True Detective—Lessons in Removing the Mask

This illustration is Part 2 of the Third-Party Management Illustrated Series presented by OCEG and Compliance Week. To download a copy of the illustration on the facing page fold-out and for prior illustrations in OCEG's GRC Illustrated Series, please go to www.complianceweek. com and select "GRC Illustrated" from the "Topics" pull-down menu on the toolbar or visit the OCEG website at www.oceg.org.

By Carole Switzer

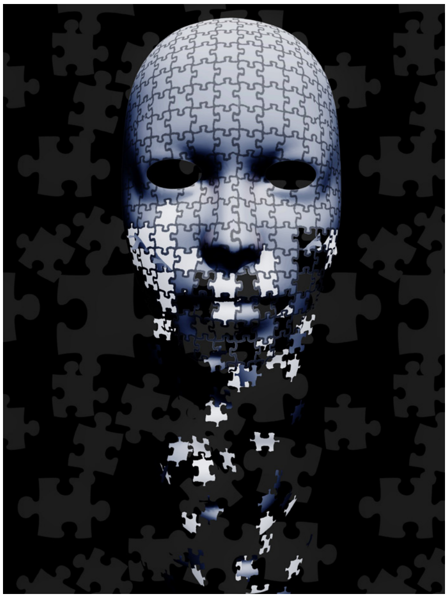
A couple of weeks ago, I spent seven hours in a marathon session watching HBO's new series, True Detective, in anticipation of the final installment. And, I must confess, this was the third time I viewed the episodes, trying to piece together more information that might let me see the true identity of the leader of a cult of masked men responsible for a raft of ritualistic killings.

And yet, I have to admit that I felt no closer to discovering the true identity of the "Yellow King," the suspected leader of this evil group, than I suspect most of you are to identifying the true beneficial owners of many of the third parties with whom you do business around the world and who are similarly masking their identities as they engage in corrupt activity.

I know it seems like this analogy is a crazy stretch, but just as Detective Rustin Cohle has to lay out the details of his analysis to his partner to convince him that there is a criminal conspiracy behind the serial murders they are investigating, let me continue just for a bit, and then see what you think.

The challenge in True Detective was three-fold: a complex and constantly changing web of information from many and often unreliable sources; deliberate deception and disguise; and an investigation hampered by manual processes that caused delay and encumbered effective analysis. The same roadblocks arise in the quest to avoid or control relationships with third parties that may present risk of corruption; in particular during the difficult and continual task of knowing with whom you really are doing business.

"Vice knows she's ugly, so puts on her mask," is the quote preceding Part 3 of the World Bank's 2011 report "The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It." The section begins with the finding that "... in the vast majority of grand corruption cases we analyzed, corporate vehicles—including companies, trusts, foundations, and fictitious entities—are misused to conceal the identities of the people involved in the corruption." Indeed, the multi-layered and hidden ownership of third parties has become one of the greatest challenges in effective management of corruption risk, leading the United States and other countries at the G8 Summit in June of 2013 to commit to creating registries of the ultimate owners of companies and enacting legislation to increase transparency.



That's a start, but unless corporate systems for tracking and analyzing multiple reliable sources of data on ownership on a continual basis are strengthened, it won't matter much. In too many companies, third-party due diligence stops at the point each party is on-boarded. Or, if information that might indicate changes in beneficial ownership of a third party is captured, it too often is not managed throughout the enterprise in a way that allows for meaningful analysis of changes in corruption risk.

Just like Detectives Cohle and Hart, who glean evidence by manually searching through box upon box of files from old cases then tack up drawings and photos on the wall and spread out handwritten notes across the floor, we might have bits and pieces of information and know that there is more to yet be uncovered, but we can't keep track of it all or see how it fits together. Just as the old case files the detectives need to review are nearly impossible to find and connections between cases go unseen because they aren't kept in the computer databases of the police force, companies can't possibly track continual changes in the use of shell companies and other forms of subterfuge that enable corrupt activity when they lack modern methods and technology to consolidate, compare, and analyze what it all means.

In the modern globally operating organization, there may be hundreds or thousands or tens of thousands of third-party relationships, each with their own extended networks of suppliers, agents, vendors, and sub-contractors. Attempts to hide true beneficial ownership and reduce potential liabilities often leads to the creation of complex, you might even say incestuous relationships, where one party owns part of another and sets up a joint venture with it that then takes an ownership stake in the first party, and so on. It is as hard to draw the family tree of these business relationships as it is to follow all of the branches of the actually incestuous family at the center of the True Detective cult.

