

INSIDE THIS PUBLICATION:

Integrated Third-Party Management

Third-Party Anti-Corruption Management

Third-Party Risk Management in Financial Services

The Building Blocks of Supply Chain Risk Management

Third-Party Management

Visualizing an Effective Capability

Getting a Handle on Third-Party Relationships

Companies have always relied on several third-party specialists and service providers to help carry out the work that they do. Vendors, suppliers, resellers, wholesalers, consultants, and many others have been part of the business equation for nearly as long as companies have existed. What is different now is how entwined those third parties can become these days. In the cases of large, global companies, it's often hard to tell where the company ends and the third parties it contracts with begin. These close relationships create compliance and regulatory risks, since the company can have legal liability—especially on the Foreign Corrupt Practices Act front—for violations by third parties working on its behalf. And even where there isn't legal liability, there is the risk of business interruption and fraud and the reputation risk that comes with working with suppliers that don't treat workers in acceptable ways.



We know that managing all those risks is no easy task, so we bring you our “Third-Part Risk Management” publication. This e-Book is a compendium of articles Compliance Week has published jointly with the Open Compliance & Ethics Group over the last few months. Here you will find all those articles, plus the roundtable discussions OCEG has run about third-party risk management with chief compliance officers and other compliance thinkers, and OCEG's famed illustrations: double-page spreads you can print out, stare at, and contemplate as you work to mitigate your own third-party risks. The articles address all the fundamentals of managing extended business relationships: business agility across the extended enterprise; third-party anti-corruption management; third-party risk in the financial services sector; managing supply chain risk; ending business relationships; and more.

Each article also has an accompanying illustration. We know the images are somewhat abstract, and they have a certain flowchart appeal to them. That's intentional. Successful third-party risk management consists of several basic principles that can apply to all, and several small details that apply to your business alone. The illustrations capture those basic principles; the articles provide context; the details we leave to you, since only you know what compliance program will work best at your business.

We hope you find our third-party risk management e-Book useful as you continue to develop and implement a robust due-diligence program. The cliché is that a picture speaks 1,000 words. Considering the huge and diverse audiences a chief compliance officer must reach these days, and the complex subject matter, visualization can only help. ■



Joe McCafferty, Executive Editor
joe.mccafferty@complianceweek.com

Inside this e-Book:

Introductory Letter	2
Business Agility Across the Extended Enterprise	5
Illustration: Integrated Third-Party Management	6
Roundtable: The Complexity of Third-Party Management	8
True Detective—Lessons in Removing the Mask	11
Illustration: Third-Party Anti-Corruption Management	12
Roundtable: Managing Third-Party Corruption Risk	14
Breaking Up Is Hard to Do	17
Illustration: Third-Party Risk Management in Financial Services	18
Roundtable: Financial Sector Third-Party Risk	20
You Are the Weakest Link	23
Illustration: The Building Blocks of Supply Chain Management	24
Roundtable: Managing Supply Chain Risk	26
About the Co-Sponsors	30

Thank you to our series sponsor:

hiperos

and to our installment co-sponsors:





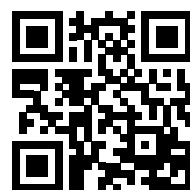
MEET YOUR THIRD PARTIES

DO YOU KNOW WHO YOU'RE DOING BUSINESS WITH?

With the majority of your revenues dependent upon suppliers, distributors and other third parties, you need to be confident who you're doing business with. A bribe paid on your watch, a data breach or a supply chain misstep could do incalculable damage to your reputation and to your bottom line.

The truth is, you cannot effectively manage what you're not measuring. Only Hiperos provides the tools and expertise to let you truly assess and manage your third parties. That's why we're #1 in third party management.

Anti-bribery & anti-corruption at hiperos.com | Or call toll-free at 844-BRIBERY



See who you might be doing business with at hiperos.com/bribery



Business Agility Across the Extended Enterprise

By Michael Rasmussen

No company is an island. Organizations are a complex and diverse system of processes and business relationships. Risk and compliance challenges do not stop at traditional organizational boundaries. Organizations struggle to identify, manage, and govern extended business relationships. The challenge is: "Can you attest that risk and compliance are managed across extended business relationships?" An organization can face reputation and economic disaster by establishing or maintaining the wrong business relationships, or by allowing good business relationships to sour because of weak oversight.

Organizations tend to look at the formation of a business relationship and fail to foresee that issues cascade and cause severe damage to reputation, and exposure to legal and operational risk throughout the ongoing relationship. They make two common mistakes:

- » **Risk is only considered during the on-boarding process:** Risks in extended business relationships are often only analyzed during the on-boarding process to validate the organization is doing business with the right companies. This approach fails to recognize that additional risk is incurred over the life of the business relationship.
- » **Partner performance evaluations neglect risk:** Metrics and measurements often fail to fully analyze and monitor risk. Often, metrics are focused on vendor delivery of products and services but do not include monitoring risks such as compliance and ethical considerations.

Organizations need an integrated approach to third-party management that brings together people, process, and technology to deliver not only efficiency and effectiveness but also agility. The building blocks of an effective, efficient, and agile third-party management program are:

1. **Define Your Program.** The first step is to define the third-party management program. While an individual needs to lead the program it also necessitates that different parts of the organization work with this role. Defining your program includes understanding board oversight and reporting for third-party risk and compliance and a cross-functional team to ensure that the operational, reputational, and compliance risks in business relationships are appropriately addressed. This team needs to work with the relationship owners to ensure a collaborative and efficient oversight process is in place.
2. **Establish Framework.** The third-party management framework is used to manage and monitor the ever-changing relationship, risk, and regulatory environments in extended business relationships. The framework starts with developing a list of third-party relationships cross-referenced to risks and regulations affecting those relationships. A framework is an organized set of controls used to measure compliance against multiple risks, regu-

lations, standards, and best practices.

3. **Onboarding.** Evaluation of risk and compliance needs to be integrated with the process of procurement and vendor/supplier/partner relations. A business relationship is to be evaluated against defined criteria to determine if the relationship should be established or avoided. When there is a high degree of inherent risk, but the relationship still is necessary, manage the risk within tolerance level by establishing compensating controls and monitoring requirements.
4. **Ongoing Monitoring.** A variety of environmental and geo-political factors can affect the success or failure of any given business relationship. This includes the potential for natural disasters, disruptions, commodity availability and pricing, industry developments, and geo-political risks. The potential risks relevant to each business partner should be taken into consideration to monitor the health and success of business relationships on an individual and aggregate level. This also involves monitoring relevant legal and regulatory environments in corresponding jurisdictions to identify changes that could impact the business and its extended relationships.
5. **Resolve Issues.** Even the most successful business relationships encounter issues. These may arise from quality, health and safety, regulatory, environmental, business continuity, economic, fraud, or legal and regulatory mishaps. The fallout from incidents is exacerbated when everyone scrambles because nobody developed defined action and resolution plans ahead of time. Management of risk across extended business relationships should account for issues and plan for containment, mitigation, and resolution.

Manual spreadsheet- and document- centric processes are prone to failure as they bury the organization in mountains of data that is difficult to maintain, aggregate, and report on, consuming valuable resources. The organization ends up spending more time in data management and reconciling as opposed to active risk monitoring of extended business relationships.

Third-party management is enabled at an enterprise level through implementation of an integrated third-party management platform. This offers the adaptability needed as a result of the dynamic nature and geographic dispersion of the modern enterprise. The right third-party management platform enables the organization to effectively manage risk across extended business relationships and facilitate the ability to document, communicate, report, and monitor the range of assessments, documents, tasks, responsibilities, and action plans. ■



