



Audit Report



OIG-14-034

OCC's Review of Banks' Use of Third Party Service Providers Is Not Sufficiently Documented

April 21, 2014

Office of
Inspector General

Department of the Treasury

Contents

Audit Report

Background..... 2

Results of Audit..... 4

 OCC Has Updated Guidance to Banks on Managing Risks Related to
 the Use of Third Parties4

 OCC Examiners' Review of the Use of Third Parties by Smaller
 Financial Institutions is Not Sufficiently Documented.....6

Recommendation 9

Appendices

Appendix 1: Objectives, Scope, and Methodology11

Appendix 2: Management Comments13

Appendix 3: Major Contributors to This Report15

Appendix 4: Report Distribution16

Abbreviations and Acronyms

CFPB	Consumer Financial Protection Bureau
EIC	examiner-in-charge
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examinations Council
FRB	Board of Governors of the Federal Reserve System
IT	information technology
MDPS	multi-regional data processing servicer
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency

This page intentionally left blank.

*The Department of the Treasury
Office of Inspector General*

April 21, 2014

Thomas J. Curry
Comptroller of the Currency

This report presents the results of our audit of the Office of the Comptroller of the Currency's (OCC) supervision of the use of third-party service providers (hereafter referred to as third parties) by national banks and federal savings associations. This is an OCC operation that we had not previously reviewed.

Our audit objective was to evaluate the sufficiency and effectiveness of OCC's procedures for supervising the use of third parties by national banks and federal savings associations. We interviewed OCC personnel responsible for supervising banks' use of third parties and reviewed relevant OCC documentation, such as policies, procedures, and guidance, as well as similar documents issued by other federal regulatory agencies. We conducted our audit fieldwork from July 2012 through July 2013. Appendix 1 contains a more detailed description of our objectives, scope, and methodology.

In brief, we found that OCC provided guidance to banks on managing risks related to the use of third parties. OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles" was in effect during our audit. Although generally comprehensive, the guidance needed to be updated. Subsequent to the end of our fieldwork, OCC issued new risk-management guidance related to third-party relationships for national banks and federal savings associations.

In addition, we found that, as part of their examinations, OCC examiners conclude upon the adequacy of bank processes for managing risks related to the use of third parties. However, we found that examination workpapers related to the use of third parties by smaller financial institutions often do not leave a clear

enough audit trail to enable a reviewer to determine how the conclusions were reached.

We are recommending that OCC reinforce to examination staff the need for workpapers to contain essential information to support conclusions about banks' governance of third parties. Essential information should include the procedures performed and the results upon which the conclusions are based.

In a written response, which is included as appendix 2, OCC management stated that it will communicate to examiners, via memorandum and discussion, the expectations for documentation when reviewing a bank's risk regarding third-party service providers. Additionally, OCC will update relevant booklets of the *Comptroller's Handbook* to incorporate references to OCC guidance on third party service providers, and revise the Community Bank Supervision booklet to more clearly address procedures for scoping reviews and monitoring of banks' reliance on third parties for critical services. We consider these planned corrective actions as responsive to our recommendation.

Background

Financial institutions use third parties to carry out significant parts of their regulated and unregulated activities. Such third parties could include vendors, agents, dealers, brokers, marketers, and bank service companies that have entered into a business relationship with an insured depository institution. A third party can be a bank or a nonbank, affiliated or not affiliated, domestic or foreign. Use of third parties can cross many business activities and may include information technology (IT) services, such as applications development, programming, and coding; specific banking and administrative operations, such as aspects of finance and accounting; back-office activities, processing, and administration; and other contract functions, such as call centers. Third party arrangements can be complex and have the potential to transfer risk management and compliance to third parties who may not be regulated and who may operate offshore. Industry and regulators acknowledge that this increased reliance on third parties

may affect the ability of the regulated entities to manage their risks and monitor their compliance with regulatory requirements.

OCC supervises 1,971 banking institutions with total assets of approximately \$10 trillion,¹ but it does not maintain statistical data on third party use by the financial institutions under its supervision.