The complexity of third-party beneficial ownership isn't an accident; it is as much a deliberate and designed attempt at disguise as is the web of secrecy and power that protects the identity of the Yellow King and members of the murderous network. To break through it, and remove the mask that hides corruption, we must be equally deliberate and design a set of processes and controls, supported by modern technology, which enables a complete and continuous view of change and allows us to see the true faces of those we are dealing with. ■

Carole Switzer is the co-founder and president of OCEG, a non-profit think tank that develops standards and guidance to help organizations achieve Principled Performance—the reliable achievement of objectives while addressing uncertainty and acting with integrity. www.oceg.org

Compliance Week and the Open Compliance and Ethics Group have teamed up to provide readers with this regular illustrated series on governance, risk, and compliance programs. For information on this series and a downloadable version of this illustration, please go to www.complianceweek.com, and select "GRC Illustrated" from the "Topics" pull-down menu on our toolbar.

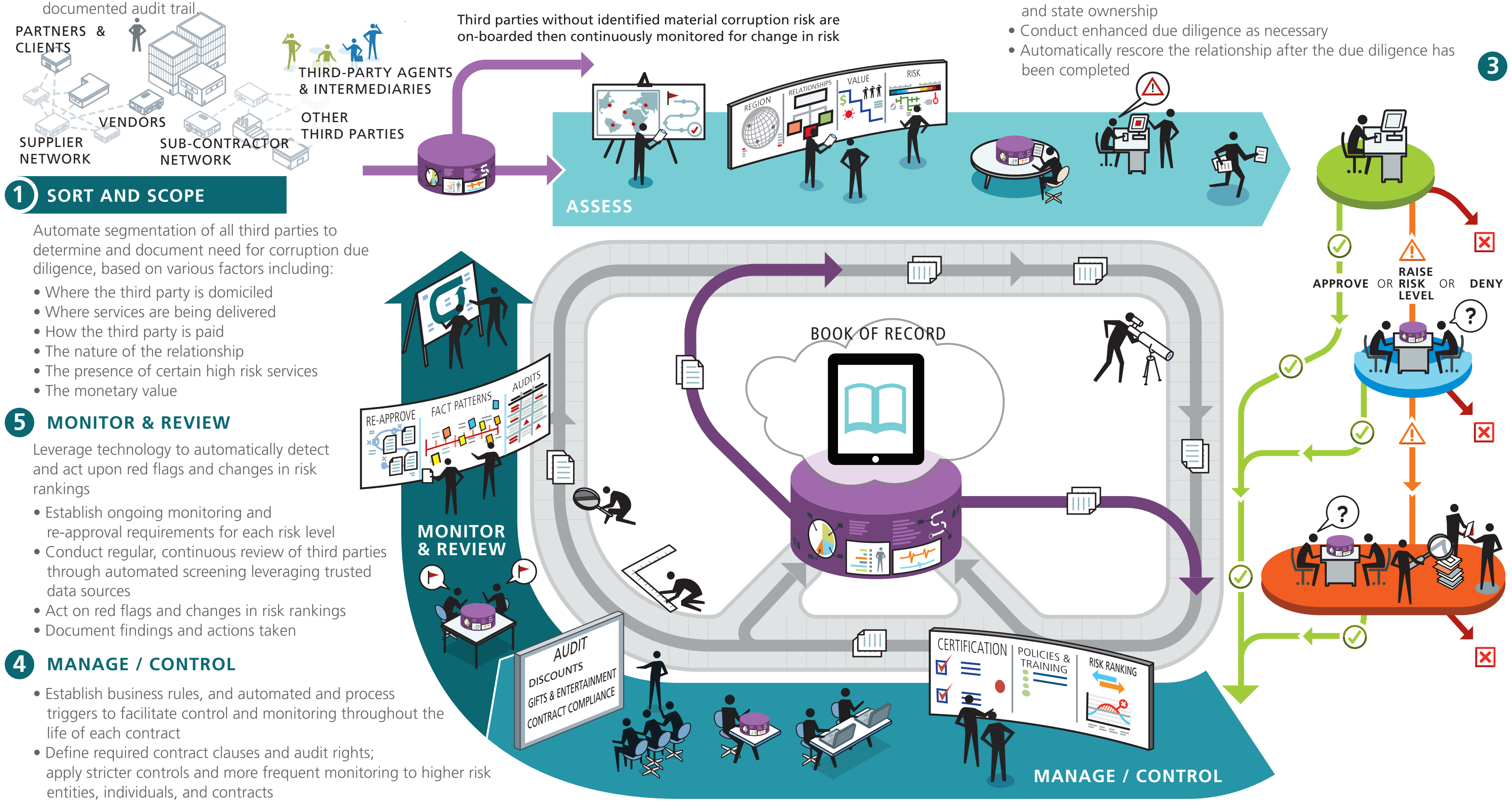
DEVELOPED BY oceg®

WITH CONTRIBUTIONS FROM hiperos MetricStream

Third-Party Management Series

Third-Party Anti-Corruption Management

Managing third parties for bribery and corruption risk requires a consistent, technology-supported approach to assessing risk, conducting due diligence and analysis, delivering training, invoking controls, ongoing monitoring, and periodic re-evaluation. A consistent method to risk score each relationship and a book of record for each third party ensures a systemic understanding of relevant information and a well-documented audit trail.



1 SORT AND SCOPE

Automate segmentation of all third parties to determine and document need for corruption due diligence, based on various factors including:

- Where the third party is domiciled
- Where services are being delivered
- How the third party is paid
- The nature of the relationship
- The presence of certain high risk services
- The monetary value

2 CONDUCT DUE DILIGENCE

Evaluate and document the level of risk for each party:

- Relationship assessment by the line of business
- Due diligence questionnaire from the third party
- Screen for disbarred individuals/businesses, political exposure, negative news, and state ownership
- Conduct enhanced due diligence as necessary
- Automatically rescore the relationship after the due diligence has been completed

3 APPROVE/DENY/ APPROVE WITH CONDITIONS

