Risk Management Principles for Third-Party Relationships

A Telephone Seminar for Community Banks

August 21, 2002, 2:00 p.m.—3:30 p.m. EDT

and again on

August 22, 2002, 11:00 a.m.—12:30 p.m. EDT

Contents

Speaker Biographies

John D. Hawke, Jr.

Comptroller of the Currency

John D. Hawke, Jr. was sworn in as the 28th Comptroller of the Currency on December 8, 1998. After serving for 10 months under a Recess Appointment, he was sworn in for a full five-year term as Comptroller on October 13, 1999.

The Comptroller of the Currency is the Administrator of National Banks. The Office of the Comptroller (OCC) supervises 2,200 federally chartered commercial banks and about 54 federal branches and agencies of foreign banks in the United States comprising more than half of the assets of the commercial banking system. The Comptroller also serves as a Director of the Federal Deposit Insurance Corporation, the Federal Financial Institutions Examination Council, and the Neighborhood Reinvestment Corporation.

Prior to his appointment as Comptroller, Mr. Hawke served for 3½ years as Under Secretary of the Treasury for Domestic Finance. In that capacity he oversaw the development of policy and legislation in the areas of financial institutions, debt management, and capital markets. He also served as Chairman of the Advanced Counterfeit Deterrence Steering Committee and as a member of the board of the Securities Investor Protection Corporation. Before joining Treasury, Mr. Hawke was a Senior Partner at the Washington, D.C., law firm of Arnold & Porter, which he first joined as an associate in 1962. At Arnold & Porter he headed the Financial Institutions practice, and from 1987 to 1995 he served as Chairman of the firm. In 1975 he left the firm to serve as General Counsel to the Board of Governors of the Federal Reserve System, returning in 1978.

Mr. Hawke was graduated from Yale University in 1954 with a B.A. in English. From 1955 to 1957 he served on active duty with the U.S. Air Force. After graduating in 1960 from Columbia University School of Law, where he was Editor-in-Chief of the Columbia Law Review, Mr. Hawke was a law clerk for Judge E. Barrett Prettyman on the United States Court of Appeals for the District of Columbia Circuit. From 1961 to 1962 he served as counsel to the Select Subcommittee on Education in the House of Representatives.

From 1970 to 1987 Mr. Hawke taught courses on federal regulation of banking at the Georgetown University Law Center. He has also taught courses on bank acquisitions and financial regulation and serves as the Chairman of the Board of Advisors of the Morin Center for Banking Law Studies. In 1987 Mr. Hawke served as a member of a Committee of Inquiry appointed by the Chicago Mercantile Exchange to study the role of futures markets in connection with the stock market crash in October of that year.

Mr. Hawke has written extensively on matters relating to the regulation of financial institutions, and is the author of Commentaries on Banking Regulation, published in 1985. He was a founding member of the Shadow Financial Regulatory Committee, and served on the committee until joining Treasury in April 1995.

Mr. Hawke is a member of the Cosmos Club, the Economic Club of Washington, and the Exchequer Club of Washington.

Born in New York City on June 26, 1933, Mr. Hawke resides in Washington, D.C. He was married in 1962 to the late Marie R. Hawke and has four adult children, Daniel, Caitlin, Anne, and Patrick, and one grandchild, Spencer Patrick Hawke.

Kirk Spurgin

National Bank Examiner and Core Policy Development Analyst

Chief National Bank Examiner's Office

Kirk is a core policy development analyst in the Chief National Bank Examiner department. The Core Policy Development division is responsible for developing regulatory policy for national banks in areas such as corporate governance, audit and controls, and supervision by risk. Kirk's primary responsibilities pertain to policy development in the arena of board and management supervision.

A native of Texas, Kirk joined the OCC in 1981 after graduating from Hardin-Simmons University in Abilene, Texas, with a bachelor of business administration degree in accounting. He spent approximately 10 years as a community bank examiner in various locations in Texas in the 1980s and early 1990s. He then transferred to San Francisco, where he managed the problem bank and examination support divisions. Kirk spent two years in the large banks program in San Francisco before relocating to Washington, D.C., and joining the Core Policy Development division in 2001.

Gregory J. Isaacs

National Bank Examiner and Credit Risk Specialist
Chief National Bank Examiner's Office

Greg is a national bank examiner and retail credit specialist for the Chief National Bank Examiner department, Credit Risk division of the OCC. The Credit Risk division is responsible for developing regulatory policy and supervisory support for national banks in the areas of credit risk related to underwriting, portfolio quality, and operations.

Greg is a native of Nebraska and graduate of the University of Nebraska--Lincoln. He began his career in the OCC's Midwestern District in 1992. His experiences are varied and include community, mid-sized, and large bank supervision. His primary emphasis has been credit risk, specifically retail-related credit risk, for the past several years. Prior to his current assignment, Greg served as a national OCC resource for retail credit examinations.

Greg's credit risk supervision responsibilities for third-parties have included, reviews of commercial and retail brokers and dealers (e.g., mortgage, vehicle, industrial equipment), merchant processing independent sales and service organizations, credit card and other consumer product marketing and servicing companies, loan wholesalers and resellers, and finance companies.

Mike Koll

National Bank Examiner and Information Technology Lead Expert

Midwestern District

Since 1997, Mike has served as the lead information technology expert, responsible for bank information technology (BIT) supervision, in the OCC's Midwestern District. Prior to that he served as a bank information systems manager for four years, working on bank information technology related supervision of national banks.

He joined the OCC in 1983, after being graduated from the University of Minnesota in 1982. He has continued to work on information technology since 1986: nine years on issues related to larger regional banks and independent servicers and eight years in policy development for information systems and technology. This experience includes developing OCC guidance on information security, contingency planning, technology risk management, Internet banking risks and controls, and participation in developing the Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook. He obtained CISA certification in 1990.

Mike also has taught the OCC's Internet banking course, including segments on encryption, PKI, and digital signatures. Mike's work on information-technology-related supervision includes evaluating third-party relationships, from both the serviced financial institution and service provider perspectives.

James F.E. Gillespie Jr.

