trade sanctions and anti-bribery laws are the greatest future risks.** In the next two to three years, respondents said their greatest third-party risks will be region-specific risks (20%), compliance (20%) and financial risks (15%).
- **Training is the best strategy for reducing third-party risk.** Respondents said providing more training for employees and suppliers/partners on major compliance issues and guidance on how to identify and mitigate compliance risks is the No. 1 way to reduce third-party risk (83%), followed by having better processes for monitoring their compliance with contractual terms (75%) and having better protocols for screening suppliers/partners (74%).
- **When selecting third parties, experience and reputation are most important.** Respondents said the most important factors when assessing the suitability of suppliers/partners are experience and track record (8.2 points out of 10), reputation (8.1), and cost (7.9).
- **Working with third parties in China, India and Africa present the highest risk.** Respondents said that their third-party risk is highest in China (40%), followed by India (30%), Africa (26%), Russia (22%), South America (21%) and the Middle East (9%).

Despite the third-party risks, global supply chains remain crucial to the success of multinational companies. Given the huge pressure to reduce costs, along with the advent of globalization, digitization and transportation advancements, few companies operate exclusively within their own four corners anymore. They have become so-called “extended enterprises” that span numerous levels up and down the supply chain, from the suppliers they source their raw materials from, to the sales agents, distributors and franchisees who sell their products on the market and all of the manufacturers, transporters, brokers and other service providers in between.

These extended enterprises move a huge volume of raw materials, components, technology, products, services and information across borders every day—creating new opportunities and greater efficiencies but also more complicated business relationships and much higher risk.

That’s why it’s more important than ever for companies to take a holistic, integrated view of their global supply chains to identify their greatest third-party risks and implement the best strategies for mitigating and managing those risks across borders and business units.

To help companies with this process, we’ve taken the greatest compliance and commercial concerns expressed by our survey respondents and provided recommendations to address those concerns within five key stages of a third-party relationship: vetting and selecting, structuring and documenting, training and educating, monitoring and evaluating, and reacting and remedying. For each stage, we provide an overview of the relevant survey findings and actions companies can take to improve efficiency and avoid common mistakes.

Any effort to create an effective strategy for third-party risk management must start with an analysis of what your legal requirements are, given your industry, the countries where you do business, and the types of third parties you work with. We also recognize that risk management programs will vary greatly depending on your company’s industry, geography and circumstances.

But regardless of your industry, our end-to-end framework provides general strategies and practical tips to help you assess and address third-party risk more quickly and effectively at a time when enforcement agencies, investors, business partners, NGOs and the general public are demanding that companies uphold the highest business and ethical standards.

# 1 VETTING AND SELECTING



# 2 STRUCTURING AND DOCUMENTING



# 3 TRAINING AND EDUCATING



# 4 MONITORING AND EVALUATING



# 5 REACTING AND REMEDYING

1

# VETTING AND SELECTING



Choosing the right third-party supplier/partner can mean the difference between having a significant asset or a major liability. The goal of vetting and selecting is to make sure that a supplier/partner can not only meet price, quality and delivery requirements but also comply with regulatory and anti-bribery standards.

In fact, **the respondents in our survey ranked reputation above cost** as the most important criteria when selecting third parties — a reflection of the damage a third party's actions can do in today's heightened enforcement environment. More than 90 percent of the FCPA actions brought by the US Department of Justice, for example, involve misconduct by a company's third party, according to a global fraud survey conducted by Ernst & Young in 2012.

"Reputation in the industry is a really huge issue because companies that have a good reputation and are concerned about their reputation tend to work toward not having something that will taint them going forward," said one of the supply chain managers interviewed in our survey.

Careful vetting and selecting is particularly important in emerging markets, where 81 percent of our survey respondents said the risks are higher, particularly in China, followed by India, Africa, Russia and South America. In China, our respondents identified **regulatory instability, a different approach to bureaucracy** and **truthfulness of information** from third parties as major hurdles.

Here are some recommendations to help you overcome those hurdles and implement better systems for vetting and selecting third parties.

**Use your RFP process to secure commitments from suppliers/partners that address your greatest legal risks while the process is still competitive.**

The vetting and selecting of third-party suppliers/partners is often left to the procurement team with little input from the legal department unless it's a particularly significant or complex agreement. But it's in the early stages of the process that you have the most bargaining power to mitigate your greatest legal risks, when the suppliers/partners know they are still in competition with each other.

To take advantage of this leverage, identify your key risk areas in that third-party relationship, then tailor your procurement documents to address those risks by listing the appropriate risk management requirements. For example, if product liability is a major concern, include a statement such as, "We require all suppliers to have product liability insurance of not less than XX amount," with two columns where a supplier/partner can check one of two boxes, "comply" or "not comply." Knowing that the more "comply" boxes they check, the more likely they are to win the business, third-party suppliers/partners are more likely to agree to the terms you want. That not only assures you greater protection in your key areas of risk, but shortens contract negotiations down the line.

"If they know they're negotiating with you one-on-one, they're more likely to say we won't do this, we won't agree to that," says Penny Ward, a trade and commerce partner based in Baker & McKenzie's Sydney office. "But if you include it in the RFP process, they're most likely to put their best foot forward."

Many multinationals also make the mistake of selecting a third party too soon, losing their competitive edge before they've locked in crucial aspects of the contract, such as pricing, service levels and liability limits. It can be an effective strategy to keep more than one supplier/partner in the running until you have negotiated these critical issues.

"You need to do as much as you can to get what you need while there are still two horses in the race," says Duncan Reid-Thomas, a partner in Baker & McKenzie's Commercial Practice in London. "Otherwise it will be a struggle to get the best deal you can."

**Create a matrix based on a risk analysis of the industry, geography and type of work third-party suppliers/partners would be doing, then vet them accordingly.**

Given that no two relationships are the same, a good starting point for due diligence is grading suppliers/partners based on the degree of risk they pose and assigning them to categories. Which category they fall into will determine the level of scrutiny you use to review them.

For low-level risk, you may do an internal review of things like ownership, financial health and whether they appear on any sanctions blacklists. For mid-level risk, you could ask the third party to complete a due

The most important factors when selecting third-party suppliers/partners are (points out of 10):

Experience and track record

8.2

Reputation

8.1

Cost

7.9

**“The reputation of third-party suppliers and partners is very important because it reflects on yours.**

Compliance Director



diligence questionnaire and conduct a more detailed review of their directors and shareholders. For the high-risk relationships, such as contractors that would interact with foreign government officials or state-owned enterprises in countries where kickbacks are common, you might hire an outside investigative firm to put together an independent FCPA/anti-bribery due diligence report.

Your legal or compliance department should review this report, along with any due diligence questionnaire and compliance certifications provided by the third party, to determine whether to approve them. Be cautious, however, not to gain a false sense of security that merely because you've commissioned one of these reports, you're covered for liability. Laws such as the UK Bribery Act require you to have "adequate procedures" for vetting third parties, which means investigating red flags and continuing to monitor your relationship.

For specific concerns such as data security and antitrust issues, it's important to conduct additional screening. To address data security concerns, check to see whether a potential third party or their major subcontractors has a history of data security breaches by consulting industry sources, such as the Chronology of Data Breaches, a US nonprofit privacy monitoring organization. You may also ask to see their written information security policies, as well as recent third-party audit reports on their data security systems to make sure they have appropriate safeguards in place to protect personal information.

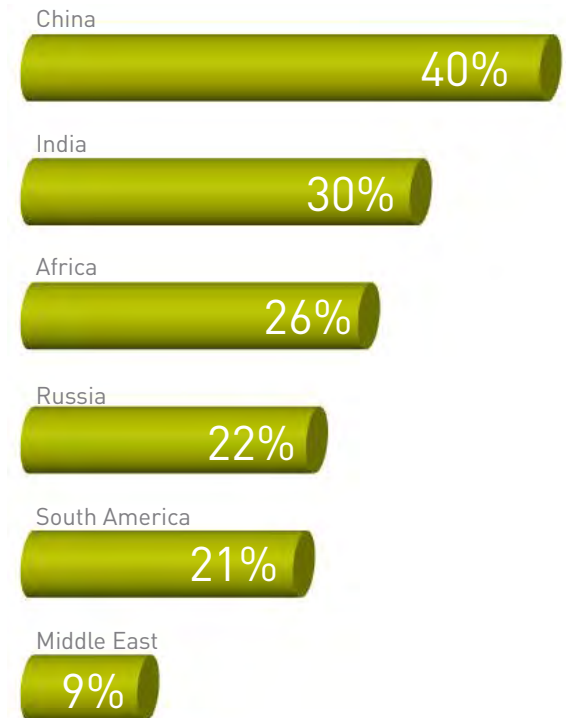
For antitrust issues, you should be sensitive to whether you or a potential third-party supplier/partner has a dominant market position and whether establishing a relationship could be viewed as abusing that dominant position. Further, if a potential business partner is an actual or potential competitor, you also want to investigate whether the proposed collaboration could be construed as anti-competitive by the antitrust authorities.