Establish low/high or more detailed risk categories, then automate scoring and document ranking, approvals, and required conditions/controls for each party. Revisit on a frequency driven by the risk score and monitoring.

LOW RISK - Level 1 Due Diligence

Trusted Data Source Screening:

Look at:

- Published convictions, penalties, and sanctions
- Politically Exposed Persons (PEPs)
- State-Owned Enterprises (SOE's)
- Negative news, public information, and social media

MODERATE RISK - Level 2 Due Diligence

Enhanced Evaluation

Level 1 activities plus consider:

- Additional trusted databases
- In-country public records
- Detailed background reports
- Interviews and questionnaires

HIGH RISK - Level 3 Due Diligence

Deep Dive Assessment

Level 1 and 2 activities plus:

- Audit and review of third-party controls and financial records
- Detailed interviews of references, political associates, business associates
- Investigative background reports leveraging local data sources

4 MANAGE / CONTROL

- Establish business rules, and automated and process triggers to facilitate control and monitoring throughout the life of each contract
- Define required contract clauses and audit rights; apply stricter controls and more frequent monitoring to higher risk entities, individuals, and contracts
- Administer training for different third-party audiences considering cultural issues and role-specific needs
- Require third-party attestation to code of conduct
- Require periodic re-evaluation appropriate for each risk level
- Document all actions and decisions

5 MONITOR & REVIEW

Leverage technology to automatically detect and act upon red flags and changes in risk rankings

- Establish ongoing monitoring and re-approval requirements for each risk level
- Conduct regular, continuous review of third parties through automated screening leveraging trusted data sources
- Act on red flags and changes in risk rankings
- Document findings and actions taken

TOP 10 BENEFITS

- ★ Protect reputation and revenues; reduce risk of litigation and likelihood of corruption
- ★ Proactively manage third-party risk consistently and objectively enterprise-wide
- ★ Demonstrate to regulators that a thorough closed-loop system is in place to continuously evaluate all third parties
- ★ Keep a clear view of the entire third-party network of your organization
- ★ Establish consistent risk scoring to apply appropriate training and controls
- ★ Ensure consistent and effective oversight and enforcement of your rules throughout the extended enterprise
- ★ Maintain an up-to-date audit trail and complete information database
- ★ Address all corruption legal requirements and organizational standards
- ★ Automate your ability to prevent, detect, and remediate risk
- ★ Reduce the cost of your anti-corruption capability and maximize human capital