Under the Bank Service Company Act, OCC has the authority to supervise third parties engaged by national banks and federal savings associations for the performance of any applicable functions of the regulated institution's internal operations.² OCC's supervision of an institution's use of third parties includes the promulgation of guidance requiring boards of directors and management of national banks and federal savings associations to oversee and manage third-party relationships,³ the evaluation of the third party governance process at individual regulated financial institutions, and the direct examination of certain larger technology service providers.

Technology service providers that service a large number of insured financial institutions supervised by more than one federal financial institution regulator may be subject to interagency examinations performed under the auspices of the Federal Financial Institutions Examination Council's (FFIEC) Multi-Regional Data Processing Servicers (MDPS) program.⁴ Two FFIEC publications provide a

¹ According to OCC's 2012 *Annual Report*, OCC supervised 1,351 national banks, 573 federal savings associations, and 47 federal branches of foreign banks in the United States. National bank and federal branch assets totaled \$9.2 trillion, and federal savings association assets totaled \$803.1 billion.

² 12 U.S.C. § 1867 (c).

³ OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," Nov. 2001, was in effect during our audit. Subsequent to the end of our fieldwork, OCC issued Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," on October 30, 2013.

⁴ The council is a formal interagency body empowered under 12 U.S.C. Chapter 34, Federal Financial Institutions Examination Council, to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and OCC. The council also makes recommendations to promote uniformity in the supervision of financial institutions. The MDPS program is a cooperative arrangement among the agencies for the achievement of shared and consistent supervisory goals and objectives. As a general rule, a technology service provider is considered for the MDPS program when the provider processes mission-critical applications for a large number of financial institutions that are regulated by more than one agency, thereby posing a high degree of systems risk, or from a number of data centers located in different geographic regions. As of December 2012, there were 15 technology service providers subject to the MDPS program.

framework for the direct oversight of these large technology service providers:

- *IT Examination Handbook: Supervision of Technology Service Providers*
- *Federal Regulatory Agencies' Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers*

The *IT Examination Handbook* also guides OCC examiners in the conduct of direct examinations of technology service providers.⁵ Such reviews are a part of OCC's supervision of third parties used by regulated institutions.

Our audit focused on OCC's supervision of individual financial institution's use of third parties. Accordingly, the direct examinations of technology service providers under the MDPS or by OCC were not included within the scope of this audit.

Results of Audit

OCC Has Updated Guidance to Banks on Managing Risks Related to the Use of Third Parties

During our audit period, OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," served as the guidance to banks on managing the risks related to third-party relationships. In this guidance, OCC established an expectation that boards of directors and management of banks should properly oversee and manage third-party relationships. OCC Bulletin 2001-47 was generally comprehensive but outdated. For example, it did not reflect the recent broader focus on operational risk rather than transaction risk.

⁵ While the MDPS program provides for interagency examinations of technology service providers, federal or state regulatory agency are not precluded from conducting an independent examination of any technology service provider that is servicing an insured financial institution for which the agency is responsible.

In October 2013, OCC issued updated risk-management guidance related to third-party relationships for national banks and federal savings associations. This issuance, OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," rescinded Bulletin 2001-47. OCC personnel stated that the new guidance provides a more comprehensive instruction for banks to ensure that third-party relationships, especially those that involve critical bank activities, are conducted in a safe and sound manner. We agree with this assessment. While the new guidance reiterates that a bank should adopt risk-management processes commensurate with the level of risk and complexity of its third-party relationships, it goes into greater detail than OCC Bulletin 2001-47 in defining attributes of an effective risk-management process for third-party relationships. These attributes include:

- plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party;
- proper due diligence in selecting a third party;
- written contracts that outline the rights and responsibilities of all parties;
- ongoing monitoring of the third party's activities and performance;
- contingency plans for terminating the relationship in an effective manner;
- clear roles and responsibilities for overseeing and managing the relationship and risk-management process;
- documentation and reporting that facilitates oversight, accountability, monitoring, and risk management; and
- independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