**Check references and conduct in-person interviews with key partners in high-risk jurisdictions, particularly in less transparent markets.**

In emerging markets, it can be more difficult to verify issues like ownership, financial solvency, proper registrations and criminal histories. To overcome these challenges while vetting, ask potential third-party suppliers/partners whether they've done similar work for other customers and get references to verify the quality of their work. It's typically a good sign if they've worked for other multinationals because that means they made it through those companies' vetting processes, which tend to be more rigorous. If you're a high-end apparel company looking to sell your clothes in Mexico, for example, a good starting point may be looking at which customs brokers similar companies in your industry are using to bring their goods into the country.

"If you know that Ferragamo and Louis Vuitton are using certain brokers, you may want to put them on your short list, then narrow your list based on your own due diligence," says Edmundo Elias-Fernandez, chair of Baker & McKenzie's Latin America Foreign Trade & Customs Practice, who is based in Guadalajara.

Respondents say the emerging markets that present the greatest risk are:





You also want to interview the company owners and managers who would oversee your business relationship to get a sense of how they operate and whether they have the capacity to handle the volume and complexity of your business. In places like China, where gift giving and hospitality is part of the local culture, you would want to ask them what their entertainment policy is. If it's a pharmaceutical distributor, for example, you should ask, "Which hospitals do you have relationships with?" and "How do you entertain the doctors you sell drugs to?"

You also want to tell them that it's strictly against company policy to bribe government officials or business associates and most importantly, watch their reactions throughout your discussion. If, for example, they tell you that they never entertain clients, that's a red flag. But if they say they send clients cans of tea from their region or moon cakes during the Mid-Autumn Festival—gifts that cost less than RMB 200 (US \$30)—they are more likely to be complying with local and international anti-bribery laws.

To verify the truthfulness of their answers, interview the owners and managers separately and compare their answers. But be careful not to turn it into an interrogation.

"It's important to make people feel comfortable and let them talk," says Michelle Gon, a Baker & McKenzie corporate compliance partner in Shanghai, who has interviewed hundreds of Chinese suppliers, distributors and other third parties on behalf of multinational companies. "That requires knowing the local language, customs and understanding their business. If you ask the wrong questions, they'll know you don't understand the culture or their industry. But if you ask relevant questions, they're more likely to take you seriously and provide substantive information."

It's also important to keep in mind that local standards on issues like bribery and hospitality are continually changing in emerging markets. Given all the international focus on corporate corruption, local governments are becoming more aggressive in enforcing their own anti-corruption regulations and modifying these laws without much public consultation. As a result, you must routinely check to see what the local standards are rather than assuming they are still the same as last year, an assumption that could lead to non-compliance.



It's important to make people feel comfortable and let them talk. If you ask relevant questions, they're more likely to provide substantive information.

Michelle Gon, Shanghai Partner

**Assess what potential suppliers or contract manufacturers know about the legal requirements of the market where you want to sell your products.**

With the globalization of the supply chain, products are often manufactured in one jurisdiction and then sold to consumers or businesses in another. It is therefore key that you discuss the regulatory requirements of the markets where your products will be sold with your suppliers/contract manufacturers at an early stage. You should evaluate their understanding of product regulatory requirements (e.g. product content restrictions, energy efficiency requirements, information and labelling requirements) in the end jurisdiction and also ascertain how trustworthy any assurances they provide will be. “In the long run, you will need to be comfortable that your suppliers have appropriate systems and quality control processes in place to ensure that the materials they use and the components and products they make on your behalf are compliant” says Graham Stuart, a product regulatory and environment partner in Baker & McKenzie’s London office.

One way of increasing suppliers’ awareness of destination market requirements is to draw up a “product specification” that details the product regulatory requirements with which any product, component or material they supply to you will need to comply. This will need to be updated as and when product laws in any of your target markets are introduced or amended but this approach is usually preferable to expecting third party suppliers, often based in emerging markets, to keep abreast of relevant regulatory changes which occur outside of their own jurisdictions. You can even provide the product specification to potential suppliers as part of any RFP process and ask them to confirm that they will be able to meet its requirements.

**Develop a checklist of legal and risk-related questions for your procurement officers.**

More often than not, a company’s legal and compliance departments aren’t involved in interviewing potential third parties, a job left largely to procurement officers. But having legal or compliance team members involved in creating or reviewing a list of questions that covers your company’s key risks areas, in addition to standard questions about product quality and operations, will help protect your interests. The list should include both local regulatory requirements, specific requirements applicable in the markets where you want to sell third parties’ products and international compliance laws. You should also train your procurement officers on the underlying reasons for each question, so they have a better understanding of what to watch out for in third-party interviews.



In the long run, you will need to be comfortable that your suppliers have appropriate systems and quality control processes in place to ensure that the materials they use and the components and products they make on your behalf are compliant

Graham Stuart, London Partner

Respondents say their top third-party risks in emerging markets are:

Corruption

69%

Bribery

58%

Political instability

33%

Lack of enforcement

18%

### **Keep records of all your due diligence.**

While vetting potential third parties, particularly in emerging markets that are less transparent, you should compile and retain all the evidence that you searched public records and verified information such as ownership, financial standing, reputation in the local market, and whether the names of any of their directors, owners and shareholders appear on restricted party lists. “You want to have a heavy paper file,” says Reagan Demas, a corporate compliance partner in Baker & McKenzie’s Washington DC office. “It’s important to have proof that you scrutinized all of the pertinent compliance and commercial issues.”

### **Be wary of using offshore third-party suppliers/partners in high-risk markets.**

Most multinational businesses, particularly in high-risk sectors such as healthcare and oil and gas, have rules prohibiting the use of offshore third-party suppliers/partners unless they have a clear legal or commercial rationale for making an exception. That’s because in many high-growth markets, service providers or distributors incorporated in places such as the Seychelles and the Marshall Islands are commonly set up offshore for illegal purposes, such as tax evasion, customs fraud, money laundering, bribery and theft by company executives and shareholders. To avoid getting caught up in these schemes, it’s a good idea to establish restrictions on using offshore third parties in high-risk markets. Valid exceptions to those restrictions would include issues such as local exchange control restrictions on advance payment that may mean using an offshore distributor is the only way you can get paid in advance and manage your credit risk. You should, however, regularly review these arrangements to make sure your underlying reasons for making exceptions are still valid.

### **Avoid selecting third-party suppliers/partners on the basis of price if it means you will be the importer of record.**

When buying materials, components or products from suppliers and manufacturers overseas, some companies will take on the responsibility of clearing those goods through customs to pay a lower price. Being the importer of record, however, can open you up to unexpected liability. In the US, for example, this includes antidumping duties and potential civil and criminal liability for violating dumping orders, such as those that may arise if the product is transshipped through a third country to avoid paying dumping duties.



It’s a mistake to give suppliers exclusivity without a real need to do it.

Carsten Dau, Frankfurt Partner

Many companies don't understand that when they pay an anti-dumping duty to get a product through customs, it is only a deposit based on an estimate, not the final price. Months or years later they can get a bill for the balance once the local trade authorities determine the exact rate — a bill that might erase any savings the company thought it had gained by being the importer of record. Buying the product US DDP (delivered duty paid), for example, can alleviate that price uncertainty and the potential for being charged with evading a dumping order, which can carry criminal penalties under the US False Claims Act. With customs officials becoming more aggressive in pursuing these types of cases, being the importer of record can become a liability fast.

### **Start small and go slowly.**

It's tempting to jump at the chance to work with a distributor that says they can sell your product throughout all of Europe or a supplier who can source all of your electronic components from China. And in some markets, you may not have a lot of suppliers or partners to choose from. But making someone your exclusive distributor or giving them too much responsibility right away can really hurt your business. They could be too small to handle selling your pharmaceuticals throughout all of Europe, provide poor service, or sell you defective or non-compliant components. If you've agreed to an exclusive relationship, you could be stuck with them for a long time.

"Sometimes clients lock themselves into exclusive relationships to save on price but it's a mistake to give suppliers exclusivity without a real need to do it," says Carsten Dau, a partner in Baker & McKenzie's Commercial Practice in Frankfurt.

Instead, start by sourcing one product from a supplier with a plan to buy more products from them if that arrangement goes well. With a new distributor or sales agent, give them a small territory to start with and expand little by little until they've established a track record and proven themselves to be trustworthy. As you expand your relationship, however, be careful not to become too dependent on any one supplier/partner for a critical aspect of your business. Doing so can become detrimental in the event of things like natural disasters, third-party insolvency or even price negotiations, since you have fewer options and less leverage.

