Business Agility Across the Extended Enterprise

This illustration is Part 1 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 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, regulations, 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. ■

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

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.

GRC Illustrated

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.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS BY convercent hiperos Securimate

CORE COMPONENTS

1 IDENTIFY
- Contracts and contact info for all third parties
- Mapping of internal relationships
- Relevant triggers for alerts or changes
- Risk exposure and level of control

2 MONITOR
- Contracts and contact info for all third parties
- Mapping of internal relationships
- Compliance with contract requirements
- Changes to risk, obligations, and business

3 ASSESS
- Risk and compliance
- Performance against SLAs and KPIs
- Identified internal and external events and changes
- Effectiveness of third-party program

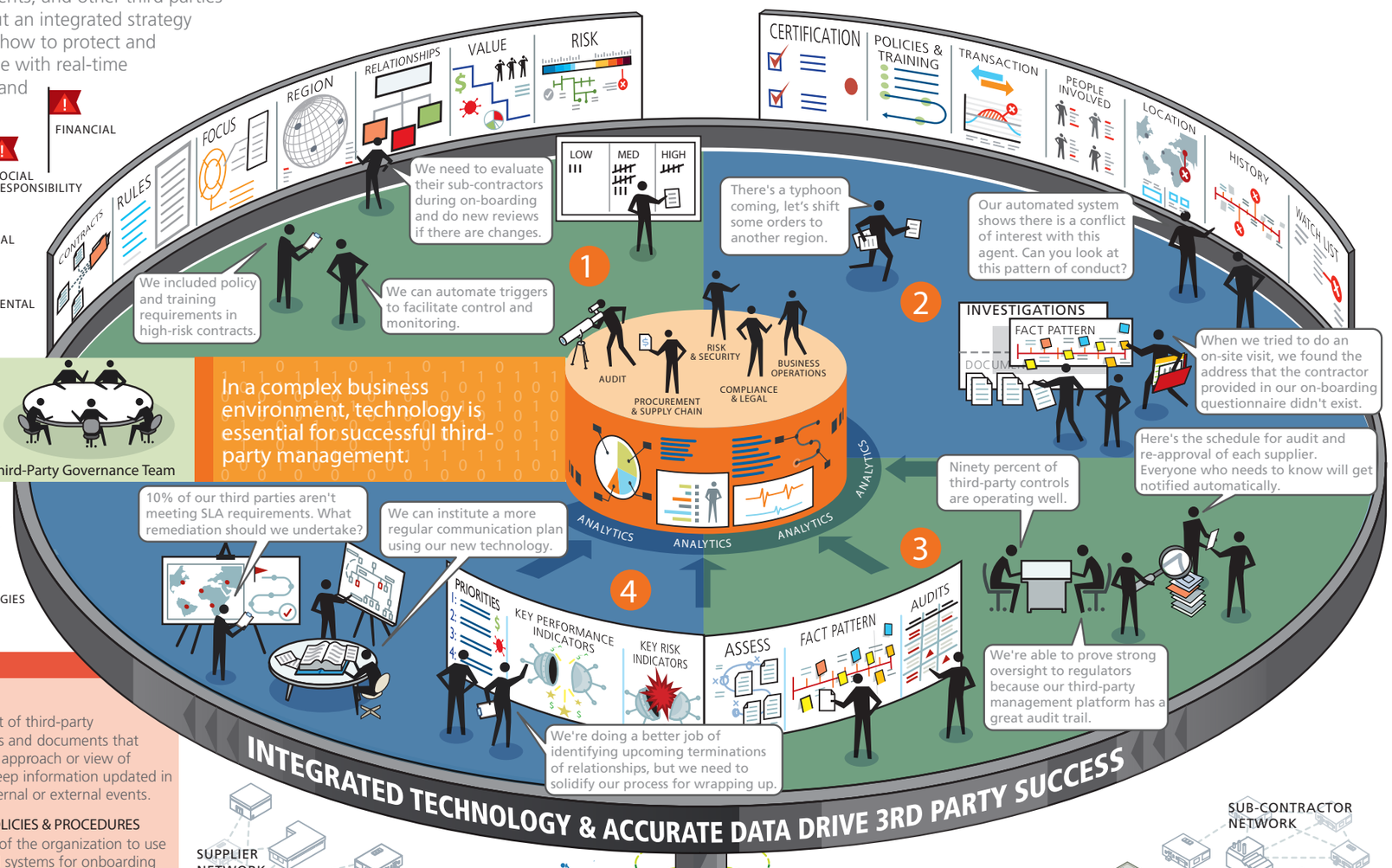
4 RE-EVALUATE
- Contract provisions and controls
- Use of each third-party and internal relationships
- Program design and operation
- Issue investigations and resolutions

RISKS: REPUTATION & BRAND; REGULATORY COMPLIANCE; INFORMATION & PRIVACY; BUSINESS INTERRUPTION; GEO-POLITICAL; ENVIRONMENTAL; SOCIAL RESPONSIBILITY; FINANCIAL

VALUE: COST SAVINGS; EFFICIENCIES; SYNERGIES; STRATEGY

3rd PARTY MGMT PLAN

Third-Party Governance Team



KEYS TO SUCCESS

KNOW WHO, WHERE & WHAT
Maintain a database on each third-party and third-party relationship, internal relationship owners, locations of operations, contract terms, risk and value assessments, required controls and measurements, and issues that arise.

CONTINUALLY EVALUATE RISK & VALUE
Use a third-party management platform to rank each party for risk in areas of concern and value added by the relationship; establish appropriate requirements and controls; and revisit as factors change.

ENSURE NOTIFICATION & ACTION
Automate triggers for notifications to all necessary internal and external parties when new information arises or review is needed; automate revised risk assessments, new training; or other actions where possible and appropriate.

COMMON MISTAKES

MANAGING MANUALLY
Allowing siloed oversight of third-party contracts in spreadsheets and documents that do not provide a unified approach or view of information; failing to keep information updated in context of change in internal or external events.

NOT STANDARDIZING POLICIES & PROCEDURES
Allowing different parts of the organization to use different procedures and systems for onboarding third parties, conducting risk assessments, and managing relationships.

FAILING TO CONSIDER INTERNAL PARTIES
Failing to map responsibilities for aspects of third-party relationships; applying the same controls to all internal relationship managers, regardless of the level of risk or value presented by their third-party contracts.

contact info@oceg.org for comments, reprints or licensing requests

FEBRUARY 2014 WWW.COMPLIANCEWEEK.COM » 888.519.9200

[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 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 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, 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

[GRC ILLUSTRATED]