CLOSE THESE COMMON LOOPHOLES

1. Assess All Third Parties

- Don't leave out those you think of as "just vendors"
- Integrate with enterprise systems to establish a closed loop that feeds every third party into the process
- Implement an automated on-boarding system to apply selection, vetting, and oversight controls

2. Manage Multi-level Relationships

- Don't stop at the business entity level; consider the individual relationships (contracts, engagements, SOWs, etc.)
- Evaluate every touch point; there may be multiple parties to a relationship from your side and from the third party, buried in different divisions, subsidiaries, geographies

3. Focus on 'Fourth' Parties

- Determine if goods and services are being delivered directly by the third party or sub-contracted to a fourth party
- Audit the controls that are in place to vet and manage sub-contractors
- Contractually require third parties to get your approval to utilize sub-contractors, potentially with conditions
- Collect fourth-party data from your third parties

REMEMBER OVERSIGHT AND ORGANIZATION

Ensure availability of resources and assignment of responsibilities and authority to:

- Develop and update standards based on legal requirements and entity values
- Define and ensure compliance with risk ranking and control processes
- Determine response and remediation when red flags arise
- Deliver reports and respond to requests for information from governing bodies

info@oceg.org for reprints or licensing requests

[AN **OCEG ROUNDTABLE**]

Managing Third-Party Corruption Risk

SWITZER: Let's start by making the point that not every third party you work with presents a risk of bribery or corruption. So how do you suggest going about determining which third parties are going to need some level of anti-corruption controls?

PATTERSON: Our customers have three initial areas of concern: First, how do I initially determine, at onboarding if possible, whether a third party could subject me to the risk of bribery and corruption? Second, how will I know if something about that third party has changed that now subjects me to risk? Third, how do I ensure that this process is being applied consistently throughout my organization? To address these, they leverage our technology solution to automatically, consistently, and objectively determine which third parties are in or out of scope for bribery and corruption risk and the level of risk involved. They can also proactively identify changes that mean the third party is now in scope, or that the level of risk has changed. The net benefit of this approach is to represent to auditors and regulators that all third parties have been or are being continuously, consistently, and systemically assessed for bribery and corruption risk in a closed-loop system which no third party can escape. The problem, for most companies, is not how to automate the performance of due diligence on third parties they already know carry risk—that is relatively easy. The real problem is knowing, with confidence, which third parties have elevated risks. For a company with tens of thousands of third parties—with whom they have very dynamic relationships—it can seem like finding the proverbial needle in the haystack! However, taking the approach of only managing presumed high risk third parties is akin to locking all of the doors at the end of the day but leaving the windows open and the key under the mat.

MARTIN: Each company must define which third parties are subjected to their FCPA due diligence vetting system. In my experience, the third-party entities that are most often subjected to due diligence by companies are commercial sales agents, customs brokers, immigration consultants, environmental consultants, joint venture partners, sponsors, and distributors who have dealings with government-owned commercial enterprises. At Baker Hughes, the key factor that we apply to identify third parties who must be certified through our FCPA due diligence system is whether those parties provide "representative services" to government-owned enterprises.

SINHA: It is important as part of initial due diligence to identify and assess the risk of bribery or corruption for the service relationship as a whole, even before looking at third parties performing those services. Our customers use our solution to support segmenting, profiling, self-assessments, internal and external validations, certifications and contract management on the basis of relationship types. This is followed by automated assessment and analysis of risk for individual third parties. This way, a weighted average scoring and mapping using risk heat maps of corruption risk is possible, thereby encapsulating both the entity and relationship risks. Having the ability to constantly monitor changes in third-party status by automating review of additional services, contract renewals, or changes etc., and aggregating information from within the organization as well as external sources is also important.

SWITZER: What sorts of training, policies, and procedures should you put in place to ensure ongoing oversight of third-party relationships that present corruption risk? Are these ranked in any way in terms of importance or risk level, or does every third-party relationship with some risk of corruption deserve the same level of control? And how do you keep track of who gets what?

MARTIN: It's important to establish controls over those in your own organization who have the third-party relationships, so we conduct a risk assessment of all aspects of our businesses to identify any job functions within the company that could potentially create an FCPA violation. We make sure those people get the right training and that they use our established policies, procedures, and processes for the identification, hiring, and ongoing management of third parties who potentially can present corruption risk in the course of carrying out their normal activities. We conduct periodic FCPA training for our people, which is both electronic and in-person in nature and which is specialized for each job category. The scope and frequency of the training in each of the aforementioned categories is proportionate to the risk presented.