Assistant Chief Counsel

Law Department

James (Jeff) Gillespie currently serves as assistant chief counsel responsible for the management of special projects, particularly those that involve electronic banking. He also co-authored, with OCC First Senior Deputy Comptroller and Chief Counsel Julie Williams, a recent law review article on risk management of third-party relationships, "The Impact of Technology on Banking: The Effect and Implications of 'Deconstruction' of Banking Functions" (North Carolina Banking Institute, April 2001).

Jeff joined the OCC in 1979 after completing a federal judicial clerkship. He has held management and staff positions in the Legislative and Regulatory Activities Division, the Corporate Organization and Resolutions Division, the Litigation Division, the Legal Advisory Services Division, and the Legislative Counsel Division. He holds a J.D. from Indiana University (1976), where he was graduated summa cum laude and Order of the Coif. He received a B.A. from Ohio Wesleyan University (1971).

Electronic Polling Question

ELECTRONIC POLLING QUESTION

How many people are at your listening site? Press:

1 for one person,
2 for two people,
3 for three people,
4 for four people,
5 for five people,
6 for six people,
7 for seven people,
8 for eight people, or
9 for 9 or more people listening at your site.

Presentation

Risk Management Principles for Third-Party Relationships

A Telephone Seminar for Community Banks

August 21 and August 22, 2002

Comptroller of the Currency
Administrator of National Banks

Risk Management Principles For Third-Party Relationships

A Telephone Seminar for Community Banks

Wednesday, August 21, 2002
and
Thursday, August 22, 2002

Comptroller of the Currency
Administrator of National Banks

OCC 2001-47: An Overview

- Why guidance on third parties?
- Types of third-party arrangements subject to this guidance
- Risks associated with third-party arrangements
- **OCC's expectations for a sound risk management process**
- Focus on:
  - ✓ *outsourced technologies*
  - ✓ *credit-related activities*
- Q & A

Comptroller of the Currency
Administrator of National Banks

Third-Party Guidance

OCC Bulletin 2001-47	Third-Party Relationships: Risk Management Principles
OCC Bulletin 2002-16	Bank Use of Foreign-Based Third-Party Service Providers
OCC Bulletin 2001-31	Weblinking
OCC Bulletin 2001-8	Guidelines Establishing Standards for Safeguarding Customer Information
OCC Advisory Letter 2000-12	Risk Management of Outsourcing Technology Services
OCC Advisory Letter 2000-9	Third-Party Risk
OCC Bulletin 98-38	Technology Risk Management: PC Banking
OCC Bulletin 98-3	Technology Risk Management
OCC Banking Circular 181 (rev)	Purchases of Loans in Whole or in Part—Participations

A more complete list is in the appendix of OCC Bulletin 2001-47.

All emphasize risk analysis, controls, and monitoring that are consistent with risk tolerances and abilities.

Comptroller of the Currency
Administrator of National Banks

Why guidance on third parties?

- OCC or the Federal Financial Institutions Examination Council has issued other guidance on vendor management for specific types of activities
- OCC 2001-47 consolidates previously issued guidelines into one “umbrella” policy that is broadly applicable to most types of third-party activities
- Examiners are citing instances of ineffective implementation and management of third-party arrangements more frequently
- In some cases, control of the activity has been relinquished to the third party
- Poor oversight has resulted in sizable financial loss, including the need for capital restoration in some cases

Types of Third-Party Activities

- A third party performs functions on the bank's behalf -- commonly referred to as *"outsourcing"*

  Examples:

  ✓ Technology services
  ✓ Internal audit
  ✓ Loan review
  ✓ Back-office functions

- A bank provides products and services originated by or predominantly offered by a third party

  Examples:

  ✓ Insurance and nondeposit investment products
  ✓ Payday lending, credit repair products, check cashing services
  ✓ Loan participations

Risks

Reputation risk arises when a third party's service or products don't meet the expectations of the bank's customers, or when the third party or line of business is subjected to public scrutiny or experiences negative publicity.

Strategic risk arises when a bank doesn't perform an adequate risk assessment or possess sufficient knowledge about a new product, business line, or activity—or when the activity is inconsistent with the bank's goals or doesn't provide the expected return on investment.

Compliance risk arises when the third party's operations are not in compliance with law or the bank's internal policies and procedures, and when audit and control features are weak or nonexistent. Banks must take special care to avoid violating fair lending and consumer protection laws.

Transaction risk arises when the third party is unable to deliver its product or provide its service due to error, fraud, or technology failure. Ineffective business continuity planning increases transaction risk.

Credit risk arises from the third party's failure to meet the terms of the contract or otherwise to perform as agreed, and when the quality of loans marketed or originated by the third party is inferior.

Comptroller of the Currency
Administrator of National Banks

General Expectations

- OCC expects banks to manage third-party arrangements in a safe and sound manner and in compliance with law
- Underlying controls should be the same as if the bank were conducting the activity directly
- Third-party arrangements do not “wash management’s hands” of the responsibility of managing the risks
- Not a “one-size-fits-all” approach
- Each bank’s risk profile is unique and requires a tailored risk-management approach appropriate for:
  - Scale and complexity of its particular third-party arrangements
  - Materiality of the risks present
  - Ability of the bank to manage those risks
- National banks should adopt a risk-management process to identify, monitor, manage, and control the risks posed by the activity

Risk-Management Process

National banks should adopt a dynamic risk-management process over third-party arrangements that includes:

1. An assessment of the risks involved in the activity and whether it coincides with the bank's strategic goals
2. Due diligence to identify and select a third-party provider
3. Written contracts that outline duties, obligations, and responsibilities of both parties
4. Ongoing oversight of the third party and third-party activities

1. Strategic Planning/ Risk Assessment

Comptroller of the Currency
Administrator of National Banks

Identify strategic goals, objectives, and business needs

- What can the activity do for the bank?
- Does it coincide with the bank's strategic goals?
- Can a third party help the bank achieve its goals?

Identify risks of the proposed third-party activity

- Use compliance officer, internal auditor, legal counsel to help analyze risks

Assess internal expertise to evaluate and manage the third-party arrangement

- Does the bank have the expertise to understand and oversee the risks and the resources to monitor and measure the performance of the third party?