OCC Examiners' Review of the Use of Third Parties by Smaller Financial Institutions is Not Sufficiently Documented

We reviewed examination workpapers supporting OCC's supervision of 18 banks' use of third parties for the two most recent examination cycles. These institutions included 2 large banks, 2 midsize banks, 10 community banks, and 4 federal savings associations. For all banks, OCC examiners reached conclusions related to the banks' management of third parties; however, OCC had comprehensive workpapers documenting the nature and scope of the work performed to reach those conclusions for only four banks (two large banks, one midsize bank, and one federal savings association). Workpapers detailing examination procedures at the remaining, mostly smaller, institutions were limited. The quantity of workpapers supporting the conclusions at these banks varied but often did not identify the extent to which the institution used third parties, identify the degree of risk presented to the institution's operations by the third parties, or document detailed procedures that validated the institution's compliance with OCC Bulletin 2001-47.

OCC officials told us that examiners did evaluate the use of third parties at these institutions and that the work was generally targeted on assessing the institution's compliance with OCC Bulletin 2001-47. The nature and scope of this work depended on the examiner's knowledge of the institution, prior examination results, an assessment of the risk to the institution, and the resources available to the examination team. We noted that the "Community Bank Supervision" booklet of the *Comptroller's Handbook* allows for the execution of limited procedures (that is, minimum objectives) in areas where the examiners deem low-risk. For these areas, examiners determine whether significant changes have occurred in the bank's risk profile, including business activities, management performance, or condition of the area, as compared to the profile noted in the previous supervisory cycle. If, after completion of the minimum objectives, examiners identify no significant changes in the institution's risk profile, they can choose not to perform further work in the low risk area.

As noted previously, the workpapers that we reviewed often did not identify the extent to which the institution used third parties or the degree of risk presented to the institution's operations by these third parties. The workpapers often did not leave a clear audit trail or contain enough documentation to enable a reviewer to understand how OCC examiners reached their conclusions on third parties.

OCC officials also told us that variations in or absence of documentation detailing examiners' evaluation of third parties can be explained by the following factors:

- Given limited examiner resources, especially for smaller institutions, OCC examiners focus on documenting their work in areas considered high-risk and on supporting negative assertions that could be subject to challenge by the bank's management. As a result, based on their knowledge of the bank, examiners may not spend resources documenting the work supporting their conclusion when they know the third party or other area they are looking at is in "good shape". For example, examiners may have discussions on the topic of third parties and vendor management, but if it is determined that management's process is satisfactory, there may not be any documentation of these discussions in the workpapers.
- In such cases where a process is satisfactory, sign off by the examiner-in-charge (EIC) on the conclusion statement in the workpapers is considered sufficient to document that adequate work was performed to reach that conclusion.
- When evaluating the use of third parties in smaller institutions, the examiner's review will tend to be business-line oriented. Although there may not be documentation of the testing of specific third parties for compliance with the institution's vendor-management process, third parties may be evaluated during the review of the business line to which they relate. Our review of OCC workpapers found instances in which concerns with a third party were noted in the conclusion statements for specific business lines of the banks. While this indicates that the examiners reviewed third parties during their examination, the nature and extent of procedures applied to third parties were not usually described.

We acknowledge OCC's desire to have examiners focus examination procedures on areas of risk and its willingness to rely on the experience, institutional knowledge, and judgment of the examination team—especially the EIC. OCC policy PPM 5400-8 states that, in most cases, supervision workpapers need not include all of the data reviewed during a supervisory activity. However, the policy also states that workpapers must contain all essential information required to support conclusions about supervisory activities.⁶ In addition, workpapers should clearly document which examination procedures were performed and whether they were performed fully or partially. To comply with this guidance, we believe that workpapers should contain, at a minimum, a description of the procedures performed and the results of the review on which the conclusions are based.

