ISG™ imagine your future®

BUILDING A FOUNDATION:

The Role of the VMO in Regulatory Compliance Planning, Due Diligence and Contract Negotiation

David England, Director, ISG

EXECUTIVE SUMMARY

Complying with OCC regulations on third-party oversight clearly represents a clear and pressing priority for banks and financial services firms.

To date, vendor management and sourcing organizations have made significant progress in navigating the tortuous regulatory maze and developing internal policies that align with regulatory guidelines and requirements.

The next step is to convert that understanding of policies into rigorous and sustainable processes that operate seamlessly and consistently across a number of entities. Specifically, the compliance oversight of any given third-party provider involves sourcing, procurement, legal, finance, contracting, IT, vendor and risk management and often multiple business units – groups with widely varying priorities and areas of responsibility. This requires clearly defining areas of responsibility and ownership, understanding what needs to get done (when and by whom), ensuring the right people are in place within each function, and then establishing and maintaining the necessary flows between those disparate organizations.

Moreover, third-party oversight must be maintained throughout the relationship, beginning with initial planning and extending through to termination. Each specific phase, meanwhile, presents a unique set of requirements.

A Vendor Management Office (VMO) can play a critical role in addressing these challenges. Uniquely positioned to facilitate communication and transparency among myriad entities, the VMO can help establish a sound compliance framework as well as manage multiple touch points and ensure process discipline over the long term.

This ISG white paper describes recent developments in the regulatory space and their implications for financial services organizations. The author analyzes the process of leveraging the VMO to establish an effective foundation for regulatory compliance, focusing on the specific phases of Planning, Due Diligence and Contract Negotiation. The Ongoing Monitoring and Termination phases will be discussed in a future paper.

BUILDING A FOUNDATION

New Game, New Rules

Regulatory guidelines for third-party oversight are nothing new to the banking community. A number of agencies – including the Office of the Controller of the Currency (OCC), Federal Reserve Bank (FRB) and Consumer Financial Protection Bureau (CFPB) – have over the years issued guidance on how relationships need to be managed. Banks have long had programs in place to manage risks associated with third party relationships. Traditionally, compliance efforts have focused on due diligence around new vendor engagement, with subsequent oversight entrusted to the protections set forth in the contract.

The global financial crisis of 2008 sparked a fundamental redefinition of the requirements banks face when managing third-party risk. Specific measures included the OCC's release of a new bulletin in October of 2013 that rescinded previous guidance. In addition, the CFPB was established, with responsibility for administering various consumer protection laws that previously fell under OCC purview.

The guideline revisions have resulted in stricter regulatory oversight of banks and their third-party relationships. At the same time, banks have steadily expanded the number, type and complexity of third-party relationships in efforts to control operating expenses and add new sources of revenue. In response to this increased reliance on third-party suppliers, regulators have strengthened third-party risk management standards even further.

The net result is that third-party management standards are now at a level that few banks have been able to meet. Indeed, banks today find themselves out on a precarious limb – they face increasingly rigorous scrutiny of their third-party relationships, precisely at a time when they are more reliant than ever on complex third-party relationships.

Phase-by-Phase Oversight

The OCC standard describes requirements for managing third-party relationships from the time they are contemplated to the time they are dissolved. Specific phases are defined as follows:

- Planning
- Due Diligence
- Contract Negotiation
- Ongoing Monitoring
- Termination

Successful compliance in today's environment requires alignment, communication and process discipline applied at each specific phase of the sourcing lifecycle. This can be best achieved through a VMO function – one that operates across organizational and functional boundaries and as such is best positioned to ensure coordination across disparate teams and business units.

Following is an examination of the specific compliance requirements and challenges related to the Planning, Diligence and Contract Negotiation phases of the sourcing lifecycle, along with a discussion of how they can be addressed.

Planning

Requirements: The OCC expects a bank's senior management to develop a plan to manage the relationship in a manner commensurate with the level of risk and complexity of the third-party relationship. The OCC's expectation is for banks to use the Planning phase to think carefully about third-party risk and associated third-party management costs, and to budget accordingly for critical downstream activities.

Challenges: The challenge for banks during the Planning phase is to accurately and adequately define the level of support needed for the subsequent phases of Due Diligence and Ongoing Monitoring. Without centralized oversight of the sourcing and procurement functions to enforce consistency and standards, banks risk underestimating or neglecting potential risk levels of future phases. If the risk levels aren't properly identified at the outset, the business plan's budget may be inadequate. As a result, funding slips through the cracks and the compliance program is compromised before it even begins.

Putting a definition around "level of risk and complexity" and "commensurate" also presents a challenge, since the OCC leaves it up to the bank to determine what these terms mean, rather than explicitly stating requirements. That said, we are seeing less confusion thanks to informal sharing of information between banks regarding standards and expectations.

Conceptually, every use of a third party introduces some level of risk into the organization. However, the level is different for each engagement. For example, the vendor that performs landscaping introduces minimal risk and requires minimal risk mitigation – the OCC would expect only that the bank is aware of the relationship and has determined and documented that the risk is minimal. However, even this innocuous task can be a big challenge when managing thousands of vendors.

The risks become more significant when the provider has access to critical systems or to information such as client or customer data, or is responsible for performing critical operations such as IT or call centers. General criteria that indicate a high level of potential risk include performing activities that would be difficult to replace, interfacing directly with customers, using offshore resources or being paid significant fees to perform services.

Another challenge is collecting information about all vendors and engagements and ensuring that the basic assessment has been performed. Some banks may have 20,000+ vendors, and even though 19,800 may be low risk, the bank still needs to demonstrate that each has been assessed. Avoiding over-analysis – specifically, collecting too much information on low-risk providers – is imperative. A few key questions are sufficient to prioritize and identify critical providers.

