Third-Party Essentials:

A Reputation/Liability Checkup When Using Third Parties Globally

Marjorie W. Doyle, JD, CCEP-F
with input from Diana Lutz

Society of Corporate Compliance and Ethics

6500 Barrie Road, Suite 250, Minneapolis, MN 55435, United States
+1 952 933 4977 or 888 277 4977 | www.corporatecompliance.org

Third-Party Essentials:

A Reputation/Liability Checkup When Using Third Parties Globally

Marjorie W. Doyle, JD, CCEP-F
with input from Diana Lutz

Not too long ago, it was the usual practice of organizations to outsource work without a second thought. It is a strategy to solve head count issues, circumvent internal processes, or staff up quickly. It often makes good business sense to outsource when the make/buy analysis says "cheaper to buy."

What has changed drastically, though, is the analysis of what is cheaper. Gone are the days when organizations could wash their hands of liability or damage to reputation from outsourced work due to ethics and compliance failures. Bottom line: Your third party's actions on your behalf are, to a significant extent, your responsibility, just like those of your permanent employees. This is true in many risk areas, but has become equally important in relation to anti-corruption laws in the U.S., the U.K., and elsewhere in the OECD (Organisation for Economic Cooperation and Development), which apply to situations worldwide if the organization does business in any of these countries.

There is no better time than now to focus on your third parties—who they are and whether you have effective processes to control their activities on your behalf.

Who are third parties?

Any person or entity that you hire who isn't your permanent employee is a third party to you. Typical third parties are contract employees, agents, lobbyists, distributors, resellers, consultants, companies that service your products, freight forwarders, suppliers, and joint venture partners, among others. What is important is that you are paying them to do something on your behalf.

The new global expectation is that you know who they are, you have vetted them, and you are in control of the activities for which you hired them.

What are your risks?

- Harm to your reputation, even from public investigations into the third party
- Civil damages and regulatory/criminal liability

What should concern you?

- You do business with people you don't know.
- Your third parties are geographically remote from company management or in a location with little oversight or true accountability.
- Your third parties work in a different culture with different customs, language, and expectations.
- Your third parties don't know your company rules or have no incentives to comply with them.

- Your third parties want to please you in the short-term, without understanding or caring about long-term consequences.
- There is pressure to get business done without concern for how it's done.
- The global enforcement climate is currently active on anti-corruption, privacy, competition, and export-import laws.

Third-party checklist

Given this new world of expectations, the following is a checklist to test your organization's health status concerning your relationship to your third parties.

1. Do you have a list or database of all your third parties and their information?

If yes, skip to the next question.

If no, create a database that contains:

a) Name and location of third party

b) Type of service being provided

c) Location of contact and file

d) Name and position of hiring person

e) Due diligence process followed

f) Audit schedule

g) Principals of third party

h) Location of work/service performed

i) Any other information needed to manage the entity according to your policies and procedures

2. Have you done a risk assessment of your third parties and prioritized them by level of risk?

If yes, skip to the next question.

If no, develop and conduct a risk-assessment process in order to focus your program on the riskiest third parties. Not all third parties require the same level of scrutiny. Obtaining detailed due diligence on an overly broad group will consume more resources than needed and can cause delay or failure in addressing the most likely risks. On the other hand, doing only a desktop due diligence on minimal, publicly available information means that some risky third parties are not getting the scrutiny that is justified by the risk.

Some things to consider in developing the risk assessment:

a) Know which third-party tasks or representations create the greatest risks (e.g., agent dealing with government, key supplier affecting quality of product). Consider the riskiest geographic areas (i.e., corrupt areas of the world). Look at the Transparency International Corruption Perceptions Index.

b) Consider whether the service is for a critical business unit or process.

c) Consider whether the service is performed in a location with little company presence or supervision.

d) Is this a task that will give the third party access to company funds, resources, and assets?

e) Will the third party be able to obligate the company contractually or financially?

f) Is this a job that involves obtaining critical licenses, government approvals, or certifications?

3. Do you have a due diligence process for the selection of third parties, based on the risk assessment?

If yes, skip to the next question.

If no, use the results from the risk assessment created under question 2 above to tailor the level of diligence to the level of risk:

a) Classify third parties by categories of risk so the category with the highest risk requires more intense diligence.

b) Use data on services, revenue, contract requirements, location, and government contacts to create risk scores.

c) Assign a risk profile to each category. Three categories are the norm (high, medium, and low), but you can have more or fewer depending on your situation.

d) Assign an initial level of due diligence to each category.

e) Provide that individual third parties can receive increased scrutiny as circumstances dictate or “red flags” arise.

4. Once the risk categories have been determined, create a written due diligence process:

a) Have the process expressed in a written policy (or policies) with a description of all necessary procedures to implement it.

b) Specify who is responsible for implementing the policy. It might be the purchasing group or some other business position.

c) List the red flags to be aware of (discussed in item 7, below).

d) Describe the process to deal with red flags (e.g., audits, face-to-face visit at their place of business).

e) Describe how to handle existing third parties.

f) Develop a procedure for payment of expense for the due diligence process.

g) Describe the use of desktop due diligence tools, such as services that check finances and other background information, and your own questionnaires.

h) Conduct face-to-face visits to third parties who are in a high-risk category (e.g., visit to an office in Nigeria to see if a viable company exists and is operational)

i) Ask for and check references of third parties.

j) Check for conflicts of interests (e.g., a relative of a government official, if government contact is part of the services to be provided, such as licenses).

k) Outline the process for documenting all due diligence, its results, and the decisions made.