Several publications describe aspects of third party examination:

- OCC Bulletin 2001-47 broadly addresses the OCC supervisory approach.
- Both the *FFIEC IT Examination Handbook* and *Federal Regulatory Agencies' Administrative Guidelines*, while directed toward IT examiners for use in IT focused exams, describe in detail the processes for examining service-provider governance.
- The "Community Bank Supervision" and "Internal and External Audits" booklets contain guidance and examination procedures addressing governance of outsourced internal audit arrangements.
- The "Retail Lending Examination Procedures" booklet of the *Comptroller's Handbook* provides detailed procedures to address the extent of third-party involvement in retail lending activities and evaluating the effectiveness of management's third-party oversight and risk-management processes.

However, the *Comptroller's Handbook* lacked separate guidance to cover examination procedures and documentation requirements for supervising an institution's governance of both IT and non-IT third

⁶ OCC, *Policy and Procedures Manual* (PPM) 5400-8 (REV), "Bank Supervision: Supervision Work Papers," Oct. 23, 2002.

parties during regular safety and soundness examinations. Specific guidance or training targeted at examination teams at similar institutions, with similar resource constraints, may prove useful to OCC in promoting sufficient documentation.

Recommendation

We recommend that the Comptroller of the Currency reinforce to examination staff the need for workpapers to contain essential information to support conclusions about banks' governance of third parties, as required by PPM 5400-8. Essential information should include the procedures performed and the results upon which the conclusions are based.

Management Response

OCC will issue a memorandum highlighting expectations for complying with PPM 5400-8 when examiners review a bank's risk regarding third-party service providers. OCC management will direct front line managers responsible for the supervision of community and midsize banks to discuss this issue with the examiners they supervise by September 30, 2014.

OCC will also incorporate references to OCC Bulletin 2013-29, its updated guidance on managing risks associated with third-party relationships, into relevant booklets of the *Comptroller's Handbook* as they cycle through the periodic review and revision process. In addition, the "Community Bank Supervision" booklet, which sets forth procedures for examining smaller banks, will be revised to include more explicit language and procedures for scoping reviews and ongoing monitoring of banks' reliance on third parties for critical services.

OIG Comment

OCC's planned corrective actions are responsive to our recommendation.

* * * * *

We appreciate the courtesies and cooperation provided to our staff during the audit. If you wish to discuss the report, you may contact me at (202) 927-0384 or James Lisle, Audit Manager, at (202) 927-6345. Major contributors to this report are listed in Appendix 3.

Jeffrey Dye /s/
Director, Banking Audits

Our objective was to evaluate the sufficiency of the Office of the Comptroller of the Currency's (OCC) existing procedures for supervising the use of third-party service providers (third parties) by national banks and federal savings associations, as well as the effectiveness of the application of these procedures. To accomplish these objectives, we:

- interviewed OCC personnel responsible for supervising banks' use of third parties;
- reviewed OCC examination policies, procedures, and guidance related to supervision of banks' use of third parties, as well as those issued by other federal regulatory agencies, such as the Board of Governors of the Federal Reserve System (FRB) and the Federal Deposit Insurance Corporation (FDIC);
- reviewed bulletins, bank guidance, and white papers, issued by the OCC and other federal regulatory agencies discussing risks involved in banks' use of third parties. These documents reviewed included: OCC Bulletin 2001-47, Third-Party Relationships: Risk Management Principles; OCC Advisory Letter 2000-9 Third Party Risk; OCC 2002-16 Bank Use of Foreign-Based Third Party Service Providers; OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance; FDIC Financial Institution Letter 44-2008 Guidance for Managing Third-Party Risk; FRB NY Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks October 1999; FRB Philadelphia Vendor Risk Management 1st Qtr 2011; and FRB DC SR-00-04 Outsourcing of Information and Transaction Processing; and
- reviewed workpapers covering two examination cycles for 18 banks selected in proportion to the number of banks in each of OCC's supervision categories.⁷ Typical documents reviewed