### **Become an AEO (authorized economic operator) and use third-party suppliers/partners that are also AEO certified.**

A growing phenomenon in the global supply chain world is to operate under the SAFE framework developed by the World Customs Organization to ensure strict control over the flow of goods and documents throughout companies' supply chains. The framework establishes a set of standards such as having cameras in warehouses, requiring employees with access to wear colored vests and monitoring loading docks. The program has a different name in various countries (in the US, for example, it's called C-TPAT) and administered by the government.



For highly sensitive data, companies should consider private cloud solutions because they provide greater control.

Brian Hengesbaugh, Chicago Partner

Adhering to these AEO standards and using third-party suppliers/partners that do so as well can really help you implement best practices. Governments have also provided incentives for following the framework. In Mexico, for example, companies with AEO certification are only subject to having 2 percent of their imports and exports inspected by customs officials, rather than the usual 13 percent. While adopting this framework often requires some investment, it can pay off quickly by raising your profile as a company that holds itself to higher standards, a reputation that can lead to increased business.

**Consider using a private cloud computing model when sharing sensitive personal information with a third-party supplier/partner.**

The first step in vetting a potential third party for data protection is understanding what personal information will be shared with or accessed by the provider, and what privacy obligations are applicable. Key factors include whether you will be sharing sensitive personal information with them such as social security, credit card or bank account numbers that would trigger a breach notification duty if it were lost or stolen. It is also critical to understand where the individuals identified in the data reside, and what privacy laws apply in those jurisdictions. Depending on the answers, you may need to establish specific privacy contracts with the provider and its subcontractors, and register with various data protection authorities.

In some cases, you should exercise caution before placing highly sensitive personal information into truly “public” cloud solutions where you won’t have visibility or control over subcontractors that have access to the data. The problem with this arrangement is that if a breach of security occurs at the subcontractor level, it can be more difficult for you to receive timely notice of the incident and conduct forensics and other assessments to determine which data was affected.

“For highly sensitive data where a breach of security may trigger notification obligations, companies should consider private cloud solutions because they provide greater control, even if they are more expensive,” says Brian Hengesbaugh, a data privacy partner based in Baker & McKenzie’s Chicago office. “Otherwise, in the event of an actual data breach, you may not be able to respond with as much speed or certainty as you could if you were using a private cloud solution.”

2

# STRUCTURING AND DOCUMENTING



The structuring and documenting phase of a third-party relationship is about allocating risk through negotiations and contracts. It's when you establish the project scope and business objectives and identify the metrics and processes for monitoring and evaluating whether the third-party supplier/partner is meeting those objectives and appropriately managing risk. It's also when you negotiate remedies for the third party's failure to meet those metrics and possibly offer incentives for high performance.

Some third-party relationships won't warrant a high level of attention and can be established using standard templates and little negotiation. For the more high-value or high-risk relationships, however, it's crucial to structure the relationship so that you are as protected as possible.

According to the 100 respondents in our survey, the greatest third-party risks they face in their supply chains are insolvency of key suppliers and partners, data/cyber security and bribery of government officials.

"A key risk we are seeing on the input side is viability of vendors in these economic times," said one head of legal interviewed in our survey. "We've had experiences where key vendors ceased supplying software. They either went bankrupt or disappeared."

Our respondents also said that in the next two to three years, their greatest risks will be region-specific risks, compliance and financial risks.

"With all the regulatory changes in the countries in which we do business, the greatest risk will be ensuring that we keep up and that our third parties are doing the same," one compliance manager said.

Here are some recommendations to help you better structure and document your third-party relationships.

### Work backwards.

A good place to start a third-party relationship is thinking through where you want to end up. Many disputes with suppliers and partners occur because company directors and managers haven't taken the time to establish the business requirements and objectives of a third-party relationship and determine the legal and operational risks associated with the project. That makes it more difficult to define the scope and negotiate the pricing, performance levels and allocation of roles and responsibilities to lay the groundwork for a productive relationship. A more strategic approach is to ask yourself questions like, What's this going to look like when it's up and running? What are the key risks? And what can I do, sitting here now, to minimize those risks? It's best to know the answers before you sit down with a third party to negotiate the contract.

### Create risk matrices or playbooks to make risk assessment easier and quicker during the heat of negotiations.

To help avoid making rash decisions when negotiating under tight deadlines with limited budgets, some companies have created templates that reflect the risk profile that a business unit is willing to accept and risk matrices or playbooks for those templates. Those matrices or playbooks spell out what terms they can accept, which ones are preferred and which are deal breakers on issues such as warranties, indemnities and liability limits. They then map the terms in a supplier/partner's contract to see where they measure up and fall short of their thresholds.

"I'm surprised that many big companies are willing to accept such a variety of contract terms," says Mattias Hedwall, chair of Baker & McKenzie's EMEA Trade & Commerce Practice, who is based in Stockholm. "Many companies could benefit from having a more structured approach to the management of their agreement portfolios."

Having this resource handy helps keep negotiators from giving up key risk protections while under pressure to get a deal signed and provides them with clear direction on how high up in the procurement department they must go to get approval, depending on the level of deviation from preferred terms.

### Establish appropriate audit rights and requirements that your suppliers/partners undergo compliance training.

Whenever possible, include a provision in your contract that allows your company access to a supplier/partner's books and records that are relevant to your business. You also want the right to inspect the areas of their facilities involved in the manufacture, transport or distribution of your product to make sure they are complying with your code of conduct. It's not vital to settle who will undertake the audit, as the supplier/partner may prefer to hire an independent auditor to conduct the review, but it is important to get the right to audit. If you've shared personal

Respondents say their top third-party supply chain risks are:

Insolvency of key partners and suppliers

43%

Data security

35%

Cyber security

33%

Bribery of government officials

32%

“A key risk on the input side is viability. We've had experiences where key vendors ceased supplying software. They either went bankrupt or disappeared.

Head of Legal



data with them about your employees or customers, you may also want to include data privacy language that allows your company or a third-party reviewer to audit their technology systems. To better ensure they comply with applicable anti-bribery, antitrust, health and safety, child labor, product-related and environmental laws, it's also advisable to require that they undergo periodic compliance training and train their employees on these topics.

**Include strict compliance covenants in your third-party contracts that describe the type of conduct you prohibit.**

With the recent surge in FCPA enforcement, enactment of the UK Bribery Act, and proliferation of local anti-bribery laws, most multinational companies are aware of the importance of having compliance language in their contracts that prohibits paying bribes or engaging in other forms of corruption. Sometimes, however, the third-party supplier/partner can resist signing contracts that require them to comply with laws that they don't think they're subject to, such as the FCPA, because they have no ties to the US. In those cases, such as contract negotiations between a UK company and a vendor in a high-risk market like India, it may be more effective to describe the type of behaviors they are prohibited from engaging in, such as actions that would constitute bribery, rather than merely citing specific laws. Even better, many multinational companies have begun creating "Supplier Codes of Conduct" that lay out their expectations for suppliers to operate in a responsible and ethical manner, such as complying with health and safety, non-discrimination and child labor laws. In their agreements with individual suppliers/partners, the multinationals then reference those codes of conduct and require that the supplier/partner comply with them.

**Make sure that your contract requires third party suppliers to comply with the regulatory requirements of the markets in which you want to sell your products.**

Ideally your suppliers should confirm in your contractual arrangements that the materials, components or products they supply you with comply with the regulatory requirements applicable in your intended markets or the requirements of your product specifications (if you have them). This includes complying with safety requirements, substance restrictions, energy efficiency and ecodesign requirements etc.

These provisions should also require suppliers to provide you with the information you need to demonstrate the product's conformity with those requirements, such as substance content declarations and testing results, etc.

Where you are purchasing products that have already been packaged and labelled you will need to make sure that the contract requires these to be suitable for your intended markets e.g. that they provide consumer information in the correct language(s).

In the next 2 to 3 years, respondents say their greatest third-party supply chain risks will be:

**Region-specific risks**, such as the ability to comply with changes in local laws in the Middle East or Africa, sanctions against Syria and Iran, and underdeveloped laws in Southeast Asia.

20%

**Compliance with rules and regulations**, such as the FCPA, UK Bribery Act and ever expanding scope of EU product related legislation

20%

**Financial risks**, such as where the world economy is headed and whether their suppliers, manufacturers and vendors will become insolvent.

15%

**Get a commitment from your third parties that they won't buy from or sell to embargoed countries or restricted parties.**


Given the recent crackdown of some governments on terrorist activities and funding, it's important to include a provision that prevents third parties from buying from or selling to anyone on the relevant restricted party lists maintained by various governments, such as Australia, Canada, the UK and the US. Various departments of the US government, for example, maintain lists of countries, companies and individuals that constitute potential terrorist threats, such as the US Treasury Department's "Specially Designated Nationals List." The EU maintains a similar list of designated entities and individuals called the "EU Consolidated List of Financial Sanctions Targets," which applies to all 28 EU member states. The UK Department for Business, Innovation and Skills also maintains the "Iran List," which names additional restricted entities believed to be involved in the development of weapons of mass destruction.