5. Once the third party has been selected based on the due diligence process, do you have a contract with the third party stating all expectations?

If yes, skip to the next question.

If no, the engagement of the third party should be stated in a written contract that:

a) states the services to be provided and the terms of compensation;

b) requires the third party to observe your organization's policies, procedures, and values that relate to the services to be provided; and that these policies, procedures, and values are clearly stated in the contract;

c) gives the company the right to audit all elements of the contract and to terminate if any elements are not met;

d) requires all employees of the third party who work on the contract to be educated regarding company standards, culture, compliance, and other requirements, and requires that they certify their understanding;

e) provides information about where third-party employees can raise concerns about anything relating to the job;

f) requires the third party to immediately report any changes in its ownership or change in structure that would affect its risk profile;

g) provides how and where payments for services will be made—specifically in the country in which the service is provided, not in cash, but under accepted financial standards;

h) requires third parties to keep proper records for review and audit;

i) requires approvals before third parties may engage sub-agents for your business;

j) includes an anti-corruption clause and an anti-retaliation clause; and

k) identifies how questions or violations are to be addressed.

6. Is there someone in your organization who is responsible for the management of each of your third parties?

If yes, good for you!

If no, consider that you would never have an employee without a supervisor for guidance and evaluation. The same goes for each third party. In fact, it's more crucial, because a third party is not subjected to the daily culture and requirements of the company.

This designated "manager" of the third party should:

a) maintain and update documentation on the third party;

b) oversee according to the degree of risk, considering the third party's tasks, financial dealings, and geographic location;

c) create and implement an audit schedule;

d) conduct evaluations of adherence to the contract;

e) stay current on changes of third-party ownership, business, legal concerns, etc.;

f) be evaluated on the oversight of the third party; and

g) be responsible for updating all information on the third party in the centralized database (described in item 1 above).

7. What are "red flags" regarding a third party?

Red flags are situations that your organization should watch out for and which should give you cause for further investigation. If they cannot be resolved to your satisfaction, they may well be reason for not selecting a party or terminating an existing third party. If undiscovered or left unresolved, these could cause you loss of reputation and resources. Examples are:

a) A representative referred by a government official

b) Someone with a lack of experience or qualifications to perform the services

c) A history of corruption in the region, country, or industry (see Corruption Perceptions Index)

d) A refusal to certify a compliance program

e) An unusually high commission or odd compensation model

f) A lack of detail on work to be performed

g) Unusual payments or financial arrangements

h) Lack of transparency in expenses and accounting records

i) Dealing with a government official instead of an agency

j) Unexplained additional third parties are brought into the transaction

k) Refusal to reveal ownership

l) Lack of appropriate staff for the work

m) Relying on someone not known or recognized in the industry

n) Using shell companies

o) Relying solely on contacts and relationships

p) Refusal to be audited

q) Providing faulty information or lies on questionnaires

r) Prior criminal or civil actions for questionable business practices

s) Requesting payment before work is completed

t) Wants to be paid in cash, off the books, or in another country than where the work is done

Bottom line

Third parties may be a necessity in today's world, but not necessarily because they may be a cheaper alternative. Your organization needs to apply the same rigor in selecting, training, and managing third parties as you do for your employees. Both hold your reputation, liability, and success in their hands. In fact, third parties who have a strong ethics and compliance program should have a competitive advantage with you, their customer.

These essential third-party elements may seem overwhelming at first, but, taken a step at a time, I've found them to streamline the process of giving your business a capability vital to your long term sustainability.

SCCE has many resources to help you, including conferences, written help, and an active social networking system where you can connect with other organizations going through the same process.

Marjorie Doyle is a Managing Director of Aegis Compliance & Ethics Center, LLP and Of Counsel, Meade & Roach, LLP. She created the ethics and compliance organization at Dupont and was its first Chief Ethics & Compliance Officer. Her expertise and interest in anti-corruption and bribery and third parties was solidified after she served as SVP, Chief Ethics & Compliance Officer for Vetco International when that company was dealing with an FCPA agreement with the US Department of Justice. Marjorie serves on the Advisory Board of SCCE and holds a CCEP-F certification in the profession. She was recognized as one of the most influential business ethics leaders by Ethisphere and is a regular speaker on all elements of a global ethics and compliance program, including anti-corruption and bribery, conflicts of interest, third parties, and policies and procedures. She works with boards of directors, all levels of management, and CECOs in creating strong cultures of ethics and compliance. She can be reached at mdoyle@aegis-compliance.com.

SCCE's MISSION

SCCE exists to champion ethical practice and compliance standards in all organizations and to provide the necessary resources for compliance professionals and others who share these principles.

Society of Corporate Compliance and Ethics

6500 Barrie Road, Suite 250
Minneapolis, MN 55435, United States

+1 952 933 4977 or 888 277 4977 (p) • +1 952 988 0146 (f)

helpteam@corporatecompliance.org
www.corporatecompliance.org