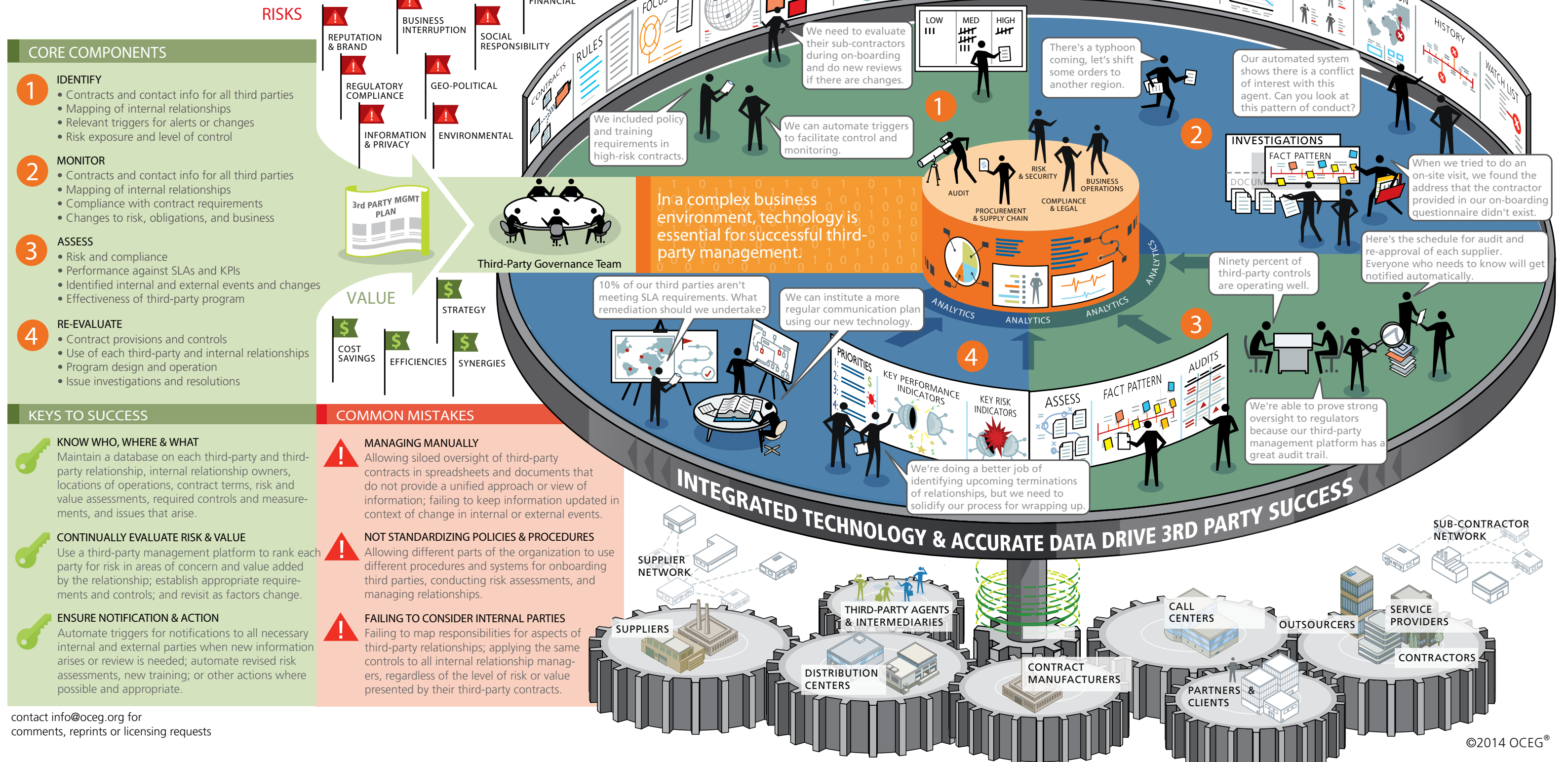
Rasmussen

Michael K. Rasmussen is a principal analyst with GRC 20/20 Research, an information technology and analyst firm. He also chairs the OCEG GRC Solutions Council and serves as an OCEG Fellow. www.grc2020.com

Integrated Third-Party Management



In today's complex economy, your suppliers, distributors, sub-contractors, agents, and other third parties play critical roles in your business success. It's too complex to manage without an integrated strategy that includes people, process, and technology. This illustration demonstrates how to protect and grow value by establishing a capability to see your entire third-party landscape with real-time information about external and internal events that may change risk profiles and impact performance.



[AN OCEG ROUNDTABLE]

The Complexity of Third-Party Management

SWITZER: Let's start with basics. How do you define and identify third parties?

PATTERSON: Third parties are any entities that are not company employees, including suppliers, vendors, sub-contractors, contract manufacturers, resellers, distributors, partners, captives, and affiliates. They represent an increasingly large portion of revenues; statistics from our customers would suggest +/- 60 percent. The challenge, for most organizations, is that they do not know with certainty who their third parties are. For companies with a lot of third parties, initial identification can seem overwhelming. Our recommendation is to approach this in three ways: (1) utilize your list of "high risk" third parties; (2) integrate with other sources—such as accounts payable where third-party payment details may be stored; and (3) given that third parties change at between 15 percent and 20 percent per year, implement a way to capture third-party details up front.

CHARLES: First, learn how business is conducted in each business unit to categorize the types of relationships. Second, identify through which business process and technology each third party is on-boarded and managed so you can aggregate historic data and define business process to capture that information moving forward. Since virtually all large, multinational corporations have grown through acquisition, they often operate globally under disparate information systems and use different terminology across regions or business units. What one part of the company calls a "vendor"

may be called an "agent" elsewhere, so they can find value by beginning with a risk inventory methodology designed to identify and define a baseline risk across the third-party population of the enterprise.

LOWRY: Sometimes companies fail to properly identify independent contractors as third parties. In general, the difference between an independent contractor who is engaging in a third-party service versus an employee is evaluated by identifying the degrees of control. For example, does the company control or have the right to control what the worker does and how the worker does his or her job? Are the business aspects of the worker's job controlled by the payer? Are there employee type benefits? If you answer no to those questions, they are likely a third party.

SWITZER: How do you identify and monitor the internal parties to third-party relationships?

LOWRY: Ideally, an organization would want a dedicated team or individual employee to maintain all third-party relationships, and specific employees should be assigned specific vendors. Prior to assigning a third-party account to an employee, there should be a determination regarding conflict of interest. There also needs to be a checks and balance system among account receivable and accounts payable for auditing purposes. This, coupled with regular external audits, is the most typical means to monitor the internal parties that oversee the third parties.

PATTERSON: Many individuals need to interact with third parties in some manner—IT, finance, HR, legal, compliance, accounts payable, procurement, etc. For the majority, the management of third parties is not their day job. The challenge is determining how you assist them to complete their third-party management tasks, ensure that they're doing so in compliance with your policies and procedures, and take appropriate steps to escalate matters when necessary. One of the big advantages of technology is that it automates this process and enforces your corporate policies and procedures in a way that's consistent and objective across the organization, while aligning the correct persons within your organization with individuals at the third party.

CHARLES: For legacy relationships, working with your data warehouse is key; if that role doesn't exist then integrate a systematic process with an existing on-boarding process. We recommend using a Business Justification questionnaire in the onboarding process, which is completed by an employee or business sponsor. This process acts as a traffic cop and provides proper categorization and an initial go/no-go decision. You reduce your exposure by reducing the number of third parties being on-boarded and identifying potential red flags before a third party intermediary begins conducting business on the company's behalf. You can continuously monitor your third parties by having a recurring certification process that incorporates input from the business as well as transactional data

that helps define risk-based performance.

SWITZER: Do you recommend particular policies and procedures for oversight of third parties based on their risk ranking?

CHARLES: We recommend applying a credible risk-based approach and model not only for due diligence, but also for contracts, training requirements, and certifications. Varying degrees of risk require varying degrees of controls and processes. Managing this using a spreadsheet is impossible: you need to use a system to prescribe and monitor requirements, and drive the process out through the business in an automated fashion. According to the Justice Dept./SEC Resource Guide "performing identical due diligence on all third-party agents, irrespective of risk factors, is often counterproductive"—as a result, we encourage a risk-based due diligence approach to the ongoing oversight of third parties utilizing a robust risk model based on a company's risk appetite. Based on the risk calculation, third parties should be associated with a risk profile and tier that has a prescribed scope of due diligence. That due diligence could include ABAC training, a due diligence questionnaire, evidence of qualification, external due diligence, and so on, based on the type of third party and their associated risk score.

LOWRY: Third-party relationships should have a base level of control and oversight to ensure that risk is mitigated. For example, there should be a period of due diligence to check for conflicts of interest, reputation, and ability to perform the task. And once a third-party is approved as an appropriate vendor, they should be required to comply with certain company policies such as a code of conduct and safety policies and enter into contracts with certain standardized clauses. Organizations also should have a third-party invoicing policy that requires invoices to contain certain information and go through a multi-person approval process before being paid. Then, some third parties absolutely should receive a higher level of control based on their level of access and risk.

PATTERSON: Policies and procedures are essential. Specifically, understanding what

your policies and procedures are and knowing when they apply. Not only does every third party not require the same level of controls, organizations also need to understand what business they're doing with a particular third party, considering the specific contracts, engagements, statements of work, consulting engagements, etc., and implement controls at

conduct additional due diligence on those sub-contractors of the highest-risk third parties, as required. Establishing requirements for your third parties' third parties poses business and legal challenges. Some of our clients have implemented monitoring processes that provide visibility both upstream and downstream, but mitigate risks around control. Using technology,

"Third-party relationships should have a base level of control and oversight to ensure that risk is mitigated."