When you are the importer of record for products you are buying from suppliers or manufacturers overseas, it's also important to include a warranty provision that requires the supplier to ensure that the product is not subject to anti-dumping duties and to provide for appropriate remedies, including the cancellation of all pending orders, if that's later determined to be untrue.

**Include breach notice provisions and check to make sure the third-party supplier/provider can pay the liability limit if a breach occurs.**


Whenever your company or customer information is involved, all contracts need to have use and disclosure limitations on that data, as well as information security control provisions. For personal information, you also need to take appropriate action depending on your industry, the type of data it is, and where it's coming from. In the US health care industry, for example, you may need to make sure your contract includes terms that satisfy the business associate agreement requirements of HIPPA and key state privacy laws. In Europe, you may have to get permission from your company's works council before outsourcing human resources functions that would involve sharing employee information.

You also want to include a provision that requires your third-party suppliers/partners to notify you immediately if there is a potential or actual data security breach. A major point of contention these days is settling on a liability limit if the third-party supplier/partner experiences a data breach. In the past, it was common for third parties to accept unlimited liability for breach of confidential information, but informed suppliers/partners will typically resist that level of exposure given more recent data security breach notification laws and the corresponding soaring costs of remediation. Once you agree on a liability limit, you should also make sure the third party has the means to pay it if something does happen. It's also a good idea to review your own insurance coverage to understand whether it covers this type of risk and how comprehensive that coverage is.



With all the regulatory changes in the countries in which we do business, the greatest risk will be ensuring that we keep up and that our third parties are doing the same.

Compliance Manager



Understanding who your supplier's suppliers are will help you manage your risk.

Penny Ward, Sydney Partner

### Keep tabs on subcontractors.

Depending on how many subcontractors your third-party supplier/partner works with, you may want to include a provision that gives you the right to approve the subcontractors that work on your project and require them to provide annual updates on who those subcontractors are. If they work with hundreds of subcontractors, it may be more feasible to require that they advise you whenever a subcontractor is involved in a product recall or other relevant legal issues. You also want to raise these issues during your annual catch-up meetings with your third-party suppliers/partners by asking whether they've changed any of their subcontractors and whether those subcontractors have been involved in issues that may affect your business. You also need to make sure that your contract states that all of the compliance requirements you imposed on your supplier/partner also apply to the subcontractors they use on your project.

"Every supplier has its own suppliers so your level of inquiry shouldn't stop at your immediate supplier," Sydney partner Penny Ward says. "Understanding who your supplier's suppliers are will help you manage your risk."

### Create a detailed exit plan.

When entering a new relationship with a third-party supplier/partner, companies often focus on negotiating the pricing, licensing and termination terms of the contract, but then neglect to finish the exit or "transitioning out" plan that lays out how they will wind up their relationship in a cooperative manner to ensure ongoing supply to the customer. The agreement will often stipulate that the exit plan will be written within X number of days from execution of the contract, but later, when something goes wrong and you go looking for it, the exit plan isn't there.

It is understandable that this often gets neglected, because writing an exit plan at the beginning of a relationship is like preparing for a divorce while you're planning the wedding. However, one of the primary reasons multinational companies seek legal counsel about their third parties is to terminate the contract, only to find it's surprisingly hard to do without the risk of being sued. In your contract, you must clearly establish the types of breaches that allow you to terminate the agreement and what steps you must take to exercise that right.

"Quite often clients ask for our advice on how to get out of their third-party arrangements because they're unhappy and we always look to see if they have the right to walk," London partner Duncan Reid-Thomas says. "You need to specify that in your contract, as well as a certain notice period or amount you must pay to sever the relationship. It's hard to overstate how important it is to get that right."



Quite often clients ask for our advice on how to get out of their third-party arrangements. It's hard to overstate how important it is to get that right.

Duncan Reid-Thomas,  
London Partner

### **Don't assume that what works in your country applies everywhere else.**

A common mistake that businesses make when expanding into new markets is using contracts governed by their own local laws without making sure those terms will be enforceable in the jurisdiction where business will be conducted. Some US companies, for example, will use their standard contract governed by California law throughout countries in Europe, then later discover that many important terms, such as termination and auditing rights, cannot be exercised in many of those countries.

"I see many US companies roll out their standard contracts with distributors, franchisees and sales agents in Europe without paying enough attention to the local regime and hurting themselves in the process," says Arne Gutermann, a commercial law partner based in Baker & McKenzie's Brussels office. "It's surprisingly common."

That's why it's so important to evaluate how much you need to tailor your standard contracts to be effective in specific countries, since local law on crucial issues such as termination, auditing and bankruptcy can vary wildly among jurisdictions. In Europe, for example, where you may not be able to automatically terminate your relationship with an insolvent third party, you can be more creative in how you structure your business arrangement and build protection mechanisms into your contracts.

If, for example, you are worried about a supplier of a critical component going bankrupt, you could consider building up an adequate amount of consignment stock that would give you a six-month cushion if the supplier went out of business. That consignment stock would be housed in your warehouse in a specially designed area, but it wouldn't become yours until you paid for it. If the supplier filed for creditor protection, you could quickly buy all the consignment stock and have it at your immediate disposal.

If you are worried about not being paid for product you've already provided to one of your distributors, franchisees or sales agents who then files for creditor protection, you can build protection mechanisms into your contracts such as requiring cash upon delivery or retention of title. In most jurisdictions, there are workarounds for major contracting issues, but it often takes local knowhow to find them.

### **Use professional legal translators.**

In countries where contracts must be translated into the local language, it's important to use professional legal translators to avoid incorrect terminology and inconsistencies that could lead to disputes over contract terms later. In some countries, it may also be helpful to have your contracts written in the same format as those in the local market so that in the event of litigation, the documents look similar to what the local courts are familiar with.

**Consider using local law or similar laws to govern your contract in markets where enforcement may be an issue.**

Many multinational companies are wary of using foreign law to govern their contracts or being exposed to proceedings in local courts, particularly those in emerging markets where the laws and legal system may not offer the same level of protection, impartiality and expediency. The problem arises, however, when something goes wrong and you try to take action only to find you can't get local enforcement. A US company may get a US injunction against its Chinese manufacturer that is making its product under its own label only to find it's possible to get the injunction enforced by a court in China. Or a German engineering company may threaten to sue one of its Indian suppliers, only to find that the supplier refuses to appear in court in Germany and the German courts have no jurisdiction over that individual. In choosing the right law to govern your contract and where and how you will resolve disputes, it can be preferable to use local law or the laws of a jurisdiction similar to those where your third-party suppliers/partners are based to improve your chances that the local courts will enforce the order or judgment. If, for example, you are a German company contracting with an Indian supplier, you may consider using UK or Indian law to govern the contract, then choose to resolve disputes via arbitration in a reputable international forum somewhere in the supplier's region, such as Singapore. Having an arbitration award that's based on laws from a legal system with similar ideas and concepts increases your chances that it would be enforced by a judge in India.

**Focus on incentives, not just penalties.**

A new trend in supply chain management is treating a third party more like a collaborator than establishing the more traditional buyer-supplier or seller-distributor relationship. This trend, often called alliancing or partnering, involves sharing the business risks and rewards of a venture based upon an agreed formula. Instead of just imposing sanctions on a third party if deliveries are late and products don't meet specifications, for example, you may give them monetary incentives or agree to increase minimum order thresholds for consistently being on time or exceeding defined quality standards.

This approach requires a high level of trust and transparency between the parties and the ability to measure soft issues such as customer satisfaction and quality to make sure the third party is meeting the goals you have agreed upon. It can, however, build more productive and cooperative supplier/partner relationships, particularly with those that provide tailored products and solutions.



Many US companies roll out their standard contracts with distributors, franchisees and sales agents in Europe without paying enough attention to the local regime and hurting themselves in the process.

Arne Gutermann, Brussels Partner



There are a lot of deals where there has been way too much arguing and not enough 'win-win' thinking.

Michael Mensik, Chicago Partner

This approach can also serve you well during pricing negotiations by helping to ease the fundamental tension between your objective to save money by outsourcing a particular function and the provider's desire to make money on that business. One way to circumvent this tension is to promise providers a major incentive if they achieve certain cost savings through innovation.

"It's recognizing that you have competing economic interests and instead of arm wrestling over whether it will be a dollar forty or a dollar fifty, you tell them if they manage this project well, you'll give them more business," says Michael Mensik, a commercial law and outsourcing partner based in Baker & McKenzie's Chicago office. "There are a lot of deals where there has been way too much arguing and not enough of that kind of 'win-win' thinking and discussion."

