COSMOS
Navigate the Compliance Universe

Compliance Today - January 2020
Third-party vendor management: Getting started

By Calvin London, PhD; Reyna-Chris Comeros; and An Nguyen

Calvin London (calvin@thecomplianceconcierge.com) is Principal Consultant at The Compliance Concierge in Beaumaris, Victoria, Australia. **Reyna-Chris Comeros** (rcomeros@celgene.com) is the Compliance Manager, and **An Nguyen** (annguyen@celgene.com) is the Quality Liaison, Australia and New Zealand, Celgene Pty Ltd. in Southbank, Victoria.

The management of third-party vendors continues to be one of the main areas of challenge for compliance. Considering that 90% of reported Foreign Corrupt Practices Act[1] (FCPA) cases involve a third-party intermediary, and one in two global enforcement actions involve a third party, a third-party risk management program would seem to be a crucial part of any compliance program.[2]There are numerous examples of where the lack of an effective program has resulted in trouble for companies; the issues in China over several years and involving multiple companies show the importance of effective vendor management. Fresenius Medical recently settled $231 million because it devoted insufficient resources to compliance and failed to train employees or perform any due diligence of third-party agents.[3]

One of the most pertinent examples of “blind ignorance” is the Unaoil case where hundreds of international companies relied on Unaoil to secure lucrative contracts for local expertise.[4]

TheDOJ’s *Resource Guide to the Foreign Corrupt Practices Act* includes third-party management as one of 11 key topics in the evaluation of corporate compliance programs.[5] Furthermore, the DOJ endorses a risk management approach.

Adam Frey, associate managing director at K2 Intelligence,[6]has pointed out that the risk appetite and risk rating criteria for third-party compliance can maximize program efficiency while saving time and effort. Given that all third parties bring risks, and every business has a different risk tolerance, the absence of a previously established risk rating mechanism can significantly hamper any effort to achieve an effective program. This is particularly apt for pharmaceutical companies where there can often be three distinct areas of third-party management: those associated with Good Manufacturing Practice (GMP), those associated with healthhare compliance (HCC), and finally, those that do not seem to fit neatly into either of these two.

Although for many companies it may seem that having a third-party management program seems logical, and many recognize that a proactive approach is far better than a reactive one, “getting started” is a daunting task. The following discussion outlies a process that has worked well for us and enabled us to make a significant impact in the area of third-party management based on a risk assessment approach.

Getting started

The first step in any third-party management program should be the creation a master list of all vendors. In bigger companies, consolidation of vendors may be challenging. This can be done by identifying vendors that have performed a service within the last year (conservatively) that will continue providing a service moving forward. The list should be inclusive of any vendor that provides a service or product that could affect the quality of the product or service and/or the reputation of the company.

From a GMP perspective, this list would include contract laboratories, contract packaging and labeling, logistic service providers (LSP), suppliers of critical starting materials or intermediates for manufacturing, suppliers of primary and secondary packaging components and labeling, and GMP consumables (e.g., sterile product final filter manufacturers). These vendors are usually adequately covered by an active compliance program that should typically include an audit cycle, training, and monitoring components. Failure to adequately control such vendors would mean the company would not be able to effectively retain a GMP manufacturing license. As such, they are essential components of a third-party program and, by default, would be considered high priority.

The consideration and assessment of HCC vendors is a little more complex and where a risk assessment can be of true value. Vendors that generate reference material, conduct market research or literature surveys, print educational or promotional materials, process or retain company data or personal data collected from patients (for which the company is responsible), or that process or generate medical information should be included in the master list.

