OCC RISK MANAGEMENT GUIDANCE ON **THIRD-PARTY RELATIONSHIPS**

sageworks®

NICK SHAKARJIAN, DIRECTOR

TABLE OF CONTENTS

INTRODUCTION

Examiners have always expected banks and credit unions to perform appropriate vendor due diligence prior to engaging a third party. But with October 2013 guidance, Third-Party Relationships, the OCC provided defined guidelines for OCC banks as a risk management framework.

In this paper, we look at some of the specific requirements and how banks can meet expectations during forthcoming exams. This will include specific questions to ask and criteria to consider during different stages of the third-party relationship.

INTRODUCTION (CONT.)

THIRD PARTY?

Includes activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records.

As the announcement points out, banks face new and increased operational, compliance, reputation, strategic and credit risks when entering into an agreement with a third party, especially when the agreement covers "critical activities". As such, the OCC asks banks to develop a risk management process proportionate to the level of risk within the relationship.

"Critical activities" are described as significant bank functions, services or activities that could have a major impact on the bank's operations. Comptroller of the Currency Thomas Curry explains: "We have concerns regarding the quality of risk management on the growing volume, diversity, and complexity of banks' third-party relationships, both foreign and domestic. This guidance provides more comprehensive instruction for banks to ensure these relationships and activities are conducted in a safe and sound manner."[1] The new guidance set forth by the OCC supersedes prior Bulletin 2001-47, "Third Party Relationships: Risk Management Principles" and OCC Advisory Letter 2009-9, "Third-Party Risk".

Third-party relationships are defined as a business arrangement between a bank and an outside entity, by contract or otherwise. Some examples are tax, legal, audit or information technology. By entering into agreements with third parties, it is the board members' and senior management's responsibility that contracted activities fall in line with regulatory guidance and uphold safety and soundness for the institution.

When circumstances warrant, the OCC will apply corrective measures to ensure banks' relationship management standards are appropriate, and these measures could include enforcement actions, special examinations and the assessment of civil money penalties.

INTRODUCTION (CONT.)

On December 5, 2013, shortly after the OCC release, the Board of Governors of the Federal Reserve System issued Guidance on Managing Outsourcing Risk[2] to supplement guidance previously issued on technology service provider risk.[3] While the Federal Reserve's guidance is less comprehensive than the new guidance set forth by the OCC, many of the themes are similar.

MADE THE MOVE TO THE OCC?

See what challenges banks faced when transitioning:

Moving from the OTS to the OCC: Impact on the ALLL

RISK MANAGEMENT **LIFE CYCLE**

As banks continue to increase the number and complexity of third-party relationships, the OCC is concerned that the quality of risk management in the relationship may not be commensurate with the level of inherent risk. This includes proper due diligence when selecting a vendor, but it also extends into the relationship.

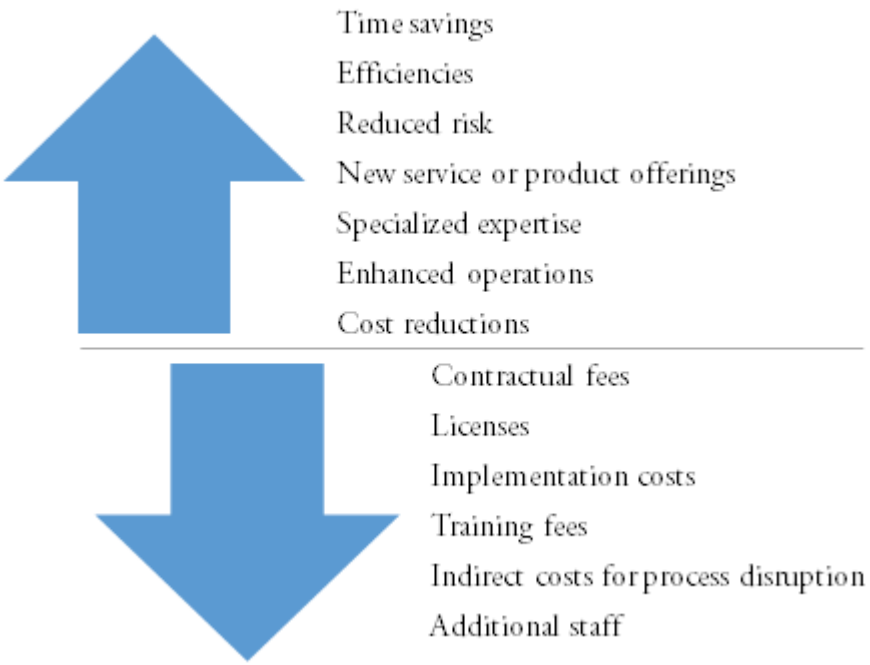
An effective risk management process includes a continuous life cycle for all third-party relationships and covers:

- Planning
- Due diligence and third-party selection
- Contract negotiation
- Ongoing monitoring
- Termination

PLANNING

Prior to entering into a third-party relationship, management should develop a plan establishing the goal of the relationship and the scope of the contract. This enables the bank to discuss inherent risks and evaluate how the contracted activity relates to the bank's overall strategic goals, objectives and risk appetite—what impact would such a relationship have?

Banks are also encouraged to perform a cost-benefit analysis at this stage to determine if the potential benefit (e.g. cost reductions, expanded bank operations, increased efficiencies, heightened expertise) outweighs the estimated cost (e.g. integration and subscription fees, training, additional staffing, interruption to existing programs), and how it might impact information security. A detailed process as to how the bank will select, assess and oversee the third party must be presented to and approved by the bank's board of directors when contracting critical activities.



DUE **DILIGENCE**

DUE DILIGENCE

The OCC provides a comprehensive list of criteria to use during diligence; be sure to review that list before signing a contract.

An in-depth assessment of the third party's ability to perform the activity while complying with regulatory guidelines should be performed before entering into a contract or relationship. Banks should not rely on experience with or prior knowledge of the third party, and the level of due diligence should be equal to the risk and complexity of the relationship.

In practical terms, this means a core system that houses all the bank's loan and customer data might require more attention than a relationship contracted to print deposit slips.

Due diligence recommendations from the OCC includes a whole host of criteria for assessing a third party, including:

1. **Corporate strategies:** Do they conflict with the bank's strategy, or will business arrangements planned by the organization affect the bank?

2. **Legality**: Does the third party have all necessary licenses and audits according to the service agreement?

3. **Financial condition**: Upon reviewing audited financial statements, does it appear the third party is in good financial health (i.e. growth levels, profitability, debt) to offer uninterrupted service?

4. **Experience**: Does the third party have a history of satisfactorily providing the service and with the level of expertise required?

5. **Fees**: Does the license fee or cost structure create financial difficulties for the bank?

4 THINGS TO CHECK

Before signing a new supplier, check these four financial metrics.

DUE **DILIGENCE** (CONT.)

6. **Principals of the company**: Does the third party periodically check the background of senior management and personnel that will participate in the relationship?

7. **Risk management**: Does the organization have proper internal controls and audit functions in place? A third party's SOC 1 report is an excellent starting point. A SAS 70 is no longer the relevant audit report. In 2011, the AICPA replaced the SAS 70 with the more comprehensive SSAE 16, also known as SOC 1.

8. **Information security**: Do the controls at the third party adequately keep data safe and quickly address new threats or vulnerabilities once identified?

9. **Information management systems**: The bank should understand how the third-party application works and should have available the third party's performance metrics to understand weaknesses in the process and in the interaction of the third party with the bank's technology, data or personnel.

10. **Resilience**: Has the third party made disaster recovery plans for continued service in light of natural disasters, cyber or physical attacks or human error? Have these plans been effective in the past?