#### **Keep your contracts current.**

Trade regulations and commerce laws are always changing so you need to periodically review statutory and other local requirements to make sure the terms of your contracts comply with current international and local laws, rules and regulations. To keep costs down and better manage the process, you could base the review on a risk assessment in which you rate your existing contracts on a risk scale of one to five according to how old they are, what type of products they involve, and what regions they involve, and reviewing those in the highest risk categories first, before the others.

# Up the chain

As companies shift more and more responsibility to the third parties in their supply chains, the risks of that chain breaking down increase — disruptions that can significantly damage a company's business operations and financial performance. Shareholder activism, corporate social responsibility expectations and new areas of quickly developing law, such as data privacy and trade sanctions, have put companies at much greater legal and reputational risk when working with third parties.

As a result, supply chain issues have reached the board room. Corporate leaders are paying much greater attention to how these issues are managed, a reality reflected in the fact that at some multinationals, such as Kraft Foods, the Chief Supply Chain Officer now reports directly to the CEO.

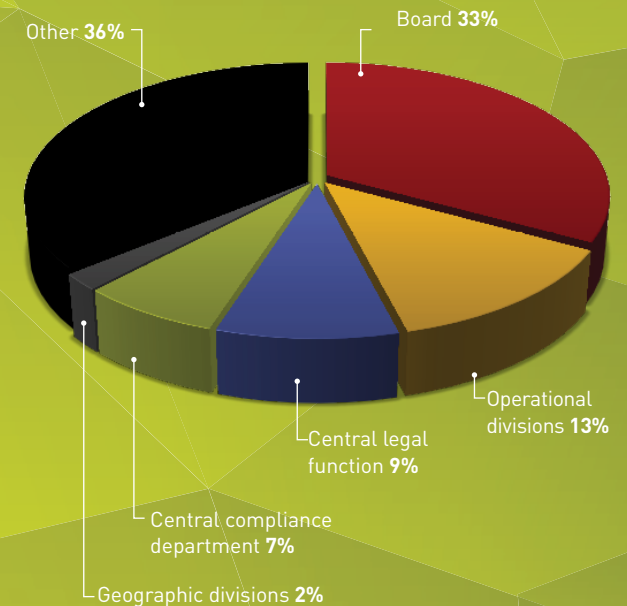
Although companies continue to struggle to create a holistic, cross-enterprise strategy for managing supply chain issues traditionally siloed in individual business units, our survey results affirm that tackling these challenges is now a significant item on the board's agenda and a major focus of corporate legal departments and global managers.

## How does your organization manage risks and compliance across its overall supply chain?

“ We have regular conferences and issue group policies on subjects such as ethics and anti-corruption. We have ethics briefings that we get all people in the organization to tune into.

Legal Counsel

### Who has ultimate responsibility for managing third-party risk?



### Who is responsible for overall compliance?





# The supply chain...



## what could possibly go wrong?

In a word, everything. One of the greatest challenges of managing a global supply chain is knowing who you are doing business with and how they operate. Who owns the company? Who are their subcontractors? Who are their subcontractors' subcontractors? And how are they all conducting business? When you're running a business with thousands of third-party suppliers and partners, it's not always easy to know the answers to these questions...

...but here are a few scenarios that illustrate why it's so important to keep track of who your third-parties are and to monitor what they are doing:

**EXPORT CONTROLS:** Let's say you're a **US** company that sells its household products in Europe through a French subsidiary. That French subsidiary sells your product to a Spanish distributor, who you think is selling your product in **Spain** and **Portugal**. Later you find out the distributor is re-exporting some of your products to **Cuba** because he can make higher profit margins. For the Spanish distributor, there is no prohibition on selling to Cuba. But for you, a US company, it constitutes selling to an embargoed country, which carries criminal penalties of up to 20 years in prison and \$1 million in fines, not to mention civil penalties of up to \$65,000 per violation.



**CONFLICT MINERALS:** You're a **US**-listed company that constructs storage tanks and processing plants for the oil and gas industry. To manufacture those tanks and processing plants, you meld together pipes and other heavy materials. Under a provision of the 2010 Dodd-Frank Act recently finalized by the Securities and Exchange Commission, you must disclose whether any of those materials contain "conflict minerals" such as gold, tantalum, tin and tungsten that may have originated from mines run by warlords in the **Democratic Republic of Congo** or any of its nine adjoining countries. The rule, which took effect in January 2013, does not ban you from using minerals from a conflict-designated area, but requires you to track and report the origin of these raw materials throughout your supply chain. That may involve going to your material suppliers, and their suppliers, and their suppliers' suppliers, all the way back to the smelters and beyond, to ask them to certify whether your pipes contain conflict minerals, as part of a compliance program that the SEC estimates will cost you \$3 billion to \$4 billion to implement. Using minerals sourced from DRC or its adjoining countries could result in unwanted scrutiny and inquiries by human rights activist groups and NGOs, as well as negative publicity.

**DATA PROTECTION:** You're a financial services company that uses call centers and data hosting providers in countries such as Costa Rica, the Philippines and India to handle customer inquiries and transactions. Those workers and providers collect and process sensitive financial data about thousands of customers. One of your providers uses a public cloud vendor to host its data, which means your customer data could be hosted on any of hundreds of servers owned by the vendor's subcontractors around the world. You later learn that a server owned by a subcontractor in the **Philippines** experiences an unauthorized intrusion. But because the public cloud environment makes it difficult to quickly determine which customer data resided on that server, you face a tough decision about breach notification. You may need to notify all potentially affected customers, as well as a wide range of state attorneys general and data protection authorities—a much more extensive and costly process than if you had been able to pinpoint exactly which data was compromised. After the notification, you may also face inquiries from the authorities about whether you failed to fulfill your obligations to protect sensitive personal data under applicable data security and privacy regulations by using a public cloud arrangement.



**PRODUCT RECALL:** You're an electronics company that discovers that some of your mobile phones on the market contain restricted substances. You must quickly determine which of your suppliers in **China** manufactured the non-compliant component, how long you've been sourcing from that factory, how many phones it affects and where those phones have been distributed to customers. The challenge is that you source the component from several different Chinese suppliers who may have outsourced the manufacturing of the components to their own vendors. If you can't trace the non-compliant components to the exact factory, batch and shipment, and contain the problem quickly, you may be subject to a wide-spread mandatory recall, a more disruptive and costly process than being able to pull a smaller number of your product voluntarily. You may also be prevented from shipping any more mobile phones until you can demonstrate to regulators that you've fully addressed the issue.

3

# TRAINING AND EDUCATING



Training third-party suppliers/partners and making sure they are educating their own employees on relevant laws, regulations, corporate policies and prohibited conduct is extremely important. It is one of the key factors that enforcement agents look at when evaluating the adequacy of a company's corporate compliance program during an investigation. Under the UK Bribery Act, for example, having a strong corporate compliance program is the only defense to certain bribery offenses, of which adequate training is a major component.

The best strategy for reducing third-party risks, according to our survey respondents, is providing more training on major compliance issues and guidance on how to identify and mitigate compliance risks.

"They have to have a robust training program so they know what to monitor and how to set up their own compliance operation," a group risk manager interviewed in our survey said.

Yet many companies fail to adequately train their third-party suppliers/partners on the key risks to look for. They also neglect to provide training often enough, conduct online training when in-person training would have been more appropriate, and fail to tailor the training to the specific business, industry and geographic issues those third party suppliers/partners are likely to encounter—all aspects that enforcement agents scrutinize when determining the adequacy of a company's training.

"We do some training of our distributors on the key risk areas, but we could do more," said a legal counsel interviewed in our survey.

Here are some recommendations to help you better train your third-party suppliers/partners and your employees who work with them.

### Train your employees on how to work with third parties based on their roles and responsibilities.

To be effective, compliance training needs to be provided to the right people on the appropriate topics. Procurement officers who vet third parties in emerging markets need to be taught how to conduct due diligence in accordance with relevant compliance standards. The account and sales managers who sign third-party contracts need to know what to include in those contracts, from both the corporate compliance, regulatory and commercial law perspective. All too often, companies find themselves in trouble with contracts that someone signed and no one seems to know why. This is often the result of the fact that the knowledge of what the legal risks are and how to mitigate them are in the compliance and legal departments, but not out in the field where business is conducted.

“Employees change, but documents stay forever,” Guadalajara partner Edmundo Elias-Fernandez says.