Identify infrastructure to manage the risks

- Determine due-diligence standards, performance criteria, internal controls, and management information systems (MIS) needed

Measure cost/benefit relationship

- Identify cost of development, implementation, and support
- Measure potential short-term profits or cost savings vs. long-term stability and viability

The risk assessment provides the foundation upon which you develop and maintain your risk-management program.

Strategic Planning/Risk Assessment
Credit-Related Issues

Comptroller of the Currency
Administrator of National Banks

- Fundamental issues need to be addressed **prior** to entering into an arrangement—expertise, resources, and controls
- A little homework up-front
  - Provides for potential savings in:
    - Time, costs, and resources
  - Provides for a greater chance of success
- Primary areas of difficulty
  - Entering credit relationships that are outside management's lending experiences
    - Expertise
    - Market or trade area
  - Failing to recognize and mitigate the risk
  - Underestimating the risk involved
  - Failing to devote the appropriate resources **prior to** implementation

Strategic Planning/Risk Assessment
Credit-Related Issues

- Insufficient expertise
  - First example: Ocean-going vessel and airplane loans
    - Bank used commercial brokers and indirect lending arrangements to originate and purchase loans
    - Bank did not understand the specialized lien perfection process
    - Bank did not understand the difficulties in locating, repossessing, and liquidating the collateral
    - Result: Millions in unsecured and questionable collateral values

Strategic Planning/Risk Assessment
Credit-Related Issues

- Insufficient expertise (continued)
  - Second example: Truck and trailer leases
    - Wanted to diversify loan portfolio/reduce industry concentration
    - Began purchasing truck and trailer leases nationwide through a third party
    - Within 12 months the bank funded leases comprising 100% of capital
  - Problems discovered
    - Leasing company curtailed collecting and remitting lease payments to the bank
    - Delinquency rate near 50%
    - Title problems

Strategic Planning/Risk Assessment
Credit-Related Issues

- Insufficient experience—leasing example (continued)
  - Why did the strategy fail?
    - Bank did not have leasing expertise and did not understand the leasing business, particularly the trucking industry
    - No formal servicing agreement with leasing company
    - No documentation review
- Outside market/trade area
  - Previous examples provide illustration of what can happen when lending outside the bank's trade area
  - Banks often do not factor into planning and risk assessment:
    - Increases in costs of collection activities
    - Dealer, broker, and other third-party reputations
    - Market differences

Strategic Planning/Risk Assessment
Credit-Related Issues

- Resource considerations
  - Sufficient risk-management resources to analyze and monitor third-party processes
    - New systems/infrastructure
    - MIS
    - Staffing
  - Capital and loss reserves to support the activity
- Two important documents in addition to OCC Bulletin 2001-47
  - OCC Banking Circular 181 (rev)
    - Prudent loan purchase and loan participation practices
  - OCC Advisory Letter 2000-9
    - Key components of third-party risk management practices
    - Examples of third-party problems and issues

Strategic Planning/Risk Assessment
IT-Related Issues

- Determine what level of expertise management needs to maintain in-house
- Integrate with existing technology infrastructure
  - Can reports be shared seamlessly with existing systems?
  - Does the service fit the future plans for the company's technological structure?
- Assess impact on the bank's control environment
  - Does the service introduce additional risks?
  - Will existing controls provide adequate security, integrity, confidentiality?
- Assess the impact on the bank's information security plan required by GLBA Section 501b
  - Who handles day-to-day compliance?
  - What changes will need to be made to the existing plan?
- Determine durability of the product/service
  - Constant change/revision?
  - Long-term, stable seller?

2. Due Diligence

Evaluate third party's experience in implementing and supporting the proposed activity

- Determine that the third party's culture, vision, and business style fit with the bank
- Check references, including peer institutions and industry groups
- Contact Better Business Bureau, state attorneys general office, state consumers affairs offices
- Consider checking backgrounds and reputations of company principals

Determine adequacy of third party's risk-management infrastructure

- MIS, internal controls, systems security, use of confidential customer information, and contingency planning
- Determine reliance on subcontractors

Analyze third party's financial information

- Would the bank extend credit to the third party?
- Audited statements should be required for material activities and relationships
- Adequacy of insurance coverage

Due Diligence
Credit-Related Issues

- Due-diligence process is critical to entering a third-party credit arrangement
  - Understand business and operations
  - Review financial condition and reputation
  - Review quality of receivables
  - Review marketing, origination, collection, and servicing practices
  - Ask questions prior to beginning third-party activities
- Basic questions
  - Would my bank make a loan to this company based on its operations, reputation, and financial wherewithal?
  - If we do this deal, how easily and timely will it be to discontinue operations if found unsatisfactory once into the arrangement?

Due Diligence
Credit-Related Issues

- OCC Banking Circular 181 (rev)—Purchases of Loans In Whole or In Part—Participations
  - Written lending policies and procedures governing transactions
  - Independent analysis of credit quality by the purchasing bank prior to purchase and throughout the life of the loan
  - Agreement by the obligor to make full credit information available to the seller
  - Agreement by the seller to provide available information on the obligor to the purchaser
  - Written documentation outlining rights and obligations of each party

Due Diligence
Credit-Related Issues

- Basic premise of conducting an independent credit analysis applies to most third-party loan arrangements
  - Banks must be conducting sufficient analysis to make a sound underwriting decision
  - Analysis needs to be completed no matter from whom the loan is purchased
- Why do I need to know the financial situation of the third-party marketer (using bank to originate loans) when they buy all the loans we fund and take all the liability?
  - Credit risk may be mitigated but is not extinguished—the bank is dependent on the third party's continued ability to buy the loans
  - Prior to purchase of loans or if unable to purchase the loans, the third party puts earnings and capital at risk, especially with some of the higher risk loan arrangements

Due Diligence
Credit-Related Issues

- Failure to understand the third party's activities
  - Example
    - Bank outsourcing servicing of credit card and merchant processing
    - Contract did not include fraud monitoring
- Operational and functional area reviews
  - Critical to understanding activities performed
  - Does the company have controls in place to perform the activities in a safe and sound manner and in compliance with laws and regulations?
  - Can the company provide the MIS needed for monitoring its activities?
  - If the answer to these questions is "no," the bank may need to reconsider doing business with the entity

Due Diligence
Credit-Related Issues

- Operational and functional area reviews (continued)
  - Allows time to contemplate quality assurance needs and audit expectations
    - Financial audits
    - Operational audits
    - Quality assurance reviews
    - Loan reviews
  - Financial audits are only part of the picture depending upon the third-party activities
  - Bank needs a strong working knowledge of how activities are being performed in the case of delegating functions such as initial underwriting and collections
    - Are the activities performed to the bank's standards?