Further complications arise if the sourcing and procurement functions are not engaged until late in the process. A common scenario is that the business decides on a provider and then expects sourcing and procurement to quickly process the paperwork and finalize the agreement. Any delays – even for legitimate review – are perceived as bureaucratic roadblocks; sourcing and procurement are labeled as villains, when in fact the business is ignorant of legal requirements.

Key Success Factors: The VMO should coordinate activity and provide oversight between the business, sourcing and procurement teams during the Planning phase. Providers must be prioritized into high, medium and low risk categories, and each category assigned a pre-defined set of activities that must be performed. High-risk relationships must be identified and the business advised on the type of due diligence and ongoing monitoring that will be needed in subsequent phases. A process to monitor Accounts Payable information to identify new relationships should be implemented during this phase. The business will likely require support to ensure that questions are answered appropriately to build consistency and standards.

Due Diligence

Requirements: The OCC requires that firms evaluate each third party's depth of resources and previous experience in providing the specific activity being contracted. The evaluation should include length of time the third party has been in business, its market share for the activities, specifically within the business model being contracted for. Reputation, including history of customer complaints or litigation, are to be included as well.

Banks are also required to independently review the third party's legal and regulatory compliance program, as well as evaluate each law and regulation that applies to the new relationship and ensure each one is mapped prior to contract execution.

Additional details include conducting reference checks with external organizations and agencies such as industry associations, Better Business Bureau, Federal Trade Commission or other regulatory filings; review of the third party's websites and other marketing material to ensure statements and assertions are in line with the bank's expectations; and an assessment of how the third party plans to use the bank's name and reputation in marketing efforts.

A key outcome of Due Diligence is to identify gaps in a potential provider's capabilities, which are then discussed during the Contract Negotiation phase. Depending on their severity and recommended actions, the gaps are either addressed to the bank's satisfaction or used as grounds to eliminate the bidder.

Challenges: A key imperative during Due Diligence is to ensure that the activities conducted are aligned with the level of risk exposure and type and complexity of the relationship being contemplated. For example, if the service provider has access to or maintains sensitive client data, the client must ensure that the provider's information security standards are at least at the same level as the client's (which, in turn, must meet regulatory compliance standards).

Potentially high-risk providers may require regular (annual) on-site assessments. A challenge here is that assessments become back-logged, slowing down the process. Using third parties to conduct assessments can help, as can advance planning to account for site visits.

In some organizations, responsibility for tracking and reporting falls to sourcing and procurement teams. While this approach enables integration with the sourcing process, the teams risk getting bogged down in dealing with bidders who aren't selected as suppliers. Moreover, fragmentation of tracking and reporting activity can occur, so that information gathered during Due Diligence isn't carried forward consistently through the life of the agreement.

Other types of due diligences that may need to be included:

- Financial condition or viability of the potential provider
- Business experience and reputation
- Background check on company principals
- Resilience – soundness of the provider's DR/BC capabilities
- Reliance on subcontractors to perform in-scope work

Key Success Factors: Coordination is essential. The VMO should be involved with potential suppliers and business SMEs to ensure that assessments are properly planned and implemented and that appropriate information is shared and communicated. Through this oversight role, the VMO enables consistent activity throughout the life of the agreement and prevents the fragmentation referenced earlier. The VMO also supports business stakeholders,

who are ultimately accountable for understanding the process and addressing questions or concerns.

While historically this has not been the case, the VMO should be closely involved in pre-contract signing activities, as this enables the coordination and linkage that become essential in the downstream execution and management of the contract.

Contract Negotiation

Requirements: During contract negotiation banks are required to provide and retain timely, accurate and comprehensive information such as records and reports to monitor third-party performance, service levels and risks. More specifically, banks must stipulate the frequency and type of reports required. These can include performance and security reports, control audits, financial statements, Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and Office of Foreign Asset Control (OFAC) compliance requirements, and reports for monitoring potential suspicious activity and customer complaints.

Additional stipulations include ensuring that third parties maintain adequate insurance, notify banks of material changes to coverage and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance and intellectual property insurance.

Contracts must also stipulate that third-party activities be subject to OCC examination oversight, defined to include access to all work papers, drafts and other materials. This generally gives the OCC the authority to oversee third parties in the same way that it oversees a bank operating on its own premises.

Challenges: The key is to ensure proper controls are in the contract. Banks are already generally adept at this phase, and sourcing and procurement functions have standard T&Cs that cover requirements. However, if the Planning and Due Diligence phases haven't been properly executed, sustaining the contractual terms and governance mechanisms over the long term will present a challenge.

Staying on Track

Once the groundwork of Planning, Due Diligence and Contract Negotiation are laid, the real test of regulatory compliance lies ahead – in sustaining consistent oversight over the life of the agreement. In a forthcoming white paper, we examine the phase of Ongoing Monitoring in greater detail.

ABOUT THE AUTHOR

BUILDING A FOUNDATION
The role of the vmo in regulatory compliance planning, due diligence and contract negotiation

DAVID ENGLAND
Director, ISG

ISG Director David England has over 25 years of experience in information technology outsourcing, with expertise in vendor management, change management advisory services. David has provided outsourcing advisory services for a number of clients supporting RFP development, provider selection retained organization design, vendor governance and obligation management. David has been with ISG for over six years, and previously held account management and consulting roles at EDS and A.T. Kearney. David has extensive international ITO experience and spent more than 11 years in Asia where he led numerous business transformation and IT transition projects.

ISG™
imagine your future®

ABOUT ISG

ISG (Information Services Group) (NASDAQ: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; technology strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

Let's connect NOW...

ISG™

imagine your future®