Training and educating should not only cover issues like what you can and can’t do under the FCPA and UK Bribery Act, but also how they interface with local anti-bribery laws that may establish different standards. Under the FCPA, for example, companies may be allowed to make facilitation or “grease” payments to a foreign official to speed up or secure a routine government administrative action. In countries like Vietnam, however, these payments are not legal. To avoid running afoul of inconsistencies between domestic and international rules, your global training program needs to account for local standards. You should also educate employees on your codes of conduct and internal risk management procedures so they know what’s expected of them, as well as what to do when compliance issues arise.

### Use your annual supplier or distributor meetings to conduct substantive compliance training.

Many multinational companies will say, “We train our suppliers,” but when asked the details of that training, it’s often not sufficient. A good rule of thumb is providing in-person training for key third parties in high risk markets for two to three hours. The training should be conducted in the employees’ native language by a lawyer (in-house or outside counsel, preferably native to the local country) who is an engaging speaker and well versed in the relevant compliance areas such as anti-bribery and corruption, antitrust, data protection, product regulation or export controls and sanctions so they can answer participants’ questions. It’s helpful to tailor the presentation to the audience by using examples of actual cases from the industry and country where they do business to make it relevant and avoid misconceptions such as, “The FCPA is a US law, it has nothing to do with us.”

In countries with hierarchical cultures, such as Brazil and China, it’s also important to have the CEO and other senior executives of your third-party suppliers/partners participate in the training by staying the whole time and asking questions. That sends a message to the employees that the training is important and gives them permission to ask their own questions.

Respondents say the best strategies for reducing third-party risk are:

**More training** on major compliance issues and guidance on how to identify and mitigate compliance risks.

**Better processes for monitoring** compliance with contractual terms and enforcing terms when non-compliance is identified.

75%

**Better protocols for screening** and selecting third-party suppliers/partners.

74%

"If the boss is there just to make opening remarks, then plays on his Blackberry the whole time, or keeps going in and out of the room, it's not only distracting but it tells the attendees that this is just a formality," Shanghai partner Michelle Gon says.

#### **Use your training and educating sessions as monitoring and evaluating opportunities.**

The questions that your employees and third-party suppliers/partners ask during training can give you valuable information about the aspects of the law they are confused about and even risky practices they are engaging in. That gives you the opportunity to explain your company policy and potentially stop illegal conduct before it leads to an investigation. Whether they are paying attention to the presentation is also important feedback. "That's why for key people, in-person training is so much better than online training," Michelle Gon says. "You get to see their reactions and learn from what they do and the types of questions they ask. If they are just sitting there playing with their phones, they are not taking it seriously. That is a red flag that they may think they can do whatever they want to after the training."

#### **Use webinars to reach a large number of suppliers/partners.**

If it's not feasible to conduct in-person training with your suppliers and partners because of their large number and geographic diversity, another option is to host training webinars. That permits broader and most cost-effective dissemination of your compliance message.

#### **Train your trainers.**

One way to save money on training is to have your in-house counsel conduct your employee training and use outside counsel to train those trainers on new developments annually. Keeping it in-house or using outside counsel who really understand your business is important because they can make the training more relevant to the participants. One benefit of using outside counsel is that it provides attorney-privilege protection in more jurisdictions, which makes it more likely that participants will speak freely.



For key people, in-person training is so much better than online training. You get to see their reactions and learn from what they do and the types of questions they ask.

Michelle Gon, Shanghai Partner

# 4

## MONITORING AND EVALUATING



One of the biggest mistakes multinational companies make is conducting thorough due diligence at the beginning of a new third-party relationship, negotiating all kinds of contract provisions to get the right to monitor and evaluate their behavior, and then never using them. Of all the five stages, monitoring and evaluating is where companies fall down most often.

“Making sure third parties are complying with international anti-corruption laws when they work on our behalf is something we continue to struggle with,” one general counsel interviewed in our survey said.

Yet survey respondents who reported implementing risk mitigation measures ranked having best practices for monitoring and evaluating their third-party suppliers/partners as one of the most effective ways to reduce risk and enhance their supply chain performance.

“It impacts our business, our reputation and our customers’ businesses and reputation if there is any weakness in third-party inputs,” another general counsel interviewed in our survey said.

Monitoring and evaluating your third parties requires making sure they are complying with the terms of your contract as well as your company’s code of conduct, local regulations, export controls, sanctions laws, and anti-corruption standards.

Here are some recommendations to better monitor and evaluate your third-party suppliers/partners.

### Conduct annual health checks.

A good first step in effectively monitoring your third-party suppliers/partners is to send them a questionnaire every year asking questions such as whether they've changed ownership, filed their required paperwork, added new subcontractors, and conducted compliance training for their employees. Many things can change over the course of your relationship and it's important to stay on top of these developments, as they may pose new risk.

"It sounds self evident but I'm surprised how often large organizations have a relationship with a distributor in some country who no one has seen, met or talked to for years," Brussels partner Arne Gutermann says. "With companies that have thousands of third-party contracts, you can see how that happens. But that third party could be doing anything. He could be re-exporting products to countries he's not supposed to."

Make sure the questionnaire you send your third-party suppliers/partners is a short checklist that covers the key risks and responsibilities in your relationship. You also want to periodically spot check the information you receive from your higher risk suppliers/partners to verify its accuracy.

If you share company or personal information with a third party, ask them to provide annual third-party audit reports attesting that they adhere to proper security standards, such as appropriate SSAE-16 reports. This will not only give you some comfort that they are following proper protocols, but demonstrate to regulators that you are fulfilling your obligation to monitor your third parties, which may be helpful to your defense in the event of a data security breach.

### Monitor for the types of risk you are most likely to face given your industry and the structure of your business.

Every industry has its own unique areas where there's a strong potential for corruption. In the pharmaceuticals industry, it could be wining and dining doctors, so you need a clear, comprehensive travel and entertaining policy. In the medical device sector, where it may be common practice for sales agents to give discounts to distributors who sell to hospital administrators, you need to watch for anomalies in those discounts or anything that creates wide margins where money could build up and be diverted to corrupt activities. Marketing and development funds are also areas to keep close tabs on.

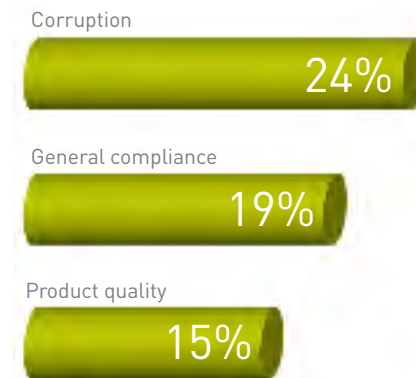
"You have to review the specific sources of trouble and red flags in your particular business," says Peter Tomczak, a corporate compliance partner based in Baker & McKenzie's Chicago office. "Time and again, businesses fail to mitigate the risk of compliance violations because they don't focus their scarce resources on the real risk they are confronting. They may have a great travel and entertainment policy, for example, but not a robust discount policy addressing greater risks with channel partners."



Making sure third parties are complying with international anti-corruption laws when they work on our behalf is something we continue to struggle with.

Legal Counsel

When using third-party suppliers and partners, respondents' top concerns are:



...particularly in emerging markets.

Their concerns also include:

Timely delivery 10%

Regional differences 9%

Insolvency risk 8%



By focusing your monitoring activities on an assessment of your actual risks, you avoid wasting money on programs that don't get to the heart of where you're vulnerable.

#### **Make sure your audit rights work in the country where you would enforce them.**

Jurisdictions vary on how willing they are to let you onto someone's property, access their records and transfer personal information. In some countries, you may be given free rein to do all these things, as long as they are provided for in the contract. But in other countries, the courts may limit your access or prohibit it altogether no matter what the contract says. If you haven't tailored the audit rights in your agreement to the local laws and culture, you may not be able to adequately monitor your third-party suppliers/partners.

#### **Conduct on-site visits every 1 to 2 years without advance notice.**

After you've gone to all the trouble to establish audit rights, it's important to use them. Your procurement, environmental, and health and safety staff should be routinely walking the floors of your third parties' factories and warehouses to evaluate issues such as working conditions, compliance with health and safety laws, and how they are safeguarding your intellectual property and trade secrets. In countries where IP theft is a major concern, you want to make sure your manufacturers keep your blueprints in a restricted area, password protect your sensitive information and give only key people access to your product specifications.

In addition to giving you the opportunity to identify problems and recalibrate your compliance efforts, these visits also send a message to your employees, suppliers and partners that you're paying attention to their actions.

"Monitoring helps deter potential wrongdoers from engaging in wrongdoing, particularly those who unfortunately are only prevented from doing something wrong by the fear of getting caught," Chicago partner Peter Tomczak says. "They need to know that you're watching."

#### **Consider the need for independent product testing.**

While your third-party supplier/partner may provide you with contractual confirmations or declarations of product conformity, you should still consider the need to have the products they make or supply you with independently tested as part of your ongoing monitoring activities. This will help to ensure that those products do, and continue to, meet the regulatory requirements of your intended market, for example the substance restrictions contained within the EU's RoHS and REACH regimes.