Due Diligence
Credit-Related Issues

- Example: Delegating and outsourcing several activities
  - Third parties performing nearly all marketing, initial underwriting, and collections
  - Activities working fine for first 12 months
  - Lender-approved marketer to introduce new subprime unsecured product
    - Growth of new product more than 100,000 accounts per month
    - Delinquencies and losses increase rapidly (over 50% annualized losses
    - Bank's shareholders injected well over $100 million in capital to maintain adequate reserve and capital levels before deciding to voluntarily liquidate the bank's remaining assets at a deep discount

Due Diligence
Credit-Related Issues

- Example: Delegating and outsourcing several activities (continued)
  - What happened?
    - Primary issue was failure of bank's due diligence of third-parties' abilities and capacity prior to introducing the new product
    - Staffing inadequate at all the third parties used to handle the rapid growth
      - Customer service bombarded with complaints
      - Underwriting overwhelmed, failed to apply any of the credit criteria
      - Collections unprepared for volume of problem accounts
    - Planning and due-diligence phases for the new product could have identified the problems
    - Marketing would have been curtailed if proper monitoring employed

Due Diligence
IT-Related Issues

- Is the company/service new?
  - Difficult to analyze financial viability
  - Hard to judge customer satisfaction
  - "Dot com" bubble burst restricts access to additional funds
- What information is available to review?
  - Is a SAS-70 available with a scope sufficient to assess control issues and risks important to the bank?
  - Will company provide a list of customers and companies that said "no"?
- Do user groups exist?
  - Check with them to see what their current levels of satisfaction/dissatisfaction are
  - See if they provide any independent reports on service performance vs. promises
- Determine how the vendor provides the service
  - Do they do all the processing themselves?
  - May find that vendor outsources key portions of the process
- Strategic planning/due diligence examples
  - Vendor mergers—surprised by merger's impact on customers/employees
  - "Who's got the data?"—data on server not owned by bank's vendor
  - Wireless network—no one at bank understands risks

3. Contracts

Comptroller of the Currency
Administrator of National Banks

Banks should consider the following issues in contracts with third parties:

- Scope of arrangement (content, format, frequency, etc.)
- Fees and costs, including purchasing and maintaining hardware and software
- Performance measures or benchmarks
- Management reports (frequency and type)
- Audit requirements and reports (financial, security, internal control)
- Security and confidentiality (including GLBA 501b requirements)
- Business continuity planning
- Default and termination
- Ownership and license
- Indemnification
- Insurance coverage
- Dispute resolution
- Customer complaints
- *The performance of services by external parties for the bank is subject to OCC examination oversight.*

Contracts
Credit-Related Issues

- Planning, risk assessment, and due diligence are fundamental to contract provisions
- Financial information requirements
  - Critical to receive timely, accurate, and meaningful financial information
    - Conduct periodic analyses of loan purchases and participations
    - Review financial wherewithal of third parties performing servicing activities such as marketing, customer service, and collections
    - Review financial wherewithal of third parties the bank is dependent upon to continue buying loans or sharing liability

Contracts
Credit-Related Issues

- Responsibilities
  - Leasing example (strategic planning section) is a classic example of the importance of outlining the servicing responsibilities of third-parties
    - Failure to collect and remit payment to the bank
    - Failure to provide proper documentation
  - Credit card and merchant processing example (due diligence section) is another example of the importance of contract provisions
    - Failure to monitor transactions for fraud or conduct chargeback processing

Contracts
Credit-Related Issues

- Liability and recourse arrangements
  - Not always aware of potential liability
  - Merchant processing example
    - Many agent bank agreements indicate the bank has liability if a merchant cannot cover chargebacks
    - Illustrates importance of reviewing contracts
- Example: Overdraft protection
  - Third party indicated no credit risk because the activity was not a loan
  - Third party created specialized monitoring reports but no mention of sharing MIS with bank
  - Contract provided bank no form of recourse in the event of credit performance or customer service issues . . . only provided recourse and termination in the event profitability hurdles were not achieved

Contracts
IT-Related Issues

Key provisions in IT contracts:

- Data ownership
  - Data may be largest asset in bankruptcy
  - May not have access to it if not specified
- Service level agreements:
  - Response time
  - System availability
  - Data integrity benchmarks
  - Report availability
- Responsibilities in key areas:
  - Customer complaints
  - Intrusion detection/monitoring
  - Security, including Gramm-Leach-Bliley Act 501b compliance
  - Business continuity planning

Key provisions in IT contracts (cont.):

- Bank access to audit reports
- Example—Contract didn't provide for access to financial and audit information
- *The performance of services by external parties for the bank is subject to OCC examination oversight.*

4. Ongoing Oversight

Comptroller of the Currency
Administrator of National Banks

Monitor financial condition

- At least annually—more frequently for riskier activities
- Require audited financial statements for significant activities or relationships
- Determine that third party's obligations to subcontractors are being met
- Review third party's insurance coverage

Monitor controls

- Review audits, security reviews, regulatory reports
- Review policies relating to internal control and security
- Review business continuity planning and testing
- Participate in user groups

Assess quality of service and support

- Review performance relative to contractual obligations and bank objectives
- Review complaints
- Consider administering mystery shopper, customer call-back, or customer satisfaction programs
- Determine adequacy of training provided to bank employees

Determine if the return on investment is in line with plan

Ongoing Oversight
Credit-Related Issues

- Credit-related problems
  - Poor understanding of activities performed by the third party
  - Improper or inaccurate MIS reporting established
  - No functional/operation reviews performed
  - No quality assurance reviews or audits performed
  - No ongoing financial monitoring completed
  - No loan concentration monitoring performed
- Many of the examples provided in the other sections indicate the importance of monitoring