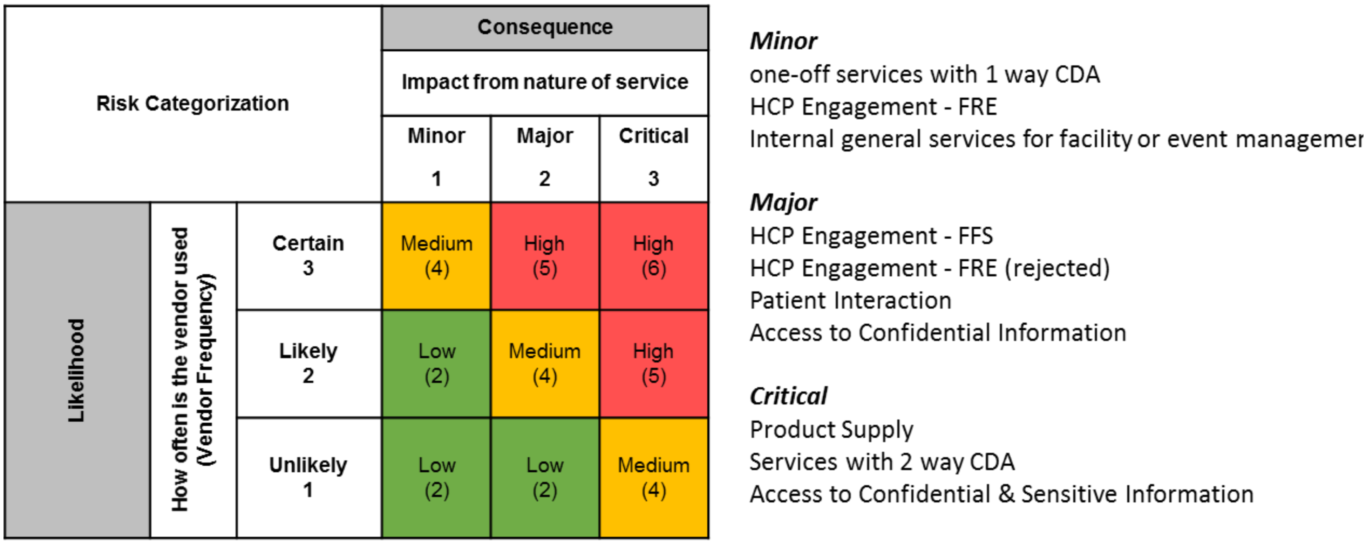
The third group of vendors are those most often overlooked, because they either span both areas of GMP and HCC or may not appear to be directly relevant to one or the other. These vendors may be commonly seen as those that provide services such as off-site archival storage of controlled documentation, retention of data in the cloud, translation of medically related documentation, event management, or management of websites. Such vendors are included in the master list, because they may have a negative effect on a company's reputation if the data was not retained appropriately or was misused, the data was involved in a privacy breach, or if the vendors engaged in acts of bribery and/or corruption.

Assessment method of risk categorization

Having consolidated all vendors into a common listing allows for a holistic review of their importance. In turn this provides the opportunity to generate a priority listing for their review. We have applied a two-step risk assessment process.

In the first instance, vendors are classified into three groups—minor, major, and critical—based on the following criteria (see Figure 1):

- Type of service provided to the business
- Volume/frequency of service provided to the business
- Due diligence around current vendor contract status
- Current internal vendor qualification status



Risk Categorization			Consequence		
			Impact from nature of service		
			Minor 1	Major 2	Critical 3
Likelihood	How often is the vendor used (Vendor Frequency)	Certain 3	Medium (4)	High (5)	High (6)
		Likely 2	Low (2)	Medium (4)	High (5)
		Unlikely 1	Low (2)	Low (2)	Medium (4)

Minor
one-off services with 1 way CDA
HCP Engagement - FRE
Internal general services for facility or event managemer

Major
HCP Engagement - FFS
HCP Engagement - FRE (rejected)
Patient Interaction
Access to Confidential Information

Critical
Product Supply
Services with 2 way CDA
Access to Confidential & Sensitive Information

Figure 1: Risk Categorization Grid

Consideration is given to more dynamic risks, rather than static risks, such as country of operation and Corruption Perceptions Index (CPI), because we deal primarily with vendors in the same country. Dynamic risks include the nature and type of business, the magnitude of business relationships, and potential transactions. This consideration can also extend to the status of the third-party executives and whether there are any current applicable investigations, any potential conflicts of interest, and/or involvement or dealings with foreign government officials.