Respondents who reported implementing risk mitigation measures say the most effective strategies for reducing third-party risk are:

Best practices for appointment

65%

Best practices for monitoring

62%

Internal processes for monitoring

57%

Greater transparency

52%

Protocols for screening

49%

“The frequency of sampling and testing that you ultimately decide to be reasonable will depend on a variety of factors” says London partner Graham Stuart. These include your relationship with the supplier, the level of confidence you have in the supplier, their reputation and past performance, the complexity of both the product and applicable regulations concerned and the potential risks that a non-compliance incident would expose you to.

#### **Consider using outside counsel for third-party audits.**

When conducting an audit, it’s important to consider using outside counsel so that if you do get investigated, that audit report is protected by attorney-client privilege. Since these reports often contain sensitive information, enforcement authorities know that requesting copies of these internal audit reports can lead them straight to significant violations. If the reports aren’t protected by attorney-client privilege, you may have no choice but to hand over that roadmap and increase your exposure during a government investigation.

#### **Keep a watchful eye on your books and records.**

The financial teams that manage the financial relationship with your third parties need to watch for red flags that could indicate issues such as bribery or money laundering. They should be reviewing receipts and asking questions such as, “Are these expenses legitimate?” and “Is that commission to the sales agent appropriate and proportionate?” In many jurisdictions, it’s important to bring in outside counsel to conduct the investigation if you detect a major problem. That will preserve attorney-client privilege of any internal report you produce and help avoid having to turn it over if you do come under investigation.



The frequency of sampling and testing that you ultimately decide to be reasonable will depend on a variety of factors

Graham Stuart, London Partner

5

# REACTING AND REMEDYING



Surprises are rarely a good thing in third-party relationships. Nor is turning a blind eye to illegal, unethical or potentially dangerous practices you know or suspect your third parties may be engaged in. You not only have a legal obligation to monitor the actions of your suppliers/partners, but to respond appropriately to any issues that arise and most importantly, remedy the problems.

“No company is perfect and issues do come up, but how do they address them?” one compliance director interviewed in our survey said. “We look at the reputation of the supplier or distributor for taking corrective action.”

More than 80 percent of the respondents in our survey said that the risks of using third-party suppliers/parties are higher in emerging markets, particularly China, India and Africa. Their greatest concerns in these regions are corruption and political instability, two reasons why it’s so important to pay particular attention to addressing flare-ups in these countries.

Here are some recommendations to help you more effectively react to issues with your third-party suppliers/partners and to learn from your mistakes going forward.

### Act as quickly as possible.

It's human nature to ignore something and hope it goes away, especially if it's an issue that could cost a lot of money to investigate or generate negative publicity. If you act quickly, you may be able to contain and remedy the problem before it turns into a government investigation, but you must first be willing to face it. Having the ability to act quickly is also why it's so important to know who your third parties are and who they subcontract with. If you have a non-compliant product, for example, you can only avoid a mandatory recall by showing regulators that you are appropriately remedying the problem if you can quickly identify the source of that non-compliance. Depending on the size of the issue you are facing, you need to put together a plan to address it, alert the audit committee, inform the executive team and the board and retain outside counsel to preserve attorney-client privilege.

### Have contingency plans and crisis management programs in place.

To prepare for the compliance flare-ups that are bound to happen at any global organization, map out your supply chain to get a big-picture view of all the agreements you have in place, your current third-party relationships and the obligations that you're subject to. Then identify your hot spots and create contingency plans for how to react if those hot spots erupt, making sure the plans are tailored to the risks specific to your industry, geography and business. The protocols should detail who should be informed internally in the event of crises such as product recalls or bribery scandals, and the best course of action.

Consider preparing tool kits and manuals explaining how compliance issues, such as product recalls, should be handled. A lot of time can be wasted identifying and mobilising internal incident/ crisis management teams; determining the steps that must be taken in order to contain and remedy the issue and the order in which they must be taken; and deciding what communications to entities up and down the supply chain, to consumers and to regulators should say. Having tool kits or manuals in place beforehand allows you to respond more quickly and effectively, which will always be the preference of regulators, and to ensure that similar issues are handled in a consistent way across your business.

Part of crisis management is also being prepared to make tough decisions, such as severing a relationship with an important distributor or key supplier at the root of the crisis, to show enforcement authorities, shareholders and the public that you have taken the issue seriously.



Be more creative and nuanced in the different possibilities you include in your contract to remedy a situation. Otherwise you may have no other option than to continue with the supplier or terminate the relationship.

Arne Gutermann, Brussels Partner

### **Establish strong internal communications.**

The farther that decision-making gets from headquarters, the more difficult it becomes to track what's going on within an organization. That's why it's so important to build strong lines of communication between those in the field and those in headquarters by eliminating unnecessary layers of management and establishing more direct reporting relationships. Then when something goes wrong with a third-party supplier/partner, those in the field have clear channels for communicating the issue to upper management and getting direction to make sure it's quickly addressed.


### **Be sure you have the power to address data security breaches quickly.**

When a third-party provider based in another country has a data breach, it can be difficult to get to the bottom of what happened and who you have to notify. That's why it's important to seek to have provisions in your contract that allow you to ensure that the provider takes any affected database offline quickly and provides you with sufficient visibility to determine the nature and extent of the network intrusion. You also want to make sure that those provisions would be enforceable in the jurisdiction where the breach is likely to occur. Without these remedies, you could run into problems such as a third-party provider who is reluctant to provide sufficiently accurate information about the incident to allow you to determine which breach notification duties apply and how to best respond to the situation.

### **Make sure your contract gives you multiple ways to remedy an issue.**

Many standard third-party contracts give companies few choices other than terminating the relationship if the supplier/partner fails to comply with the terms of the agreement. That's a very important right to establish, given that you may not be able to get out of the contract unless you specify which types of breaches would enable you to end the relationship.

Depending on the circumstances, however, termination may not be the best way to remedy the problem. It's a good idea to give yourself several courses of action, with varying degrees of severity, such as negotiating the right to temporarily suspend the relationship without penalties if something goes wrong or the right to partial termination, which would enable you to excise only the part of the relationship that created the issue. In respect of defective or non-compliant products, you should also ensure that your contract contains provisions specifying who will be responsible for costs of issues such as handling product recalls and repairing or replacing defective or non-compliant products.



If something sounds sketchy, it probably is.

“You want to be more creative and more nuanced in the different possibilities you include in your contract to remedy a situation,” Brussels partner Arne Gutermann says. “Otherwise you may have no other option than to continue with the supplier or terminate the relationship.”

#### **Don't fall victim to claims like “This is how it's done in China.”**

In emerging markets, there's a lot of temptation and pressure to accept shady practices on the basis of “that's just the culture.” If something sounds sketchy, it probably is. To avoid this pitfall, it's prudent to investigate what the real rules are, determine whether what's being proposed complies with local laws, and evaluate your level of risk if you don't comply. Problems arise when a middle manager in the field says things like, “I know our distributor pays bribes but he's an Indian distributor and that's what they do in India.” What the manager doesn't realize is his attitude would be considered “willful blindness” under the FCPA and his company could be held liable for those bribes under the statute.

#### **Take a step back and look for patterns.**

Because of the siloed nature of global operations, a multinational company can have similar compliance issues pop up in multiple parts of the world without anyone stepping back to examine the big picture. You may have a bribery issue arise in one jurisdiction one year, and a similar problem crop up in another jurisdiction another year that may be handled by different teams within the company. If no one compares notes, you're at greater risk of it reoccurring.

“There needs to be a centralized place where people say, ‘Wait a minute, something like this happened in that other jurisdiction two years ago.’” Chicago partner Peter Tomczak says. “Companies should be frequently asking, ‘What's causing all of this?’ and ‘What are the underlying patterns?’”

Some compliance issues may well be an isolated incident. But your chief legal officer, chief compliance officer, head of internal audit and if appropriate, the board of directors should be asking these questions as part of their ongoing risk-based assessments.