Autumn Lowry, Manager, Investigations, Convercent

that level. The challenge for companies is that they are dealing with so many third parties and the requirements for initial and ongoing due diligence is unique for each. Again, depending on the number of third parties, this is impossible to manage manually, which leads to companies not completing appropriate due diligence or never updating it. The beauty of technology and automation is the ability to apply appropriate controls based on specific circumstances.

SWITZER: How do you control what your third parties do in terms of their own agents and suppliers?

PATTERSON: In certain industries, such as banking, the management of sub-contractors is required by regulators, but everyone needs to understand whether goods and services will be delivered directly by the third party or by a sub-contractor to appropriately manage risk. For example, one of our customers found that a number of their third parties were actually all using the same sub-contractor, creating consolidation risk, so they increased the risk ranking of these third parties, put additional controls in place, and identified additional sources.

CHARLES: Each regulation has varying degrees of expectations around how far your span of control and liability extends. Knowing that boundary is important. Asking third parties to identify their sub-contractors as part of the due diligence questionnaire allows the company to

they have been able to define the depth of control using customized workflows that are intelligent and only collect information and require certifications (including annual re-certifications) for relevant relationships. While it is commonly suggested that companies require audit rights in their agreements with third parties as a means of monitoring the third party's commercial activities on behalf of the company, this is only advised if the company plans to exercise those audit rights. Having audit rights as part of a compliance program and not using them increases your legal exposure and makes the program less credible than not having them in the first place.

LOWRY: You can contractually require third parties to perform certain monitoring or training of their own contractors, but this is very difficult to enforce even if they agree to the terms. Best practice is to have contractual language with third parties that requires them to consent to regular audits and comply with any internal investigations, and then to conduct those audits. The contract should explicitly note that they are providing a third-party service and are independent contractors and all work could be subjected to inspection. And the contract should have some wording that work which may present certain risks cannot be sublet without written consent. Lastly, organizations should require the third party to notify the company in the event of any lawsuits or claims served on the third party related to work performed by them or their own third parties. ■

ROUNDTABLE PARTICIPANTS



MODERATOR
Carole Switzer
President,
OCEG



Tony Charles
Senior Director,
Strategic Development,
STEELE



Autumn Lowry
Manager,
Investigations,
Convercent



Marie Patterson,
VP, Marketing,
Hiperos

With MetricStream...



A Leading Hi-Tech Manufacturing Company consolidated Conflict Minerals, Supplier Survey management across its supplier base



Fortune 100 Pharmaceutical and Health Care Giant simplified its Supplier Risk Assessments across more than 150 global sites



An International Banking and Financial Services Conglomerate strengthened its 3rd Party On-Boarding and Due Diligence across a wide vendor base



A multinational energy corporation implemented a robust anti-bribery program for FCPA compliance



One of the World's Largest Consumer Goods Manufacturer streamlined its 3rd Party Risk Management across 80 countries

What can we do for you?

For a Live Solution Demo
Call: +1-650-620-2955
Email: info@metricstream.com

MetricStream GRC Solutions

Third Party

- Third Party Management
- Third Party On-Boarding Management
- Third Party Risk Management
- Third Party Due Diligence

- Compliance Management
- Regulatory Change Management
- Policy Management
- Risk Management
- Quality Management
- EHS Management
- Ethics & Corporate Compliance
- Case & Issue Management
- Audit Management

MetricStream
www.metricstream.com

True Detective—Lessons in Removing the Mask

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.

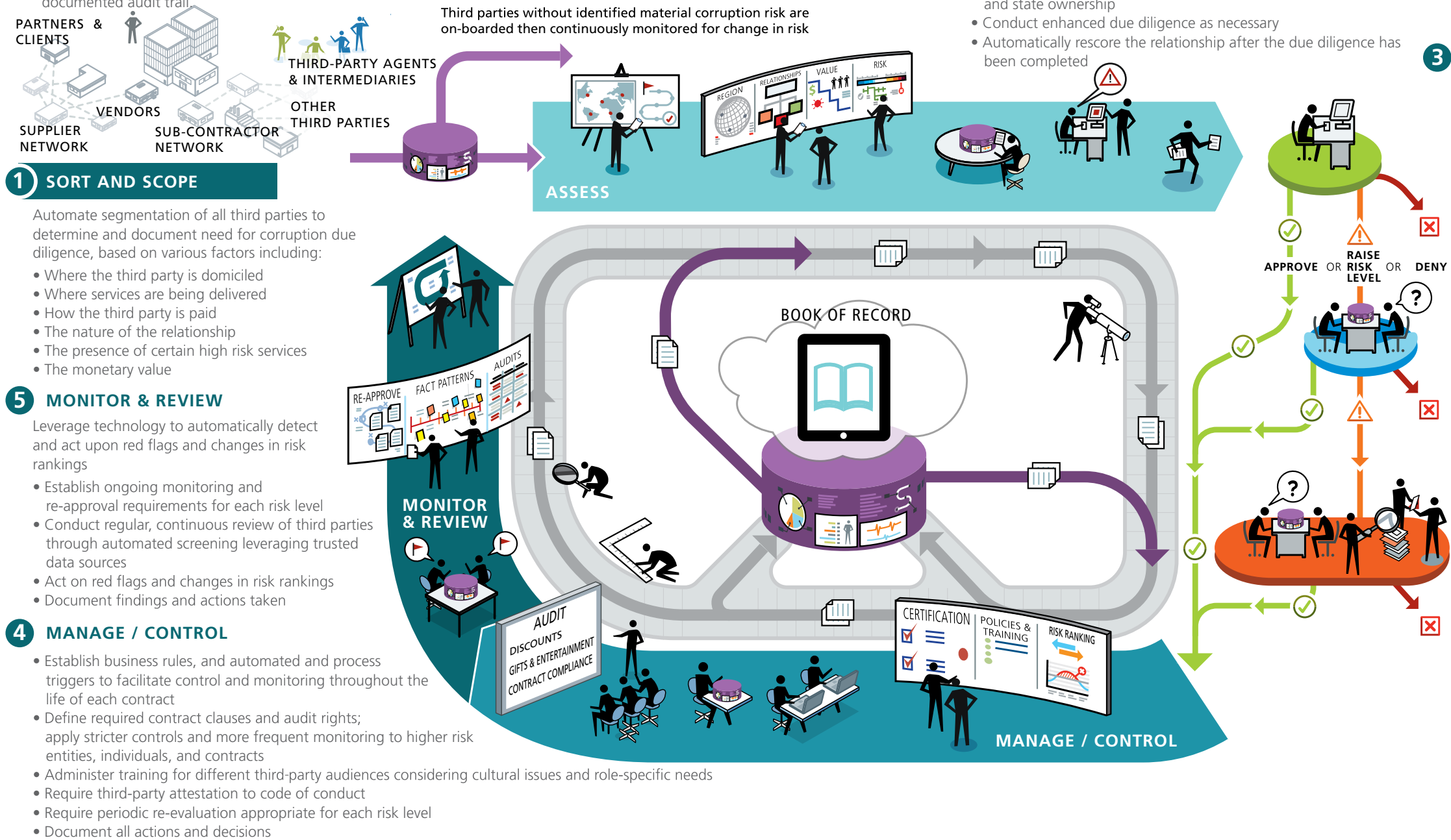
The complexity of third-party beneficial ownership isn't an accident; it is as much a deliberate and designed attempt at disguise as is the web of secrecy and power that protects the identity of the Yellow King and members of the murderous network. To break through it, and remove the mask that hides 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

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.



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

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

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

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

[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 proactively 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 up-

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

“... 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.”

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

dates 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

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



BECAUSE YOU CAN'T BE EVERYWHERE. WE ARE.

**800 SPECIALISTS. 170 COUNTRIES. ONE MILLION INVESTIGATIONS.
OUR EMBEDDED THIRD-PARTY EXPERTS TURN COMPLIANCE INTO CONFIDENCE.**

To successfully identify and mitigate corruption risks, you need compliance investigators and analysts who speak the language. Who know the business customs. Who can skillfully navigate in-country intelligence and data privacy regulations. STEELE's professionals are this rare breed. We deliver prompt and accurate due diligence that proactively identifies risk to avoid costly violations and business disruption. When compromise isn't an option, our professionals, powerful online compliance solution, and over 20 years of industry leadership translate into an unmatched third-party program that stands up to DOJ and SEC scrutiny.