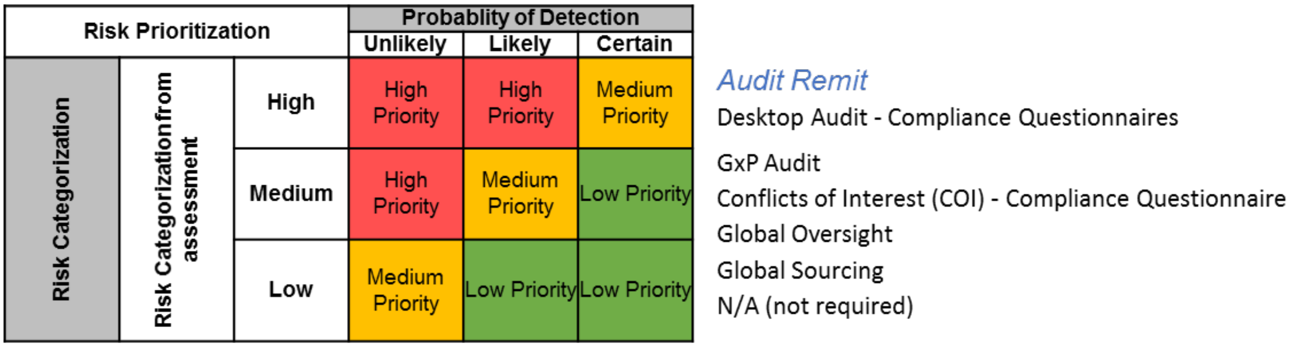
This analysis allows us to provide some categorization of the vendors. A vendor would be classified as a critical risk if they: (1) have the potential to interact on a frequent basis with healthcare professionals (HCP) who are also government officials, or (2) are a vendor that we intend to use on a frequent basis (more than three times in a year) and they also have access to senstive company data.

By contrast, a vendor that is responsible for translation of educational materials that may be used once a year with little opportunity for interaction with government officials or HCPs would be classified as a minor risk.

The purpose of this risk assessment is to provide insight into the respective importance of vendors to address those of highest risks first. It is not intended to minimize vendors classified as minor risk, although in some situations it may be that the level of review and monitoring is low. All vendors identified as critical risk are put through appropriate due diligence up to and including a red flag assessment, conducted by an independent third party, as a starting point.

Assessment of risk prioritization

The second phase involves taking each of the risk categorizations (minor, major, and critical) and assessing the level of probability of being able to detect any variations or deviations from the required processes or levels of compliance. For some vendors it will be easier to detect variations in compliance than for others (see Figure 2).



Risk Prioritization			Probablity of Detection		
			Unlikely	Likely	Certain
Risk Categorization	Risk Categorization from assessment	High	High Priority	High Priority	Medium Priority
		Medium	High Priority	Medium Priority	Low Priority
		Low	Medium Priority	Low Priority	Low Priority

Audit Remit

Desktop Audit - Compliance Questionnaires

GxP Audit

Conflicts of Interest (COI) - Compliance Questionnaire

Global Oversight

Global Sourcing

N/A (not required)

Figure 2: Risk Prioritization Grid

For example, those vendors that have an active quality system or compliance management system will have a component defining the management and process conduct for deviations or excursions. Requiring this vendor to advise if any variations occur provides some level of surveillance and ongoing monitoring for the company. In most cases, vendors (except those associated with GMP activities) will start as having an "unlikely" probability of detecting variations in compliance. A market research company is likely to have higher risk associated with the inability to detect risks. They will also require a higher degree of initial assessment and/or oversight compared to a vendor that provides retention of data in the cloud and may be more familiar with risk levels as part of required protection for integrity and data privacy.

Combining prioritization and risk to create a risk score

Summing the two aspects of the assessment (risk categorization and risk prioritization) results in an overall risk score (RC + RP = Overall Risk). This provides a classification index from which we can then prioritize in our vendor management process where the vendors of greatest importance (from a risk assessment) and the highest priority (in terms of frequency of use) are evaluated first.

