Breaking Up Is Hard to Do

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

This illustration is part of the OCEG GRC Illustrated Series. You can download it and earlier installments at www.oceg.org/illustrations or from "GRC Illustrated" in the toolbar "Topics" pull-down menu at www.complianceweek.com

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.

Switzer

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. ■

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

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

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 sub-contractors, 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 OCEG®

WITH CONTRIBUTIONS FROM hiperos

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.

DELEGATE

Oversight Personnel
High-level executives and board members accountable to stakeholders and responsible for oversight.

CCO GC CxO

Strategic Personnel
Responsible for planning and design of policies and procedures for due diligence, contract negotiation, ongoing monitoring, and termination management.

Operational Personnel
Responsible for day-to-day execution of the plan. This should include staff embedded in lines of business, as well as procurement

START THE INTEGRATED PROCESS

A fully integrated risk management process supported by unified technology ensures consistency, effective communication and documentation in each step throughout the relationship lifecycle.

INTEGRATED TECHNOLOGY

1 PLAN AND ORGANIZE
Develop a plan to assess the level and complexity of inherent risk presented by each activity, segment to identify critical or high risk activities, and establish required resources.

THINGS TO CONSIDER
· Volume of Activity
· Nature of Risks
· Use of Sub-contractors
· Customer Interactions
· Information Security
· Regulatory Requirements
· Contingency Plans
· Required Approvals

RELATIONSHIPS VALUE RISK

Our strategic plan addresses when and how we use third parties.

2 PERFORM DUE DILIGENCE
Evaluate each third party's controls relative to the level of defined inherent risk; determine mitigating controls to implement and document in the book of record.

ITEMS TO EVALUATE
· Compliance and Risk Management
· Financial Condition and Resilience
· Experience and Reputation
· Company Principals
· Information Security and Systems
· Incident Management and Reporting
· Human Resource Management
· Conflicts of Interest

We put the self-disclosure surveys, interview reports, and documentation of other credible information into the system.

3 MANAGE CONTRACTS
Establish contract terms based on due diligence conclusions; through ongoing review of the relationship, re-negotiate terms addressing required and prohibited actions, SLAs, and KPIs; gain oversight approval for critical contracts or those with exceptional risk.

We need to track and manage these items

CONTRACT TERMS
Key Performance Indicators (KPI)
Information Management/Reporting
Audit and Oversight Rights
Compliance Requirements
Use of Information, IP, and Technology
Confidentiality and Integrity
Conflicts of Interest
Sub-contractor Requirements
Termination Terms
Covenants

4 CONDUCT ONGOING MONITORING
Oversee and pro-actively monitor and review each third-party relationship at a level commensurate with risk, to assess ability to meet SLAs, performance metrics, duties and responsibilities, and other contractual terms. Also, monitor compliance with legal and regulatory requirements. Ensure that issues are identified and appropriately escalated for remediation.

I'm set up to get automatic notifications if the risk of any relationship changes based on our established criteria.

We've had a report of some key personnel changes and new sub-contractors, so automatic due diligence updates have been triggered.

We need to consolidate information in a unified technology system to effectively manage,document, and report on each third-party relationship.

5 MANAGE TERMINATIONS
Whatever the reason for termination, follow an established plan for transitioning to another third party, bringing activities in-house, or ending activities. Consider need to protect information, maintain smooth operations, and protect reputation during transition.

STEPS TO TERMINATION
1. Implement established transition plan
2. Manage disposition of data, IP, and assets
3. Discontinue and monitor all access points
4. Evaluate need to address reputation risk

Have we allocated adequate resources to efficiently manage the transition?

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.

INTERNAL AUDIT

We are here for the annual audit of the risk system

EXTERNAL AUDIT

This integrated technology system lets us really see what is being done and how well it is working

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 confidential 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 third-party 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

[GRC ILLUSTRATED]