Leverage STEELE's in-country expertise by downloading
STEELE & ACC's China Compliance Series, at steelecis.com/china6.

STEELE
COMPLIANCE & INVESTIGATION SERVICES

Breaking Up Is Hard to Do

Avoiding Pain by Planning for the End of a Third-Party Relationship

By Carole Switzer

Paul Anka crooned, "Breaking up is hard to do" as he begged his love not to leave him in one of his most famous songs, but alas, we all know that relationships often come to an end.

By contrast, management guru Peter Drucker cautioned "begin with the end in mind," and even though it isn't as romantic a sentiment, it is good advice whenever you enter into a new business relationship.

Call it an exit strategy, a transition plan or a pre-nup—whatever the title, it's best to begin by planning for the end which, in the case of business at least, will always eventually come. Whether due to contract completion or material breach, turning over responsibility to another party, or abandonment of the contracted activity altogether, contract termination is an inevitable phase in the third-party relationship lifecycle.

As many risks as there are in the active phase of a third-party relationship, there are some that remain and also new ones that arise when the relationship is ending. The more long term and layered the relationship, the more difficult it will be to disentangle. The deeper the third party is embedded in and uses the confidential information of the company and its customers, the greater the risks presented by failing to design a smooth transition process.

Probably the most difficult transitions arise in information technology contracts. Just take a look at one legal case that came about because there was lack of clarity in a master service agreement and you'll begin to sweat as you wonder how well your own contract termination provisions protect you.

Back in 2011, pharma giant Astra Zeneca announced it was terminating a contract with one of its major IT outsource partners, IBM, for cause. Reportedly, Astra Zeneca was dissatisfied with the services that included server and storage hosting, desktop management, network maintenance and management and help desk support for AstraZeneca's 61,000 employees in 60 countries.

Despite having a very long and detailed contract, it turned out that the key term "shared infrastructure" was not clearly defined, leaving the court to conclude that it included equipment, systems and facilities at IBM's shared data centers worldwide, and requiring IBM to provide more services during the agreed upon termination term than it believed it had agreed to extend for a fixed price. While Astra Zeneca won this dispute, just think about the stress caused by not knowing for sure that it could continue to serve its customers well during the contract transition to another provider if the decision had come down the other way; not to mention the cost of the litigation.

The risk of business interruption is important, but

it is not the only issue to be addressed in a termination plan.

- » The risk of cyber-security breaches must be addressed by having clear procedures and requirements for data retention or destruction, termination of access control for shared technology, and removal of system connectedness, including consideration of what fourth parties (your third party's third parties) may have.
- » Competitiveness and corporate value must be protected by clearly designating the disposition of shared intellectual property and infrastructure assets.
- » Smooth transition must be planned for by ensuring rights to hire or continue use of key contractor employees who have been servicing your account, arranging to bringing new contractors or internal managers up to speed, and filing any regulatory or other required notifications.
- » Reputation must be protected by controlling and planning for issuance of public statements and social media postings by terminated contractors or their employees, or the best laid transition plans may be for naught.

An effective termination plan starts with, but goes far beyond, the establishment of well thought out contract clauses for various types of third-party relationships. To work out a smooth transition, the plan must also include internal change management processes and policies, designated transition team members, contingencies, and adequate resources and time allowances.

The need for a well-developed termination contingency plan is recognized by the U.S. Treasury Controller of the Currency (COC) in updated guidance on third-party management issued in October of 2013 (available at OCC 2013-29). The COC outlines contract terms to address termination rights and process, including a provision for ongoing monitoring of the third party after contract terms are satisfied. The guidance also states that companies must have a termination contingency plan addressing the capabilities, resources, and time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.

It really is not unlike a break up of a personal relationship. Not only do you need to define who gets what of the shared assets, you also need to plan how you will continue to operate in your daily life and what you will say, or not say, about each other in public. But in the business relationship case, the tension between what's practical and what's romantic doesn't come into play, so waiting to make your plans until you are in the throes of the relationship "divorce" shouldn't ever be an option. ■

Third Party Risk Management in Financial Services

Banks and other financial services providers have increasingly complex relationships with third parties both at home and abroad. As outsourcing of key functions, sales and customer relations expand, and third parties themselves turn more to the use of subcontractors, the risks presented become more complex. Companies that use an integrated technology based management system can establish effective control throughout the third party lifecycle.