Vendors found to be inadequate (high overall risk score), result in a mitigation plan that potentially includes an onsite review (where applicable) with a high-level monitoring plan. Where the risk is considered too high, we would make a compliance recommendation to not engage the vendor. Thankfully we have not yet encountered the latter.

If a vendor was found to be adequate but warranted areas of observation (i.e., medium risk score), mitigation would include performing the initial qualification/due diligence assessment, with a subsequent requalification at next engagement. For vendors identified as adequate with good controls (i.e., low risk), mitigation is limited to an initial vendor qualification/due diligence assessment that is valid for two years with a low degree of monitoring.

The levels of acceptance can be determined differently for different aspects of the business or to reflect areas of highest concerns for particular countries. For example, it is envisaged that in a country like China, a higher risk score would be required for event mangers or third-party vendors associated with venues that have been recognized as carrying increased compliance risk and burden. In another situation, there may be a greater focus on market research vendors, requiring a higher overall risk score.

Mitigation plans and monitoring

Recognizing that it may not be possible to assess all vendors in person in an acceptable time frame, the use of desktop checklists as a first assessment has proven valuable, especially where a vendor is classified as acceptable-to-low risk. Questionnaires are used to collect information from the vendor to assess the adequacy of vendor quality systems, processes, and security controls that pertain to any product, material, and/or service. The templates are developed and maintained by the compliance department and are subject to mandated reviews. Questionnaires are tailored specifically to vendor types that are frequently used, such as:

- Translation vendors
- Printing vendors
- Document destruction vendors
- Document retention/Archival vendors,
- Market research vendors
- Advertising vendors

On receipt of completed vendor questionnaires, compliance conducts an initial desktop evaluation and review based on the information provided. A vendor is deemed "qualified" if the evaluation demonstrates an adequate-to-good level of standards through implemented quality systems, processes, and security controls that pertain to the material and/or service:

- Good = High level of resemblance mirrored to our standards of internal quality systems.
- Adequate = Similar resemblance mirrored to our standards of internal quality systems.
- Inadequate = No resemblance to controls for standards of internal quality systems.

Conclusion

Adopting a risk-based approach to due diligence and third-party vendor management can help to mitigate high-level risks. Mapping out the vendor landscape and then assessing each vendor against established criteria provides a basis to at least start the daunting process of assessing all vendors, commencing with those third parties of highest risk. Establishing a foundation of qualification also provides a platform from which an ongoing monitoring program can be launched that has as its ultimate aim the prevention of corrupt behavior or noncompliant actions that could affect the reputation of the company. Prevention is always better than remediation and, in this day and age, "It was too difficult," is not an acceptable excuse to at least get started and get going.

Takeaways

- Management of third-party vendors continues to be one of the main challenges for compliance.
- Numerous examples demonstrate the lack of an effective program results in trouble for companies.
- A proactive approach is far better than a reactive one, but getting started is a daunting task.
- Risk categorization provides the opportunity to generate a priority listing for third-party review.
- Assessment of risk categorization and risk prioritization results in an overall risk score that can be used to assess third parties.

[1] 15 U.S.C. §§ 78dd-1, et seq.
[2] Anne Fleur Goedegebuure, "What can go wrong (and right) with third-party due diligence?" *TheFCPA Blog*, May 11, 2018, https://bit.ly/2qWQxAw.
[3] Michael Volkov, "Fresenius Pays $231 Million to Resolve Long-Standing FCPA Enforcement Action (Part I of III)," *Corruption, Crime & Compliance* (blog), April 1, 2019, https://bit.ly/2Qh8FzM.
[4] Nick McKenzie et al., "The Bribe Factory Unaoil: The Company that Bribed the World," *The Age, Huffington Post,* https://bit.ly/32OPJey.
[5] U.S. Dept of Justice and U.S. Securities and Exchange Commission, *FCPA:A Resource Guide to theU.S. Foreign Corrupt Practices Act*, 2012, 61, https://bit.ly/2qQzlNg.
[6] Adam Frey, "The DOJ Expects 'Third Party Management' from compliance programs," *TheFCPA Blog*, March 8, 2017, https://bit.ly/2rMLEL5.