While we do have numerous procedures that apply to all types of third parties, we also augment these baseline procedures with additional safeguards in situations involving what we consider to be extraordinary risks. In this regard, we would look closely at both the nature of the job category as well as the geographical location where the job is being performed. As you might expect, those countries which have a history of a greater number of corruption offenses get more focus and attention than those which have been historically less problematic. For example, we require all of our third parties to sign our standard form agreements, which contain FCPA protective language as well as having to execute annual FCPA compliance certifications. In addition, we require the third parties to provide information to us regarding their FCPA compliance programs and we conduct spot FCPA audits of some of our third parties on a periodic basis. In certain instances in the highest risk locations, we may also require that some of the key subcontractors of the third party to which we are contracting have to also be certified through our FCPA due diligence system. Finally, we also internally assign a business sponsor to each third party with the responsibility of carefully managing the ongoing relationship with that third party.

SINHA: Ongoing monitoring of third-party bribery and corruption risks is as important as the initial due diligence. We automate the periodic evaluation process with questionnaires and self-assessments and generate performance and compliance scorecards against pre-defined Key Performance Indicators. These are linked to Key Risk Indicators, enabling a risk-based approach to defining the extent and frequency of monitoring each third party. A well-designed system will link third-party processes not only to risks, but also to regulations, assets, organizations, policies, and associated controls. Control testing and monitoring improves governance, verifies access and transactional rules, and automates third-party risk-management processes.

PATTERSON: We find that ongoing monitoring of third parties and remediation of risk changes are the biggest challenges for most organizations. Our customers use our technology to help automatically and pro-actively monitor the third party—and the level of activity is directly driven by the risk associated with them. The reason that works across thousands of third parties is that the system automatically creates the due diligence roster for each third-party relationship and then continuously updates that roster as the relationship changes … all without human intervention. There are not enough people in the company to look at each relationship and decide what sort of training is aligned to the risk of that relationship. Hence, for want of an effective technology system, companies blindly apply potentially inappropriate training to large segments of their third parties because that is the only way that they can get the needed coverage. Or conversely, they limit training to a small number of "high risk" relationships.

SWITZER: A third party may work with many different parts of your organization that don't communicate with each other on a regular basis. How do you keep a clear record of the relationships or issues that might arise, and changes in risk level so that everyone is on the same page?

SINHA: Too often, the siloed approach towards managing third-party functions by different entities within the organization leads to duplication of due diligence effort and data redundancies. This really can only be avoided today by using technology that can provide a 360 degree view of each third party, from profile information such as type, category, contacts, facilities, and so on, to associated products, services, relationships, certifications, policies, risks, and controls. You want a system where this information can be both created and maintained within the application itself and imported and interfaced from one or more external sources such as the ERP system so that you can ensure good data aggregation, cleansing, merging, and de-duplication. A well-designed technology should provide reporting, analytics, and business intelligence capabilities and have role-based dashboards that let you track third-party corruption risk and associated regulatory compliance metrics and indices, leading to improved decisions based on hard facts and data.

PATTERSON: It's usually pretty difficult for companies that do business with hundreds or thousands of different third parties to be able to keep track of the different contracts they have in place with them and understand the risk of each contract as well as the overall risk of the third party. The only way that companies can effectively achieve this is by having a single "Book of Record" where every interaction with and about a third party is maintained. This includes integrating with the company's existing enterprise systems such as accounting and ERP, as well as external data sources. Technology, when implemented correctly, eliminates the usual siloed approach that challenges most companies, enables you to communicate across your company and different departments and stakeholders, and provides intelligent analytics and dashboards where you can pro-actively monitor and manage changes and look at a third party across different elements of risk. While it's hard, maybe impossible, for risk and compliance teams to fix organizational dysfunction, they can use technology to fix what today is dysfunctional communication by having one golden record—one source of truth—that keeps everyone on track. ■

ROUNDTABLE PARTICIPANTS

MODERATOR
Carole Switzer
President,
OCEG

Jay Martin
Vice President, Chief
Compliance Officer and
Senior Deputy General
Counsel, Baker Hughes

Marie Patterson,
VP, Marketing,
Hiperos

Sonal Sinha
Associate Vice
President, Industry
Solutions,
MetricStream