DEVELOPED BY

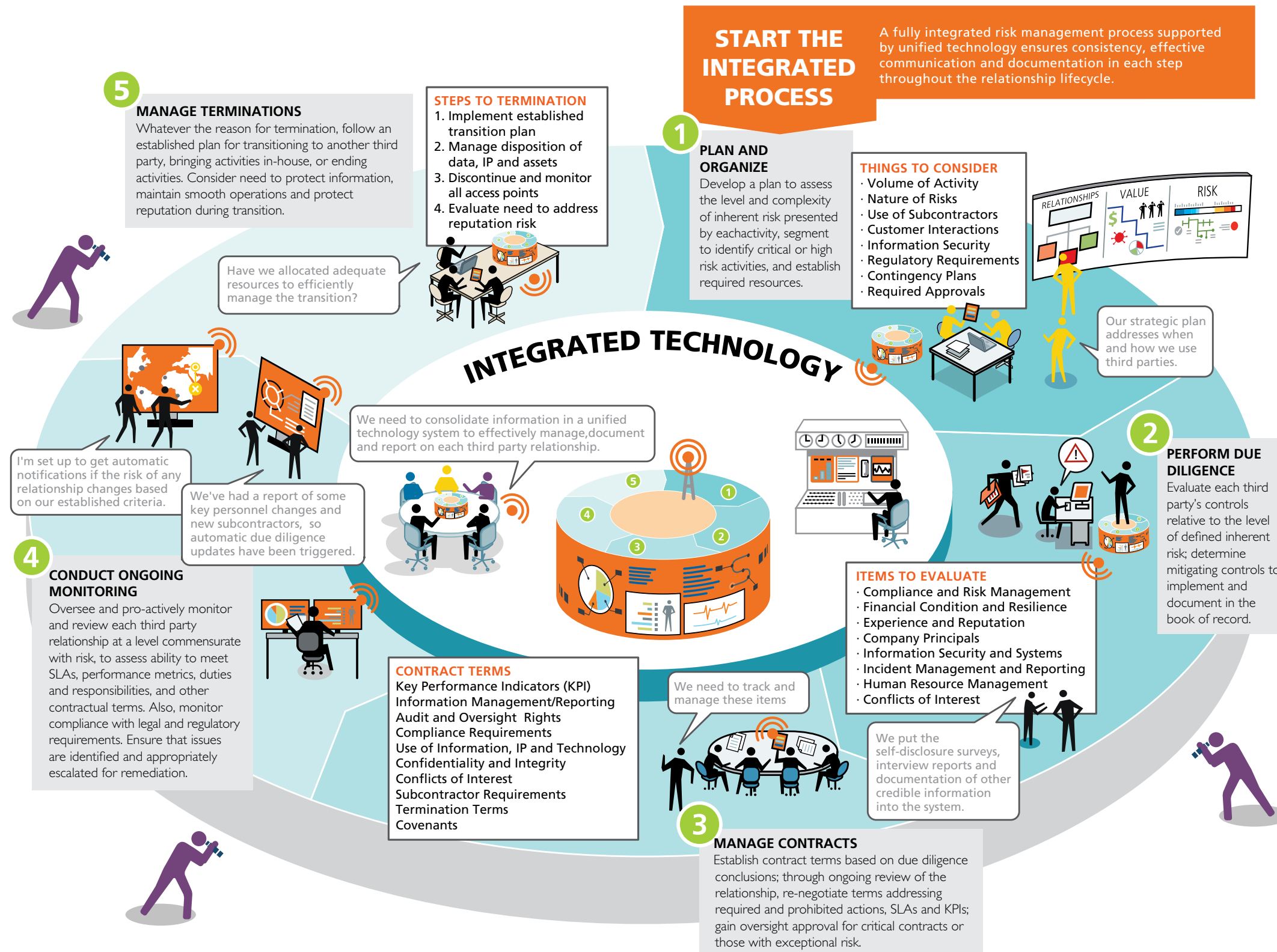


WITH CONTRIBUTIONS FROM



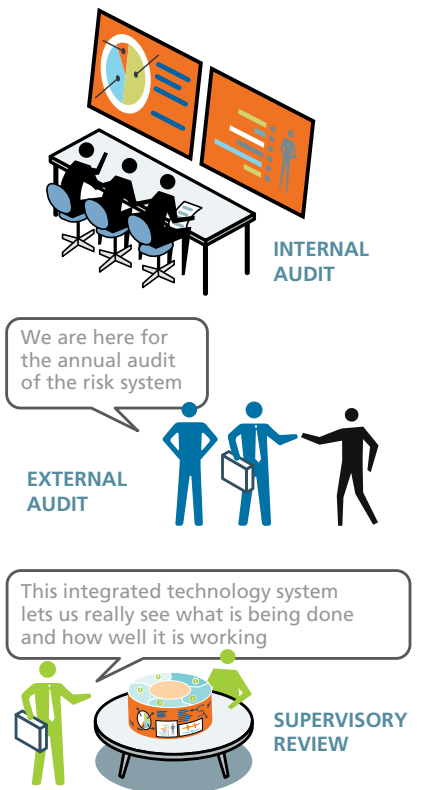
OVERSIGHT & ORGANIZATION

Clear accountability and authority provide a "line of sight" from the boardroom to frontline operations. Qualified personnel must be responsible for program oversight, strategy and operation. Third party risk management responsibility should be "baked-in" to lines of business so that all executives are accountable. Communication between all functions should be frequent and ongoing.



INDEPENDENT ASSESSMENT

Conduct independent review of the risk management system design and operation to ensure alignment with organizational strategy and effective third party risk management. The level of assurance desired will determine the scope and frequency of internal and external audit. Assessment also enables preparation for supervisory review.



DEFINING THE THIRD PARTY RELATIONSHIP

- Outsourced products and services
- Independent consultants
- Networking and joint ventures
- Merchant payment processing
- Affiliates and subsidiaries
- Other business arrangements

[AN OCEG ROUNDTABLE]

Financial Sector Third-Party Risk

SWITZER: Let's start with what seems like a simple question but isn't really: Who or what is a third party for a bank or other financial institution or lender?

SPEARS: Merriam Webster states, "a third party is someone who is not one of the two main people involved in a legal agreement but who is still affected by it in some way." At times companies need to share information with third parties to facilitate a transaction, which poses various levels of uncertainty from both the company and the consumer perspective. This uncertainty is the risk that peaks our attention.

PATTERSON: A third party, per the OCC, is "any business arrangement between a bank and another entity (that is not a customer), by contract or otherwise." So while vendors and IT providers fall into that category, "third party" must also include any contractor, broker, sales agent, franchisee, networking arrangement, joint venture, correspondent bank, marketing partner affiliate, or subsidiary as examples. Historically, banks have focused on their "supply chain"—vendors providing goods and services to support a bank's operations. Recent guidance and reports from different banking regulators have made it very clear that they're concerned with a bank or regulated entity's ability to understand and manage the risk across their ecosystem. OCC Bulletin 2013-29 issued in October 2013 is very explicit that the entire risk-management framework applies not only to vendor relationships but to all third-

party relationships within the value chain.

HOOGMOED: Third-party risk is the exposure that an organization has inherent to the business because the organization is leveraging a third party to execute or deliver upon a product or service. For example, if a bank is highly dependent on a service provider for credit card processing, the bank is subject to the potential exposures of the service provider, including whether the service provider is financially solvent, whether the operations/processing could be disrupted and have significant effect on the bank's customers, and/or whether the service provider is complying with local laws and regulations.

SWITZER: What is driving a deeper focus on third-party management in the financial services sector right now?

HOOGMOED: As financial services institutions focus to reduce operational costs, deliver innovative products/solutions, and leverage scarce talent, etc., the use of third parties continues to be a key component of business strategies. The recent third-party management guidance from the OCC and Federal Reserve has provided additional considerations for more comprehensive and standardized management capabilities. Non-compliance with certain laws and regulations in the credit card and mortgage businesses has increased sensitivity. Significant losses of confidential data have heightened awareness for the importance of how third parties protect the bank's

data. The complexity of third-party relationships is a growing concern, including the number of third- and fourth-party relationships or sub-contractors that are involved in the supply chain of a service or product.

SPEARS: Per the Bureau of Consumer Financial Protection, part of an effective compliance management system (CMS) is for businesses to adequately oversee affiliate and third-party service providers. In my opinion, businesses have a number of pressures from consumers, internal business partners, and regulatory bodies to establish and maintain appropriate ways to properly oversee third-party service providers in order to reduce overall risk. This is a very complex task that requires developing risk-based policies and procedures to manage the lifecycle of each individual third-party service provider relationship.

PATTERSON: The comptroller of the currency summed it up in his introduction to OCC 2013-29 when he said that the regulators "have concerns regarding the quality of risk management on the growing volume, diversity, and complexity of banks' third-party relationships, both foreign and domestic." Use of a third party does not absolve the institutions of obligations to ensure prudent conduct of operations, including business continuity, disaster recovery, and termination strategies. There also is concern about data protection. Whether it is protection of personal information of employees or consumers, or con-

fidential information of customers or the bank itself, it is imperative that the bank ensures the third party has sufficient controls in place to protect the data it will access. Finally, it's about ensuring protection of the consumer. If a third party utilizes inappropriate marketing techniques or coercion on a consumer and misrepresents the facts to induce a consumer to take action, the bank for whom they are doing so will be held liable.

SWITZER: One key issue is the need to address so called fourth parties—those entities that your own third parties may outsource to or use for certain tasks. How do you address this issue and keep it from becoming a rabbit hole?

PATTERSON: If the third party is going to sub-contract work, the bank needs to ensure that the third party has adequate controls in place to assess and manage their sub-contractor risk and that the bank has the ability to terminate their relationship with the third party in the event there is an issue with the fourth party. The regulators don't expect banks to perform the same level of due diligence on fourth parties, but if a problem occurs with a fourth party, the bank will be held responsible. So they need to have sufficient visibility to ensure compliance.

HOOGMOED: It is important to consider that businesses are highly interdependent with each other. There needs to be more awareness and transparency to the exposure that an organization has to these interdependent relationships. Third parties, such as major fourth parties, often have a set of third parties that enable the outsourcer's business. For example, it is the bank's responsibility to understand which of those outsourcers support the bank's outsourced processes, particularly those supporting critical bank processes. Similar to manufacturing and consumer products industries, the bank is dependent on this 'supply chain,' not just a given third party. With that being said, contract provisions should be enhanced for clarity of controls and liability, approvals for serial outsourcing should be implemented, and selective

testing for fourth/fifth parties should be considered. There may be some lessons learned from non-FSI industries, such as the automotive industry, where shared investments are made to establish a set of pre-qualified and certified third/fourth parties for a given critical product/service.

SPEARS: Due diligence coupled with a strong legal contract team are crucial. It is very important to develop a minimum standard, in the contract with the third party, to ensure that the third party only does business with fourth parties that meet the first-party requirements. The first-party business has everything to lose and has to understand who the fourth party is, understand their business credit risk, inquire about their transactional risk, consider the overall compliance risk, and require a minimum level of liability insurance to indemnify the first and third-party businesses harmed as a result of any wrongdoing. The provisions should include that no sharing beyond a fourth party is allowable. The last critical point of this is to ensure that the first party adds a mechanism for accountability. This mechanism is what prevents this from becoming a rabbit hole.

SWITZER: The OCC guidance goes into quite a bit of detail about third-party risk-management practices. What is most important?

SPEARS: This bulletin really has a lifecycle perspective in the detail noted throughout the document. While I think all parts of this plan are very important to successful third-party management, having a solid plan for setting the tone with third parties is key. Maintaining that standard throughout your due diligence, negotiating, and selection process are critical elements of a great start. Operationalizing your business message through performance monitoring while documenting and reporting are not easy tasks. OCEG's illustration on the topic gives some great guidance on how to properly overcome this plateau. Finally, managing terminations are just as important as all of the other steps. You must plan and act accordingly.

HOOGMOED: We think that the full inventory and understanding of the third-party relationships that an organization maintains is very important in order to understand the magnitude and dimension of exposure the organization has to its third-party portfolio. Developing some advanced risk tiering and assessment methods will help organizations focus their limited resources on managing the risk, compliance, and controls on the most critical/highest-risk relationships. Engaging senior management in the risk analysis and reporting is also very important to balance the appropriate level of risk taking with the costs and investments necessary for the business. Ultimately, the business leadership and business managers should own the risk decisions for their operations/products. Third-party risk is just another area of exposure that business managers need to manage as part of their day-to-day activities. There is some déjà vu with where we were with information security a few years ago.