11. **Incident reporting**: In the event of an incident, is the organization equipped—through processes and accountability programs—to quickly remedy the incident?

DUE **DILIGENCE** (CONT.)

12. **Physical security**: Does the third party mitigate physical risk for its employees, data facilities and technology?

13. **HR policies**: Are employees properly trained and held accountable?

14. **Use of subcontractors**: If the organization uses another company(s) to help deliver the service, is that subcontractor relationship one that might introduce risk? And, should it be similarly assessed for risk to the bank?

15. **Appropriate insurance**: Does the third-party organization have bond insurance or other types of protection for IP rights and assets that are not generally covered by commercial policy?

16. **Agreements with other parties**: In other agreements does the organization indemnify itself, which might pass risk on to the bank?

This list is meant to start the due diligence thought process but may not be conclusive; it's recommended to read the guidance in its entirety to gauge how the identified risks could apply to a bank's specific relationship.

A chief financial officer of a privately held bank in the Northeast commented, "The new OCC guidance forces banks to be more cognizant of the relationships they undertake and assess the risk involved with third parties. As banks recover from the financial crisis in 2008, it's clear the OCC is promoting a more structured approach to mitigate risk."

DUE **DILIGENCE** (CONT.)

While this list may be onerous to administer, it does help bank management and board members understand and execute a thorough vendor due diligence program.

It is management's responsibility to review and determine whether or not the third party meets expectations. If critical activities are part of the contract, senior management must present the due diligence results to the board for approval when making recommendations on third-party relationships.

CONTRACT **NEGOTIATION**

Upon selecting a third party, a bank's management will likely negotiate or review a contract detailing the responsibilities of each party. Contracts should fully describe compensation, fees and the circumstances under which the cost structure may be changed. Moreover, contracts need to specify what constitutes default and stipulate the conditions for termination. Banks should also re-visit existing contracts to ensure they comply with risk controls and legal protections.

The contract should also cover performance expectations, and it's recommended for a bank to use industry standards to evaluate the contract's service level agreement. For software, these standards might measure

1. Service availability
2. Responsiveness of support requests and/or
3. Update or enhancement timelines.

Again, senior management will need to get approval from the board on all contracts, prior to execution, when critical activities are involved.

ONGOING **MONITORING**

Once a contract with a third party has been executed, bank management should dedicate staff with expertise and authority to oversee and monitor the relationship, especially if it involves critical activities. And the criticality of an activity may change over time, making a relationship more or less of a source of risk.

Consequently, banks will need to adapt its monitoring accordingly.

Many of the due diligence criteria will extend throughout the contract's lifetime, so banks are expected to include these reviews as part of the ongoing monitoring process. In instances where a discrepancy or issue is identified, senior management should take action and escalate significant issues to the board.

TERMINATION

The termination phase of the risk management lifecycle is new to OCC guidance. Under the new guidance, banks are required to implement risk management controls and maintain them through the termination phase, or the end of the contract. Contracts with third parties may be terminated by the bank for several different reasons, including expiration, breach of contract, vendor change or the decision to bring the activity in-house.

It's management's responsibility to have a plan in place and to be proactive in the event of a contract default or termination, ensuring compliance throughout the entire relationship. A bank's contingency plan should address reputation risks, joint intellectual property, data retention and deconstruction in accordance with regulatory laws and guidelines.

CONTINUING **EXPECTATIONS**

Throughout the lifecycle, there are ongoing expectations laid out by regulators:

- Oversight and accountability
- Documentation and reporting
- Independent reviews

Oversight and Accountability

Clearly defined roles for board members, senior management and bank employees who directly manage third-party relationships are outlined in the new OCC guidance.

1. Senior management must establish and implement the bank's third-party risk management process along with planning future engagements with third parties and their ongoing monitoring.

2. Bank employees must confirm that the third party complies with the bank's policies and, when needed, escalate significant issues to management.

3. The board of directors must approve contracts with third parties and the bank's risk-based policies with jurisdiction over third parties.