Ongoing Oversight
Credit-Related Issues

- Additional examples
  - Indirect dealer and broker arrangements
    - Important to have MIS to track the performance of loans purchased from individual dealers and brokers
    - Analysis of credit booked and ongoing performance often indicates if the decision was wise from a credit and profitability perspective
    - Poor performance or changing performance can indicate changes in the business practices of a dealer or broker (e.g., new versus used vehicles or expanded marketing)

Ongoing Oversight
Credit-Related Issues

- Additional examples (continued)
  - Improper monitoring of delegated underwriting (where bank relies on third party to conduct underwriting with final approval coming from the bank)—common when the bank is acting as a conduit for payday lenders and subprime credit card marketers
    - Failure to review the third party's adherence to underwriting standards
    - Failure to create a quality assurance review process for the final approval
    - Results in potential booking of loans not meeting underwriting standards as well as opportunity to book fictitious/fraudulent loans
    - Risk is compounded if collection activities are poor or manipulated by the same party

Ongoing Oversight
Credit-Related Issues

- Additional examples (continued)
  - Reputation and compliance issues
    - Risk for third-party credit arrangements is not only credit risk
      - Justice Department recently levied fines for abusive practices and discrimination against an institution
      - Third-party marketers violated Equal Credit Opportunity Act by actions
      - Institution either did not know about or ignored the activities
      - Result: over $1 million reimbursement

Monitor financial condition

- May be difficult in many situations
  - Privately held companies
  - “Dot com” start-ups
- Key asset may be largely intangible
  - Value of software developed
  - Goodwill from mergers/assumptions
- Atypical balance sheets
  - Intangible assets
  - Goodwill
  - Analyze this info to the best of your ability

Assess quality of service and support

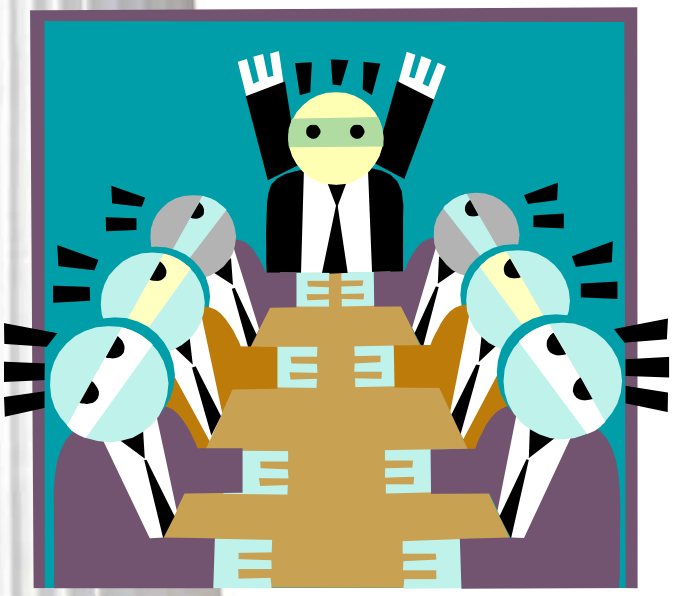
- Without service level agreements, difficult to define “good,” “poor,” and “fair” performance
- Frequency of performance data can be a key factor in determining service quality
- If using a third party for customer support, who defines “dissatisfied customer?”
- How quickly can bank change product terms, conditions?
- Does company respond well to bank concerns?

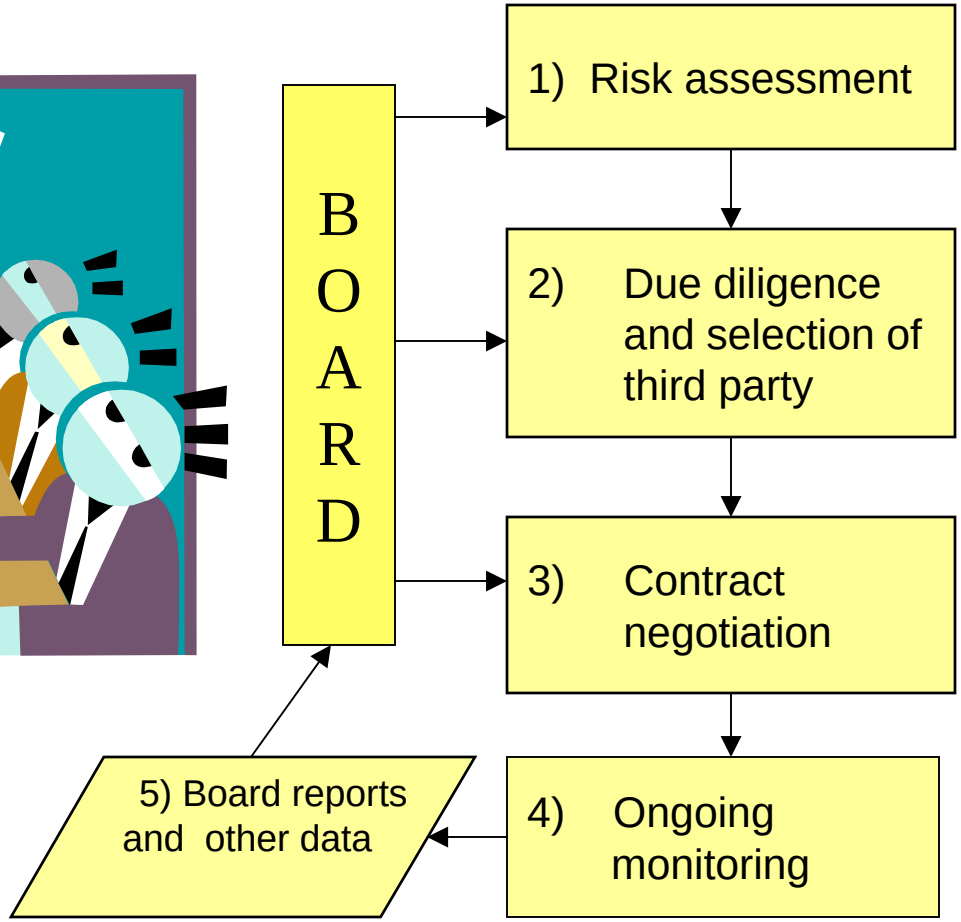
Monitor controls

- Review SAS-70 reports
- Request regulatory report from your primary regulator
- Understand bank responsibilities for business continuity planning and participate in tests
- Review vulnerability assessments and penetration test results
- Example—Bank “hacked” using known vulnerability

Dynamic Risk Management Process
Over Third-Party Arrangements

Comptroller of the Currency
Administrator of National Banks





The board should be involved in the entire process.