PATTERSON: The feedback from our customers and banking industry groups with whom we've engaged has highlighted the explicit, prescriptive tone of OCC Bulletin 2013-29, as well as the major changes. While you've touched on some of the key issues, the most important aspects of the recent guidance all deal with impact. The scope of the guidance has been broadened, both in terms of the expansion of what a "critical" activity is and the redefinition from vendor to third party. The importance of these obligations has been elevated with the explicit inclusion of the board at a much deeper level than previously, and the requirement for independent audit to be involved. And finally, the effort has been expanded significantly to include the entire lifecycle of thirdparty management from planning through termination and every step in between. The level of detail provided by the OCC is far more prescriptive than has been the case historically. While in some ways this should simplify things, as the map is relatively clearly designed, it raises a number of questions relative to interpretation that will likely take months, if not years, to flesh out fully. ■

ROUNDTABLE PARTICIPANTS



MODERATOR
Carole Switzer
President,
OCEG



Walter L. Hoogmoed, Jr.,
Principal,
Deloitte



Marie Patterson,
VP, Marketing,
Hiperos



Billy Spears,
Chief Ethics, Privacy
and Compliance Officer,
Hyundai Capital America



THIRD PARTY THREATS COULD YOU BE HELD LIABLE FOR THIRD PARTY SHORTCOMINGS?

Trends such as outsourcing, globalization, lean processes and the geographical concentration of production have made supply chain networks more efficient, but have also changed, and increased, their risk profile. Thomson Reuters Accelus offers a connected solutions-based approach to mitigating, on-boarding and maintaining your third party relationships in terms of risk.

When used together, our products form a solution that helps mitigate third party risk by:

- Helping to manage overwhelming workload
- Using market leading risk intelligence
- Applying time & resources spent where most needed
- Offering comprehensive support services

A third party who provides no serious questions at the outset may present difficulties as the relationship unfolds. The due diligence process should, therefore, never be considered finished!

For more information, visit accelus.thomsonreuters.com

You Are the Weakest Link

By Carole Switzer

We talk a lot today about the growing complexity of supply chains in the global economy. With an almost uncountable number of parties (or links if you will) in many undefined and ill-managed supply chain relationships, the chance of significant or fatal weakness seems immeasurable. The complexity presented by the number, nature, and structure of these relationships is exacerbated by uncertainty about risks that each may present; which may cause disruption in the supply chain, economic loss, or reputational damage. And yet, complexity is necessary to compete.

So how do you find the proverbial weakest link in a supply chain? How do you reduce the uncertainty that contributes to complexity in a negative way without sacrificing the structure that satisfies your supply chain needs?

I recently read a whitepaper entitled “Top 5 Reasons for Supply Chain Complexity,” published by Ontonix (a firm that specializes in measuring complexity in business operations), which lists the key factors as: numerousness, variety, inter-connections, opacity, and dynamic effects. While some of these seem self-explanatory, even the scope of the variables within each factor can be challenging to define. For example, the factor of “numerousness” refers not only to the number of suppliers, but also to variables such as number of parts, available inventory levels, orders completed, and other items that can be counted and that have an effect on supply chain needs. As noted in the whitepaper, the inter-connections between the many influencing variables are constantly changing in ways that increase complexity even more.

But the factor that interests me most is the one that the whitepaper calls “opacity,” for this is something that risk managers can and must address. Opacity is the flip side of transparency. And to gain transparency, and thus a clear view of supply chain risks as they grow and change, requires thoughtful management of information about all of the contributors to complexity in a structured way that enables analysis.

In too many organizations, that structured system of information management, measurement, and analysis simply does not exist. Even the view of whom and what is part of each supply chain, and the types and ranking of risks presented by each such “link,” is opaque. There is no unified approach to identifying risks and mapping them to each participant, and there is no method for determining how many relationships a given supplier has with various parts of the organization. Too many organizations can’t see the cumulative or domino effects that a weakness or realization of risk in one link

of a supply chain may have on them.

This can lead to significant disruption if, for example, there is too much reliance on one supplier and that source has a high level of risk that comes to pass and causes problems. This may be the case even when there are multiple sources, if the risks they face aren’t properly analyzed so that consolidation of risk is evident. We saw for example, where companies may have had multiple suppliers but they were all located in the path of Hurricane Katrina.

Even worse, many organizations believe they are taking a mature approach to supply chain management because they are focusing on optimization. This is a management technique that seeks to better refine

Even worse, many organizations believe they are taking a mature approach to supply chain management because they are focusing on optimization.

understanding of the true needs, in terms of timing and number, for receipt of parts for example, so that inventory is kept at exactly the right level with neither too little or too much. While this is helpful in terms of managing things like warehouse space and accounts payable levels, if the potential of risk realization is not taken into the mix to ensure contingency planning, optimization can leave the organization in a vulnerable state.

Another analysis that is often ignored regards the capacity of selected suppliers. For example, during the BP spill disaster in the Gulf of Mexico, the media reported that most (if not all) of the oil rigs in the region were supported for disaster response by the same third party. Just how well could that company respond if multiple issues arose at the same time? How many supply chains would be disrupted then?

I would argue that the overall lack of insight is grounded in a failure to build and support an integrated supply chain risk-management capability with clear assignment of duties, provision of standard processes and training, and technology that allows for real in-depth monitoring and oversight. The failure to gain and use timely information inevitably challenges the organization’s ability to compete.

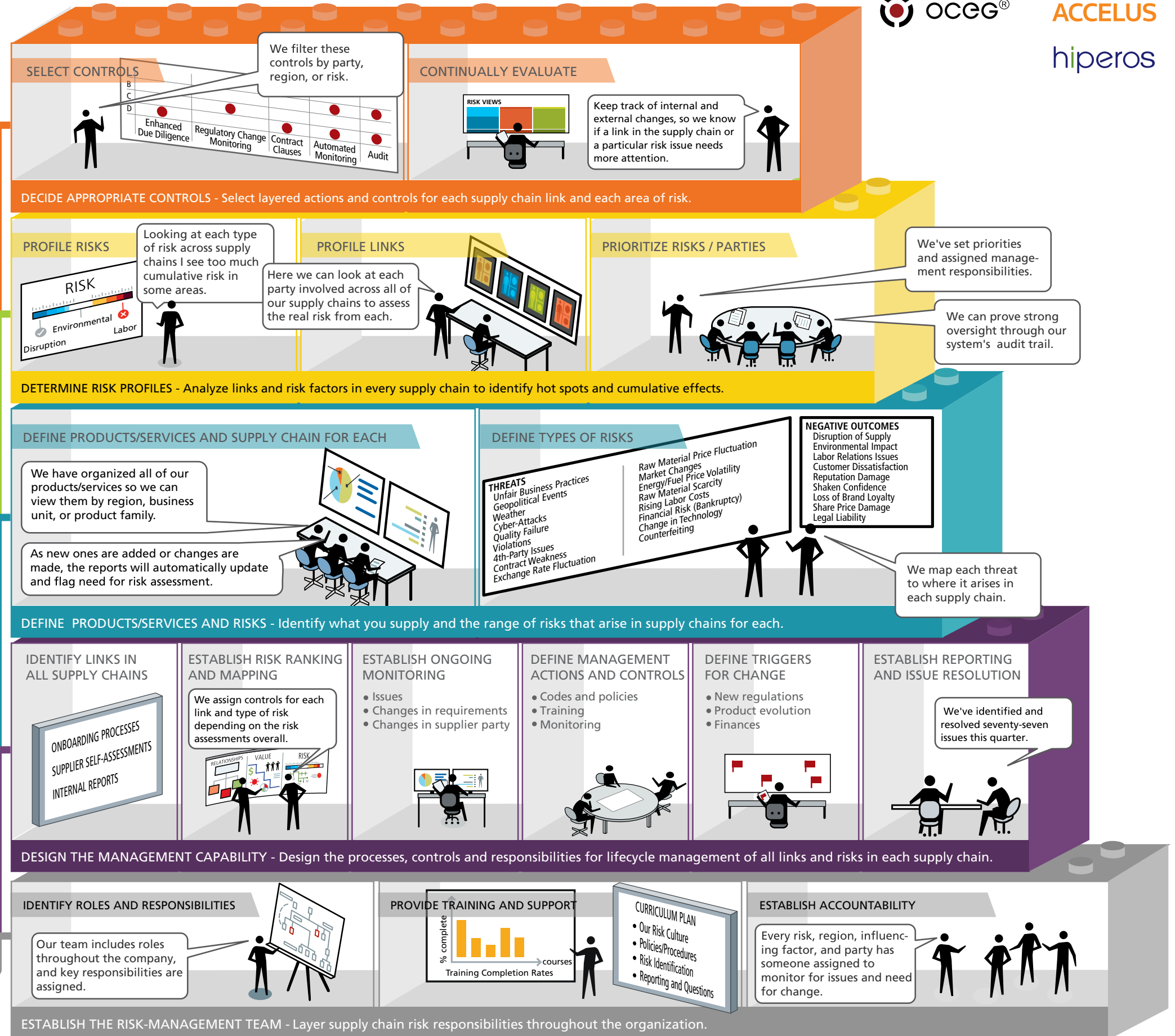
In these instances, the answer to the question of who is the weakest link is clear. In the words of Anne Robinson, the dour game show host, “You are the weakest link.” And just like the contestants on her show, who were dropped through a hole in the floor as she dismissed them with these words, your organization will fall out of the competitive landscape if you aren’t better prepared to know the answers you need to succeed. ■