⁷ OCC supervises both national banks and federal savings associations. For supervision purposes, national banks are categorized by size: large banks include the largest national banking companies which generally are involved in the most complex activities and operate over wide geographic areas; midsize banks (generally assets of \$10 billion to \$50 billion); and community banks (generally assets of less than \$10 billion). According to data extracted from the institution directory at FDIC's website as of September 2012, OCC supervised 19 large banks, 17 midsize banks, 1,235 community banks, and 569 federal savings associations. We selected 2 large banks, 2 midsize banks, 10 community banks, and 4 savings associations for testing.

included reports of examinations, supervisory letters and/or conclusion memos, scope memos, examination planning request letters, core assessments, risk assessments, supervisory strategies, work activities, and examination procedures.

We performed our audit fieldwork from July 2012 through July 2013. We did not include reviews of technology service providers under the Federal Financial Institutions Examination Council (FFIEC) Multi-Regional Data Processing Servicer (MDPS) program or by OCC.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix 2
Management Comments



Office of the Comptroller of the Currency

Washington, DC 20219

April 7, 2014

Jeffrey Dye
Director, Banking Audits
Office of Inspector General
Department of the Treasury
Washington, DC 20220

Subject: Response to Draft Report

Dear Mr. Dye:

We have reviewed your draft report titled "OCC's Review of Banks' Use of Third Party Service Providers Is Not Sufficiently Documented." Your audit objective was to evaluate the sufficiency and effectiveness of OCC's procedures for supervising the use of third parties by national banks and federal savings associations (banks).

You found that OCC has updated guidance to banks on managing risks related to the use of third parties. You concluded, however, that OCC examiners' review of the use of third parties by smaller financial institutions is not sufficiently documented.

You recommend that the OCC reinforce to examination staff the need for workpapers to contain essential information to support conclusions about banks' governance of third parties, as required by PPM 5400-8. Essential information should include the procedures performed and the results upon which the conclusions are based.

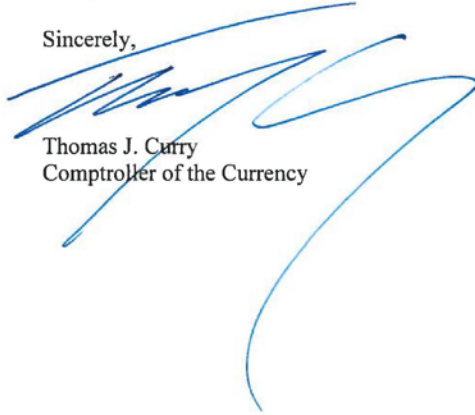
To that end, we will issue a memorandum highlighting expectations for complying with PPM 5400-8 when examiners review a bank's risk regarding third-party service providers. We will direct front line managers responsible for the supervision of community and midsize banks to discuss this issue with the examiners they supervise by September 30, 2014.

We will also incorporate references to OCC Bulletin 2013-29, our updated guidance on managing risks associated with third-party relationships, into relevant booklets of the *Comptroller's Handbook* as they cycle through the periodic review and revision process. In addition, the "Community Bank Supervision" booklet, which sets forth procedures for examining smaller banks, will be revised to include more explicit language and procedures for scoping reviews and ongoing monitoring of banks' reliance on third parties for critical services.

Appendix 2
Management Comments

If you need additional information, please contact me or Jennifer Kelly, Senior Deputy
Comptroller for Midsize and Community Bank Supervision, at 202-649-5420.

Sincerely,



Thomas J. Curry
Comptroller of the Currency

Appendix 3
Major Contributors to This Report

James Lisle, Audit Manager
Adelia Gonzales, Auditor-in-Charge
Marco Uribe, Auditor
Cecilia Howland, Referencer

Department of the Treasury

Deputy Secretary
Office of Strategic Planning and Performance Management
Office of the Deputy Chief Financial Officer, Risk and Control
Group

Office of the Comptroller of the Currency

Comptroller of the Currency
Liaison Officer

Office of Management and Budget

OIG Budget Examiner