What will examiners want to look at?

- In assessing your risk management system, examiners may want to review:
  - ✓ Business plans for significant new products using third parties or newly outsourced functions
  - ✓ Results of due-diligence reviews
  - ✓ Contracts
  - ✓ MIS from third party
  - ✓ Information provided to board reflecting results of ongoing monitoring activities
- *Examiners will criticize banks whose third-party activities pose undue risk or whose risk management systems over such activities are inadequate or ineffective.*

Recap

- Third-party arrangements can be a legitimate and safe way to gain a competitive edge and improve earnings.
- Management and the board remain responsible for managing the relationship.
- Risk-management system should be commensurate with the risks posed by the arrangement and management's expertise to oversee the activity.
- Third-party arrangements should be subject to the same risk-management, privacy, security, and consumer protection policies that would be expected if the bank were conducting the activities directly.

Appendix

OCC 2001-47

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Third-Party Relationships

Description: Risk Management Principles

TO: Chief Executive Officers of National Banks, Federal Branches and Agencies, Service Providers, Software Vendors, Department and Division Heads, and Examining Personnel

PURPOSE

This bulletin provides guidance to national banks on managing the risks that may arise from their business relationships with third parties. It supplements, but does not replace, previous guidance on third-party risk. The principles presented are largely derived and adapted from supervisory principles that the OCC or the federal banking agencies have already issued.[1]

A bank's use of third parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Many third-party relationships should be subject to the same risk management, security, privacy, and other consumer protection policies that would be expected if a national bank were conducting the activities directly.

The OCC expects the boards of directors and management of national banks to properly oversee and manage third-party relationships. National banks should adopt a risk management process that includes:

- A risk assessment to identify the bank's needs and requirements;
- Proper due diligence to identify and select a third-party provider;
- Written contracts that outline duties, obligations, and responsibilities of the parties involved; and
- Ongoing oversight of the third parties and third-party activities.

The risk management principles identified in this guidance are intended to be used as tools for banks and adapted as necessary to reflect specific circumstances and individual risk profiles. In practice, a bank's risk management system should reflect the complexity of its third-party activities and the overall level of risk involved. Each bank's risk profile is unique and requires a

[1] Additional guidance on third-party relationships can be found in the documents listed in the appendix of this document.

tailored risk mitigation approach appropriate for the scale of its particular third-party relationships, the materiality of the risks present, and the ability of the bank to manage those risks.[2]

No single system is ideal for every bank. Large banks typically require sophisticated risk management systems involving a complex and diverse array of third-party products and services. On the other hand, community banks may be able to adopt this guidance in a less formal and systematic manner because of the relative simplicity of their risk exposures and management's direct knowledge of the third parties. The OCC does not view the supervisory principles in this guidance as all-inclusive, since many risk management techniques and controls are evolving rapidly to keep pace with new technologies and business applications.

BACKGROUND

More and more banks are looking to third-party relationships as a way to gain a competitive edge. The OCC recognizes that third-party relationships can offer banks a variety of legitimate and safe opportunities to improve financial performance. With the rapid evolution of the financial services industry, many national banks are utilizing third-party relationships by implementing advanced technologies, leveraging expertise, and specializing in core competencies. Through effective use of third-party relationships, banks can enhance product offerings, diversify assets and revenues, access superior expertise and industry best practices, devote scarce human resources to core businesses, facilitate operations restructuring, and reduce costs. Third-party relationships also enhance opportunities for banks to provide particular products or services when banks have strategic or operational advantages in producing or delivering those products or services.

Banks utilize third parties in three main ways[3]:

1. **To perform functions on the bank's behalf.** A bank contracts with third-party servicers to perform functions of the bank's operations rather than conduct them internally (commonly referred to as "outsourcing").

   This type of third-party relationship covers a wide variety of arrangements, including core information and transaction processing. Banks also may use third-party servicers to provide back-office management and support, such as electronic funds transfer, payroll processing, and mortgage servicing. More recently, banks are contracting with third-party servicers to provide Internet banking services, bill payment, bill presentment, account aggregation, digital

[2] National banks that provide services to other national banks should expect to be held to the same standards of due diligence, controls, and oversight as they would apply to their servicing entities.

[3] Third parties subject to this guidance may be bank or nonbank, regulated or nonregulated, foreign or domestic, affiliated or independent. National banks considering operating subsidiaries, financial subsidiaries, and minority interests as service providers should refer to OCC regulations 12 CFR 5.34, 5.36, and 5.39 regarding the permissibility of the activities to be conducted. Also, affiliate relationships are subject to their own rules. See sections 23A and 23B of the Federal Reserve Act, 12 USC 371c and 12 USC 371c(1).

certification, merchant processing activities, and customer call centers. In addition, some banks have outsourced internal functions such as loan review, asset management, network security management, human resources administration, treasury operations, and internal audit.

2. **To provide products and services that the bank does not originate.** A bank makes available to its customer products and services produced by third parties.

   A bank can expand products and services using third-party relationships to remain competitive and meet customer needs. For example, a national bank may enter into joint marketing relationships in which the bank sells to its customers nonbank products (e.g., nondeposit investments or insurance) made available by a brokerage firm or insurance company. A bank may choose to sell these products as principal or agent directly on its premises or make them available as a finder to its customers over the Internet by means of links on the bank's Web site to the Web sites of the third parties.

3. **To "franchise" the bank's attributes.** The bank lends its name or regulated entity status to products and services originated by others or activities predominantly conducted by others.

   Banks authorizing third parties to conduct business in the banks' name is potentially the most problematic of the third-party relationships and often warrants significant additional supervisory scrutiny by the OCC. This third-party activity takes many forms, from complete pass-through type arrangements, in which the bank basically receives a fee in return for the use of its name, to more participatory arrangements on the bank's part.