Switzer

The Building Blocks of Supply Chain Risk Management

Supply chains present almost unimaginable complexity, often having an undefined and ill-managed number of levels with various parties involved across multiple supply chains. Each of these "links" in the chain presents a range of risks. The challenge of effectively managing the ever-changing and often cumulative risks in thousands of continually shifting supply chains can be overwhelming. Having a well-developed capability with appropriate technology, processes, and assignment of responsibilities is essential.



BUILDING BLOCKS

A strong supply chain risk management capability is built on a solid foundation of design and knowledge. Set the building blocks of that foundation in place and connect them in a unified technology system to ensure effective lifecycle management.

KEYS TO SUCCESS

- Identify every link in every supply chain, the roles they play, and the risks associated with them.
- Use a code of conduct, policies, and training to promote awareness of supply chain risk and understanding of required conduct for both employees and parties in the supply chain.
- Select the right technology platform and due diligence partners to build risk intelligence.
- Identify, evaluate and manage risk consistently across and throughout all supply chains, using a standard approach to risk ranking and prioritization.
- Continually monitor and evaluate the supply chain risk management capability.

COMMON MISTAKES

- Addressing only a small subset of parties in the supply chain, and then failing to manage even these based on risk ranking
- Failing to do business continuity planning
- Having inadequate communication between management and personnel involved
- Allowing activities that reduce supply chain transparency
- Not considering consolidated impact



[AN OCEG ROUNDTABLE]

Managing Supply Chain Risk

SWITZER: Let's start with what we mean by supply chain—who and what make up a supply chain?

PATTERSON: While our customers across different industries define “supply chain” in many ways, ultimately they are concerned with the inter-related dependencies of materials, products, and services that allow them to deliver their goods and services to their customers. For our customers in the oil and gas sector, this can mean the 30 or more different entities involved in moving equipment from a manufacturing location in the United States to an oilfield in the Middle East—think freight forwarders and customs brokers. Our banking customers are more concerned with service delivery, increasingly dependent on technology providers and concerns about consumer impact. In food manufacturing, our customers think about availability and traceability.

WYLIE: Often the term “supply chain” is used in the context of tier 1 suppliers, but there is much more to it. We are really talking about the “value chain” and not one, but multiple chains each consisting of multiple layers. It's the movement of materials as they flow from their source to the end customer—not only raw materials, but labor, utilities, management, and all inputs to the product or service. It's made up of the people, activities, information, and resources involved in moving a product from its supplier to its customer. Although this definition may sound complex, effective management of a supply chain for some or-

ganizations can prove even more so. Value chains are multi-tiered, and a problem in one area can quickly have a ripple effect up and down the chain.

KEVERN: I agree the traditional term “supply chain” does not nearly reflect the complex third, and fourth and fifth, and so on party relationships we are seeing today. In recent years, Dell has significantly shifted from computer hardware manufacturer to provider of end-to-end technology solutions in virtually every corner of the globe. At the same time, our sales model has shifted from primarily direct to include channel. Consequently, our “supply chain” has grown from suppliers of product components our company manufacturers to include multi-tier channel partners, resellers, distributors, consultants, agents, vendors, and other business partners.

SWITZER: As we expand beyond concern for efficiency, what are some critical aspects of supply chain risk management today?

WYLIE: Supply chain resilience and minimizing costs are two goals that frequently conflict, and that's a challenge. Years back, Whirlpool decided to outsource the production of dishwasher water seals to a Chinese supplier which totalled a saving of over \$2 million annually. But soon after the arrangement was made, the Chinese supplier changed to a different rubber supplier, raising a multi-tiered effect as previously mentioned. The seals made from this new rubber leaked in dry climates,

causing a failure rate of nearly 10 percent, reputational damage, and revenue loss. So, often it takes a crisis to motivate action and change the way in which we mitigate supply chain risk. Every decision made to increase resilience or reduce costs should be viewed through a risk lens to determine how the decision will modify the company's risk profile.

KEVERN: The main concern companies face today is damage to brand or reputation brought forth by a rogue third-party employee or result of poor business practices. There is also a balance between refraining from exercising too much control over third parties and providing direction and oversight necessary for adequate assurance. For this reason, it's important to establish controls at the entry points into an organization. Dell deploys third-party due diligence to determine whether a given supplier, vendor, or sales partner has the same ethical and compliance values and principles as Dell. Companies that do not share this philosophy are not invited to be part of the Dell family. Changing the way companies view success in the supply chain is a shift in thinking, and more and more companies are seeking the right business partners. Meaning, business partners who share a passion for winning and demonstrated commitment to ethical business practices. This concept applies throughout the duration of the relationship. Meaning, if a distributor sells to an embargoed country or a logistics service provider is engaged in bribery, established processes

“The main concern companies face today is damage to brand or reputation brought forth by a rogue third-party employee or result of poor business practices.”

Kristi Kevern, Director Operational Compliance, Dell Inc.

to off-board as well as prevent re-entry are critical. This proactive management of the supply chain helps mitigate risk of a future catastrophic event.

PATTERSON: The challenge for so many of our customers is that traditional supply chain management only gives them visibility to their immediate tier 1 with whom they contract. So visibility to tier-N—across what is now a value chain, versus only a supply chain, is limited. Our increasing dependence on global, cross-border flows is introducing additional elements to supply chain management. Traditional supply chain concerns of cost, quality, timely delivery, IP protection continue to be paramount. However today's supply chain managers are also being tasked to understand and address broad risk concerns that can affect not only a company's revenues but also their reputation and brand—bribery and corruption, data protection, performance, and broad compliance risks. For our manufacturing customers in particular, the need to manage their multiple vertical customers' regulatory requirements varies considerably and, again, enforces this notion of a value chain, versus only a supply chain.

SWITZER: Supply chains seem like perpetual motion machines—something is always changing. How do you continually monitor and adjust when there are so many moving parts?

KEVERN: Dell addresses this by having a seat at the table, conducting annual compliance risk assessments, and using data analytics technology. Having a seat at the table—whether its periodic staff meetings, quarterly business reviews, or annual leader events—is essential to remain in touch with changes in business strategy and ensure real-time discussion about potential compliance implications in light of supply chain changes. Formal annual compliance risk assessment is another means to keeping a pulse on supply chain activity. In compa-

nies such as Dell where formal compliance risk assessment is part of the culture, business leaders expect questions such as “Are you considering outsourcing?” or “What are your financial incentive targets for resellers next year?” At Dell, it is only fitting that we leverage technology to proactively monitor our supply chain. With our automated continuous monitoring capability, we are able to identify sales activity as compared to population of sales partners cleared through due diligence; ensure third parties with a red flag are further analyzed for suitability; and ensure prospective third parties not deemed suitable for Dell business are not on-boarded or further engaged by Dell. Efficiencies achieved have allowed us to reallocate resources to identify trends, resolve exceptions, and continuously improve programs.

PATTERSON: One of the biggest drivers for technology is the threat to supply chain resilience due to the fact that the supply chain and elements of risk are constantly changing. While capturing all third-party data is important, dynamic monitoring and managing is key—this is not a static environment and no company that I know of has sufficient employees to manually monitor and manage the changes as they happen. So technology and processes that can dynamically and automatically detect and act on changes as they happen and that proactively adjust to changes—particularly changes in elements of risk—are essential.