Documentation and Reporting

A bank should properly document and report on its current inventory of third-party relationships and identify those that involve critical activities. This will assist in sustaining accountability, monitoring and overall risk management, and it will make exam-time easier with all the data in one central location. This list must be kept up to date, especially since examiners may request it at any time.

CONTINUING **EXPECTATIONS** (CONT.)

Independent reviews

A bank's senior management should ensure that periodic, independent reviews are conducted on its third-party risk management process. An internal auditor or independent third party may perform the review, in which case senior management is expected to present the results to the board of directors.

These results will help management determine whether and how to adjust the bank's risk management process, policy, reporting and controls. As the figure from the OCC guidance shows, it's an iterative and repeated process that will be refined through time.

Chart from the OCC Guidance[4]

CONCLUSION

The aforementioned criteria and expectations are indispensable when dealing with third parties.

Under the new OCC guidance, it is the senior management's responsibility to develop and implement the bank's third-party risk management process; however, it is up to the board of directors to approve any of the bank's risk-based policies and contracts encompassing critical activities.

This OCC guidance does put more of the onus on the board compared to recommendations put out by the Federal Reserve. But in both cases, there is a clear effort and expectation from the OCC and Federal Reserve for banks to be more attentive to and proactive with third-party relationships and inherent risk.

ABOUT **SAGEWORKS & THE AUTHOR**

Sageworks (www.sageworks.com) is a financial information company working with financial institutions, accountants and private-company executives across North America to collect and interpret financial information. Thousands of bankers rely on Sageworks' credit risk management solutions to streamline credit analysis, risk rating, portfolio stress testing, loan administration and ALLL calculation. Sageworks is also an industry thought leader, regularly publishing whitepapers and hosting webinars on topics important to bankers.

sageworks® | ALLL

Sageworks ALLL is the premiere automated solution for estimating a financial institution's reserve. It helps bankers automate their ALLL process and increase consistency in their methodology, making it defensible to auditors and examiners. Sageworks' risk management consultants also assist clients with the implementation of their ALLL models and guidance interpretation. To find out more, visit www.sageworksanalyst.com.

Nick Shakarjian is a director of financial markets at Sageworks, where he assists financial institutions with credit and portfolio risk management solutions. Working with banks and credit unions across asset ranges, Nick is responsible for working primarily with the allowance, helping financial institutions to minimize regulatory and accounting risk. Nick is a graduate of the Alfred Lerner School of Business at the University of Delaware, where he studied business marketing.

ENDNOTES

[1] "Office of the Comptroller of the Currency Releases Guidance on Third-Party Relationships," Office of the Comptroller of the Currency. October 30, 2013. Accessed at http://www.occ.gov/news-issuances/news-releases/2013/nr-occ-2013-167.html.

[2] "Guidance on Managing Outsourcing Risk," Board of Governors of the Federal Reserve System. December 5, 2013. Accessed at http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf.

[3] "Outsourcing Technology Services," Federal Financial Institutions Examination Council. June 2004. Accessed at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.

[4] "Third-Party Relationships," Office of the Comptroller of the Currency. October 30, 2013. Accessed at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

ADDITIONAL **RESOURCES**

"e-Book: The Complete Guide to the ALLL," *Sageworks.*

http://web.sageworks.com/complete-guide-ALLL-reserves/

ALLL Forum for Bankers, *LinkedIn.*

http://www.linkedin.com/groups/ALLL-Forum-Bankers-4844399/about

Appendix B of "Third-Party Relationships," *OCC. Contains a list of additional, helpful regulations in the area of third-party relationships.*

http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

"Moving from the OTS to the OCC: Impact on the ALLL," *Sageworks.*

http://web.sageworks.com/OTS-OCC-alll-impact/

"9 Ways to Prepare for Your Next Examination," *Sageworks.*

http://web.sageworks.com/banking-exam-preparation/