   The risks to the bank from these franchising arrangements vary based on the terms of the agreement between the bank and third party and the nature of the products offered. In all of these relationships with third parties, however, the bank must conduct adequate due diligence of all third parties and understand the market, customer base, products offered, and attendant risks prior to entering into contractual relationships. Franchising activities often involve significant reputation, strategic, transaction, and compliance risk to the bank.

   National banks should be especially mindful of any third party seeking to avail itself of the benefits of a national bank charter, particularly with respect to the application of state and local law. In some instances, nonbank vendors may target national banks to act as delivery vehicles for certain products and services, or to act as the nominal deliverer of products or services actually provided by the third party, in order to avoid state law standards that would otherwise apply to their activities. Further, some product vendors engage in practices that may be considered predatory, abusive, or unfair and deceptive to consumers under OCC guidelines.

   Whenever a bank permits itself to be used as a delivery vehicle for products or services that are offered under the bank's name, but provided by an unrelated third party, it can be exposed to substantial financial loss and damage to its reputation if it fails to maintain adequate quality control over those products and services and adequate oversight over the third-party activities. National banks that participate in this kind of program with nonbank

vendors or marketers should take special care to avoid violating fair lending and consumer protection laws and regulations, particularly when the actual involvement of the bank and the third party may be invisible to the customer. National banks should be extremely cautious before entering into any third-party relationship in which the third party offers products or services through the bank with fees, interest rates, or other terms that cannot be offered by the third party directly. Such arrangements may constitute an abuse of the national bank charter.

The OCC will scrutinize carefully any such arrangement and may use its supervisory authority to examine the operations of third parties who act as service providers to national banks which are sought out to deliver potentially abusive, predatory, or unfair and deceptive products. Accordingly, the OCC will likely conduct regular examinations of both the bank and the third party to assess the risks associated with these activities.

RISKS ASSOCIATED WITH THIRD-PARTY RELATIONSHIPS

Reliance on third-party relationships can significantly increase a bank's risk profile, notably strategic, reputation, compliance, and transaction risks. Increased risk most often arises from poor planning, oversight, and control on the part of the bank and inferior performance or service on the part of the third party, and may result in legal costs or loss of business. To control these risks, management and the board must exercise appropriate due diligence prior to entering the third-party relationship and effective oversight and controls afterward.

Strategic risk. Strategic risk is the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions. National banks are individually exposed to strategic risk if they use third parties to conduct banking functions or offer products and services that are not compatible with the bank's strategic goals or that do not provide an adequate return on investment. Strategic risk exists in banks that, in an effort to remain competitive or boost earnings, use third-party relationships without fully performing due diligence reviews or implementing the appropriate risk management infrastructure to oversee the activity. Strategic risk also arises if management does not possess adequate expertise and experience to properly oversee the activities of the third party. The board and management should fully understand the key risks associated with the use of third-party relationships.

Reputation risk. Reputation risk is the risk to earnings or capital arising from negative public opinion. Third-party relationships that do not meet the expectations of the bank's customers expose the bank to reputation risk. Poor service, disruption of service, inappropriate sales recommendations, and violations of consumer law can result in litigation, loss of business to the bank, or both. In particular, when the third party's employees interact directly with bank customers (in joint marketing arrangements or from call centers, for example), such arrangements pose reputation risk if the interaction is not consistent with the bank's policies and standards. Also, publicity about adverse events surrounding the third parties may increase the bank's reputation risk. Banks that use third-party relationships to offer new products or services or expand existing ones should closely monitor the quality and appropriateness of the provider's products and services to ensure ongoing customer satisfaction.

Compliance risk. Compliance risk is the risk to earnings or capital arising from violations of laws, rules, or regulations, or from nonconformance with internal policies and procedures or ethical standards. This risk exists when products, services, or systems associated with the third-party relationship are not properly reviewed for compliance, or when the third party's operations are not consistent with law, ethical standards, or the bank's policies and procedures. The potential for serious or frequent violations or noncompliance exists when a bank's oversight program does not include appropriate audit and control features, particularly when the third party is implementing new bank activities or expanding existing ones. Compliance risk increases when privacy of consumer and customer records is not adequately protected, when conflicts of interest between a bank and affiliated third parties are not appropriately managed, and when a bank or its service providers have not implemented an appropriate information security program. Banks should involve their compliance management function in the due diligence and monitoring process when third-party products or services present significant risk to regulatory compliance.

Transaction risk. Transaction risk is the risk to earnings or capital arising from problems with service or product delivery. Transaction risk is evident in each product or service offered by the third party. Transaction risk can increase when the products, services, delivery channels, and processes that are designed or offered by a third party do not fit with the bank's systems, customer demands, or strategic objectives. A third party's inability to deliver products and services, whether arising from fraud, error, inadequate capacity, or technology failure, exposes the bank to transaction risk. Lack of effective business resumption and contingency planning for such situations also increases the bank's transaction risk.

Credit risk. Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Credit risk may arise under many third-party scenarios. Third parties that market or originate certain types of loans subject the bank to increased credit risk if bank management does not exercise effective due diligence over, and monitoring of, the third party. Third-party arrangements can have substantial effects on the quality of receivables and other credit performance indicators when the third party conducts account management, customer service, or collection activities. Improper oversight of third parties who solicit and refer customers (e.g., brokers, dealers, merchant processing ISOs, and credit card marketers), conduct underwriting analysis (credit card processing and loan processing arrangements), or set up product programs (overdraft protection, payday lending, and title lending) can also result in substantial credit risk. The credit risk for some of these third-party programs may be shifted back to the bank if the third party does not fulfill its responsibilities or have the financial capacity to fulfill its obligations. In those situations, it will be important for bank management to assess the financial strength of the third party at the outset of the relationship and periodically thereafter and to have a contingency plan in the event the third party is unable to perform.

Other risks. Depending on the circumstances, third-party relationships may also subject the bank to liquidity, interest rate, price, and foreign currency translation risk. In addition, a bank may be exposed to country risk when dealing with a foreign-based service provider. Country risk is the risk that economic, social, and political conditions and events in a foreign country will adversely affect the bank's financial interests.