WYLIE: Supply chains are ever changing and highly dependent on the flow of information up and down the value chain. Ideally, companies should follow a continuous process that begins with assessing the current state of supply chain, pinpointing critical vulnerabilities, and then creating a prioritized roadmap for improvement. Part of this assessment is capturing all third-party data in systems, which are frequently updated, and then constructing real-time visual value chain networks. By mapping value flows, geographical lo-

cations of operations, and transportation links, it is easier to see your greatest potential value losses. Equally important is the establishment of accountability—not having a single point of accountability can lead to fragmented decision making and a tendency to optimize risk at the local or functional level, rather than for the overall supply chain. Working from this foundation, companies can implement improvements and establish processes for monitoring and managing risk over the long term.

SWITZER: Where do you suggest beginning to develop a better view into supply chains?

WYLIE: Simply put—data! Gather it and implement technology that organizes it. An extensive database of third-party information as well as specific supply chain risks, along with proven risk response strategies, helps a business quickly assess its unique situation and develop a customized set of solutions to address its most critical vulnerabilities.

KEVERN: You need to start with business leader accountability. Business leaders must clearly understand why it's important to know your third party as well as the effect on the company (and personal liability) for not doing so. Business leaders must also be committed to making a decision that may not be favorable to the local bottom line, but best for the enterprise as a whole in the long term. Business leader commitment goes hand in hand with the exercise of data discovery.

PATTERSON: All of our customers have some systems in place today that, at a minimum, give them line of sight into their critical suppliers. What they're trying to address is what they don't know below that and within those associations. And, within those associations usually lie the greatest risks. Our recommendation, therefore, is to extend the current set of information and data to address all third parties within the value chain. Most customers begin by addressing specific elements of risk or specific supply chains or criticality and progressively expand down the value chain. Think of it in terms of implementing a strategic framework and executing in a phased or sequenced approach. ■

ROUNDTABLE PARTICIPANTS



MODERATOR
Carole Switzer,
President,
OCEG



Kristi Kevern,
Director Operational
Compliance,
Dell Inc.



Marie Patterson,
VP, Marketing,
Hiperos



Nicola Wylie,
Proposition Marketing
Manager – Enhanced
Due Diligence,
Thomson Reuters



PROFESSIONAL

www.grccertify.org

AUDITOR

GRCP CERTIFICATION

GRCA CERTIFICATION

What is the GRC Professional Certification?

Whether you are an auditor, lawyer, risk manager, compliance director or other professional, GRC Certify can help to extend your skills.

- A way to build on your existing profession and advance your career
- A credential that demonstrates you have the knowledge to design and operate GRC processes
- The best way to ensure that you and your staff understand the GRC Capability Model and other standards





Convercent's risk-based global compliance solution enables the design, implementation and measurement of an effective compliance program. Delivering an intuitive user experience with actionable executive reporting, Convercent integrates the management of corporate compliance risks, cases, disclosures, training and policies. With hundreds of customers in more than 130 countries—including Philip Morris International, CH2M Hill and Under Armour—Convercent's award-winning GRC solution safeguards the financial and reputational health of your company. Backed by Azure Capital, Sapphire Ventures (formerly SAP Ventures), Mantucket Capital and Rho Capital Partners, and based in Denver, Colorado, Convercent will revolutionize your company's compliance program. Learn more at <http://www.oceg.org/organization/convercent>



Hiperos is the number one provider of Third Party Management software, implemented by the Global 1000, including many of the world's largest companies across a range of industries including energy, financial services, manufacturing, real estate, pharmaceuticals, and technology. While third parties offer significant benefit, they can increase a company's regulatory, reputational and revenue risks. The only technology solution to be purpose built to address disparate third party management requirements, Hiperos 3PM™ enables companies to protect their brand and bottom line across the myriad of risks associated with use of third parties. Whether you need an immediate solution to address a pressing regulatory challenge, such as compliance with anti-bribery and anti-corruption laws, or the adaptability to evolve in a dynamic environment, industry-leading Hiperos protects you like no other. And, Hiperos gives your stakeholders everything they need to increase the topline value that third parties can deliver to your business. Hiperos' clients include many of the world's leading companies such as Aetna, Alcoa, AON, Arrow Electronics, Astra Zeneca, AXA, Bank of Montreal, CA Technologies, Charles Schwab, Halliburton, Huntington Bank, JLL, Kraft Foods, Mondelez, Microsoft, News Corporation, Peabody, PNC Bank, Rockwell Automation, Sun Life Financial, State Street, TD Bank, and United Technologies. Learn more at <http://www.oceg.org/organization/hiperos/>



MetricStream is a market leader in Enterprise-wide GRC and Quality Solutions for global corporations. MetricStream enterprise solutions are used by leading corporations in diverse industries to manage quality processes, corporate policies, and regulatory and industry-mandated compliance and corporate governance initiatives. MetricStream's product portfolio comprises of a comprehensive suite of applications based on the patent-pending Enterprise GRC Platform. The applications are designed to manage compliance with quality standards, industry regulations, risk programs and corporate policies. Learn more at <http://www.oceg.org/organization/metricstream/>



STEELE Compliance and Investigation Services (CIS) is a global business advisory and compliance intelligence firm offering comprehensive third-party due diligence solutions that help organizations comply with regulatory requirements and align with best practices. With more than 20 years of experience, STEELE CIS provides Fortune 1000 companies and mid-sized businesses with pragmatic solutions, including Regulatory Due Diligence, Third-Party Program Advisory Services, Program Management Services, and Compliance Analytics and Benchmarking Services. With engagements in over 170 countries, STEELE CIS delivers local and regional expertise with 'on-the-ground' resources. Learn more at <http://www.oceg.org/organization/steele/>



The Thomson Reuters Governance, Risk & Compliance (GRC) business delivers a comprehensive set of solutions designed to empower audit, risk and compliance professionals, business leaders, and the Boards they serve to reliably achieve business objectives, address uncertainty, and act with integrity. Thomson Reuters Accelus connects business transactions, strategy and operations to the ever changing regulatory environment, enabling firms to manage business risk. A comprehensive platform supported by a range of applications and trusted regulatory and risk intelligence data, Accelus brings together market-leading solutions for governance, risk and compliance management, global regulatory intelligence, financial crime, anti-bribery and corruption, enhanced due diligence, training and e-learning, and board of director and disclosure services. Thomson Reuters has been named as a category leader in the Chartis Risk Tech Quadrant™ for Operational Risk Management Systems, category leader in the Chartis Risk Tech Quadrant™ for Enterprise Governance, Risk and Compliance Systems and has been positioned by Gartner, Inc. in its Leaders Quadrant of the "Enterprise Governance, Risk and Compliance Platforms Magic Quadrant." Thomson Reuters was also named as Operational Risk Software Provider of the Year Award in the Operational Risk and Regulation Awards 2013. Learn more at <http://www.oceg.org/organization/thomson-reuters/>



OCEG is a global nonprofit think tank dedicated to helping organizations reliably achieve their objectives, while addressing un-certainty and acting with integrity. This is what OCEG calls Principled Performance, and it is a goal that every organization can achieve by integrating and aligning their approaches to the governance, assurance and management of performance, risk and compliance (commonly referred to as GRC). By integrating these areas, organizations simultaneously increase performance, address risk and reduce costs.


As a nonprofit that does not represent a specific profession, we are uniquely positioned to serve as a hub around which many professions can collaborate on solutions. OCEG's 40,000+ members include:

- board members
- risk executives
- audit executives
- compliance executives
- financial executives
- IT executives
- HR executives
- and other business leaders

Processes for achieving that integrated approach, commonly called GRC, is supported by the open source standards set out in OCEG's Red Book GRC Capability Model and the companion set of agreed upon procedures set out in OCEG's GRC Assessment Tools (the Burgundy Book). The Red Book is used by organizations of all types and sizes, including both businesses, nonprofit organizations and government entities worldwide.

OCEG offers an on demand education series called GRC Fundamentals, and many other resources including its acclaimed GRC Illustrated Series. Through its affiliate, GRC Certify, OCEG offers the opportunity to gain credentials that demonstrate your expertise in establishing, managing and auditing GRC capabilities including the GRC Professional Certification and the GRC Auditor Certification.

Join OCEG today for free, or support our nonprofit mission and gain a wealth of resources by getting an OCEG All Access Pass for yourself, or for your team members. Learn more at www.oceg.org

A large flock of birds flying in a curved path against a sunset sky. The birds are silhouetted against the bright orange and yellow light of the setting sun, which is visible at the bottom center of the frame. The sky is filled with soft, glowing clouds.

How do you
align all the
moving parts of
third party
management to
achieve principled
performance?

Find out for FREE at
www.oceg.org

Nonprofit
Objective
40,000 Global Members