#### **Use that information to revise your contracts, protocols and processes to keep the problem from reoccurring.**

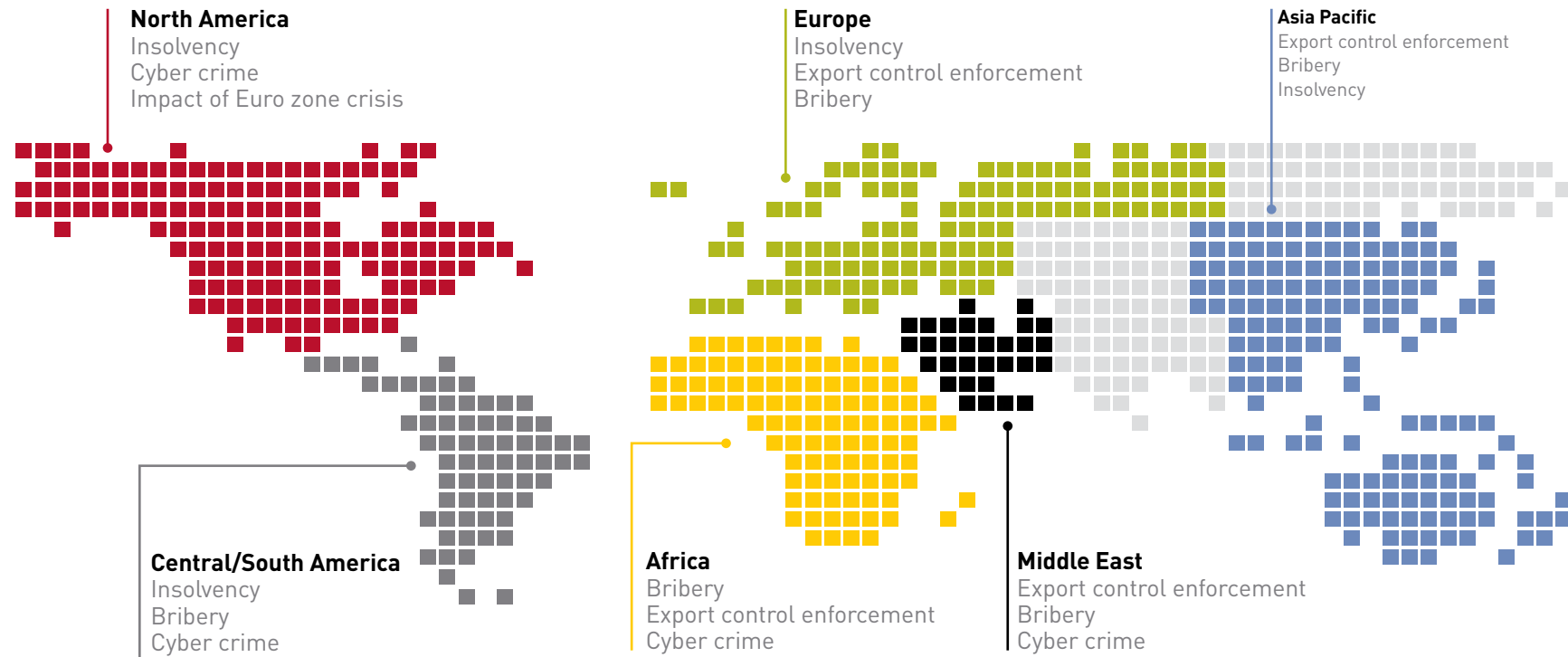
Every time you have a compliance incident, it gives you more information about where your risk exposure is, what types of behavior your employees and third parties are engaged in and what issues could get you into trouble. That enables you to take what you learned in one investigation and see if the potential for similar violations exists elsewhere. That's not to say you should investigate yourself around the world every time you have an issue, but learn from your mistakes by using them to inform how you adjust your protocols and structure your contracts to reduce your risk in the future.



There needs to be a centralized place where people say, ‘Wait a minute, something like this happened in that other jurisdiction two years ago.’

Peter Tomczak, Chicago Partner

Respondents say their greatest third-party risks by region are:





## Conclusion

Given the magnitude of today's supply chains, it can be a daunting prospect to effectively vet, select, train and monitor the thousands of third-party suppliers and partners that make up your global enterprise. It's also a major challenge to properly structure and document those arrangements and react quickly and appropriately when something goes wrong.

Besides being shrewd about approaching the commercial aspects of these relationships, companies must also find ways to manage the ever-increasing compliance aspects of working with third parties and minimize their legal exposure — a process more often an art than a science.

"What is the right level of risk that an organization should have?" asked one license manager interviewed in our survey. "We spent three to five years wondering about this. To be honest, we do not quite have it right."

With the right tools, systems, resources, attitude and insight, it is possible to gain a greater sense of security and confidence when approaching the many challenges of working with third-party suppliers and partners. In addition to his comment about the importance of reputation, Warren Buffett once said, "You can't make a good deal with a bad person." He also said, "Risk comes from not knowing what you are doing." Now that you have this framework, you are one step closer to acquiring the knowledge that will help you make informed decisions going forward.



What is the right level of risk that our organization should have? We've spent three to five years wondering about this. To be honest, we do not have it quite right.

License Manager

# Methodology

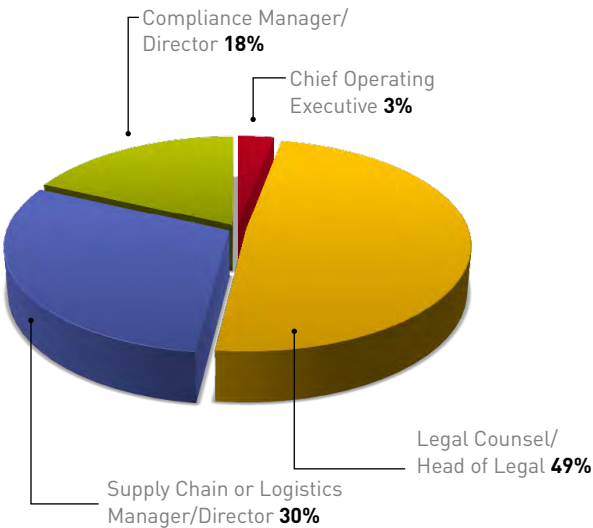
This report is based on a survey conducted by Gracechurch Consulting, a London-based research firm that Baker & McKenzie commissioned to help identify and address the key risks that businesses face when using third parties to source, manufacture, transport, distribute and sell their products around the world.

Gracechurch interviewed 100 senior executives across various industries who are involved in overseeing their companies’ global supply chains. Of those 100 senior executives, 89% are solely responsible for managing the third parties in their company’s supply chain. Nearly 80% of them are in-house legal counsel or supply chain managers. More than one-third have global responsibility; the others have a regional focus.

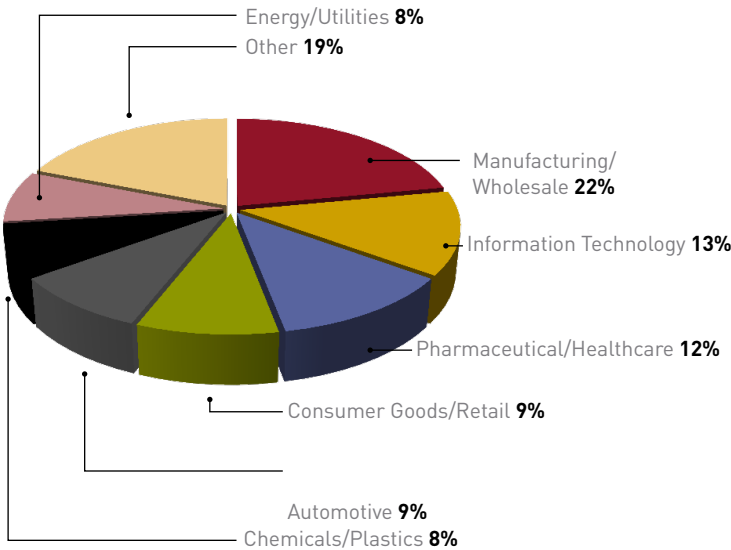
All of the executives surveyed work for companies with global footprints. The majority are involved in the manufacturing and wholesale, IT, pharmaceutical, consumer goods and auto industries. During in-person and phone interviews, they were asked to rate their greatest third-party risks, identify what helps them reduce those risks, and rank what is most important when choosing third-party suppliers and partners. The survey questions focused on the movement of goods rather than other aspects of a supply chain management, such as the flow of services, people and money across borders.

Based on the findings, we created a framework that reflects the five aspects of managing third-party relationships: vetting and selecting, structuring and documenting, training and educating, monitoring and evaluating, and reacting and remedying. We then interviewed 15 Baker & McKenzie trade and commerce partners based in Asia Pacific, Europe, Latin America and North America who specialize in the areas of concern raised by our survey respondents. Their input forms the basis for our recommendations, which aim to offer companies practical steps for better managing the third parties in their supply chains, as well as a framework for approaching the exercise more holistically.

Respondents by job title:



Respondents by industry sector:



[www.bakermckenzie.com](http://www.bakermckenzie.com)

Baker & McKenzie has been global since inception.  
Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in more than 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.

If you have any questions about this report or would like to know more about the Global Trade & Commerce Practice, contact:

Shama Perera  
+44 (0)20 7919 1853  
[shama.perera@bakermckenzie.com](mailto:shama.perera@bakermckenzie.com)