OCC SUPERVISORY APPROACH

Supervision by Risk

The OCC expects bank management to engage in a rigorous analytical process to identify, measure, monitor, and establish controls to manage the risks associated with third-party relationships and, as with all other risks, to avoid excessive risk-taking that may threaten the safety and soundness of a national bank. Because third-party relationships are important in assessing a bank's overall risk profile, the OCC's primary supervisory concern in reviewing a bank's relationships with third parties is whether the bank is assuming more risk than it can identify, monitor, manage, and control.

Examiners will review the risks associated with all material third-party relationships and activities together with other bank risks using the supervision-by-risk framework. They will review the effectiveness of the bank's oversight program, including its strategic planning, third-party selection process, and ongoing monitoring.

In addition, the OCC will review the bank's information security and privacy protection programs regardless of whether the activity is conducted directly by the bank or by a third party.

Bank Service Company Act

The OCC treats as subject to the Bank Service Company Act, 12 USC 1867(c), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its internal operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third-party servicers to the same extent as if they were performed by the bank itself on its own premises.[4] Such examinations may evaluate safety and soundness risks, the financial and operational viability of the servicer to fulfill its contractual obligations, compliance with applicable consumer protection, fair lending, and anti-money-laundering laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law. In addition, the OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the national bank or its third party.

The OCC will use its supervisory authority to examine the operations of service providers who seek out national banks to deliver potentially abusive, unfair and deceptive, or predatory products.

The OCC has the authority to assess a national bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party that provides services to the bank. The OCC will conduct such special examinations or investigations if the activities

---

[4] If the third party is a functionally regulated entity (FRE), the Gramm-Leach-Bliley Act of 1999 limits the OCC's ability to examine and require reports from it. However, in these situations, the OCC still regulates how the bank oversees and manages the risk posed by the FRE.

conducted by the service provider for the bank present heightened risks or are of an unusual nature, or if the bank's risk management system is insufficient.[5]

Notwithstanding the OCC's authority to examine the performance of services by service providers directly, the OCC emphasizes that the board and management of national banks are responsible for adequately managing third-party relationships and identifying and controlling the risks that can arise from them.

RISK MANAGEMENT PROCESS

Managing the risks of third-party relationships is fundamental. Reliance on third parties to perform banking functions, to provide products or services to bank customers, or to provide products or services under the bank's name decreases management's direct control, and therefore requires management's intensified oversight efforts. Banks should rigorously analyze and manage the risks posed by material third-party relationships. Doing so involves understanding the risks associated with the activity, conducting thorough due diligence of the proposed third party, implementing an ongoing oversight program of the third party that includes performance monitoring, and developing a contingency plan in the event the third party cannot perform as expected.

The following risk management principles are essential components of well-structured risk management processes. While the principles apply to all third-party activities, not all of the specific elements presented may be necessary for a bank to achieve the desired goal of effective oversight, depending on the scale of the activity and the risks presented.

Risk Assessment and Strategic Planning

Integration with overall strategic objectives. When considering whether to enter into a third-party relationship, the board and management should identify the role of the relationship given the bank's overall business strategy and objectives and should ensure that third-party activities are clearly integrated with corporate strategic goals. At the outset, banks should identify the strategic purposes, benefits, legal aspects, costs, and risks associated with the third-party activity, including reputational risks if the standards associated with the activity or product differ from those customarily employed by the bank. Management should develop a complete and realistic understanding of what the relationship can do for the bank. This analysis requires a thorough corporate self-assessment of core competencies, managerial strengths and weaknesses, and the bank's overall values and goals. This assessment, which should be performed at the highest levels of management, is integral to the bank's strategic planning.

---

[5]OCC 2001-28, "Assessment of Fees; Special Examination of Third Party Service Providers" (June 22, 2001). The factors the OCC will consider in determining whether to impose a fee for the examination of a bank's third-party service providers are (1) the high risk or unusual nature of the activities conducted by the service provider for the bank; (2) the significance to the bank's operations and income of the activities conducted by the service provider for the bank; and (3) the extent to which the bank has sufficient systems, controls, and personnel to adequately monitor, measure, and control risks arising from activities conducted by the service provider for the bank.

The risk assessment phase should include the identification of performance criteria, internal controls, reporting needs, and contractual requirements. Internal auditors, compliance officers, and legal counsel could help to analyze the risks associated with the third-party relationship and to establish the necessary control and reporting structures. Banks should also consider how best to ensure that third parties meet information security and customer privacy requirements. Based on this strategic planning and risk assessment, objectives should be set and specific third-party activities evaluated. Banks may also develop an appropriate exit strategy and contingency plan should the need to terminate the third-party relationship arise.

Expertise to oversee and manage the activity. Management should assess internal expertise to evaluate and manage the activity and the third-party relationship. It is crucial that banks have the requisite expertise to understand and oversee the risks presented by the third-party relationship. Responsibilities for managing third-party relationships should be clearly assigned. The bank must be able to devote the resources necessary to monitor and measure performance under the terms of the third-party agreement. Management may consider appointing a senior officer to sponsor the third-party relationship. The sponsor would be responsible for the due diligence, implementation, management, and monitoring of the arrangement, including periodic reports to the board. The sponsor should have sufficient knowledge and skills to critically evaluate the design, operation, and oversight of the third-party relationship.

Cost/benefit relationship. Banks should be careful to measure long-term stability and viability against potential short-term profits or cost savings. While third-party relationships can be an effective means of reducing operating costs or boosting fee income, these goals should always be balanced with due diligence and adequate oversight. The financial risks posed by an ineffective selection process and inadequate oversight are potentially much larger than any short-term profits and operational cost savings achieved. Without adequate up-front strategic review and ongoing performance-to-plan assessments, banks are at risk of underestimating the cost and of overestimating the benefits of third-party relationships.

Customer expectations. The board and management should also consider how they will manage customer expectations and understandings with respect to joint marketing and franchising activities. Whenever a bank provides its customers with access to products and services not originated by the bank, it must recognize that a wide range of customer relationship issues will inevitably arise. The bank's reputation rests upon its ability to develop standards that meet customer expectations regarding the quality of products and services that are provided through the bank, regardless of whether the product or service is originated by the bank.

Selecting a Third Party and Due Diligence

Regardless of the type of third-party relationship, selecting a competent and qualified third-party provider is essential to managing third-party risk. The due diligence process provides the bank with an opportunity to identify qualitative and quantitative aspects, both financial and operational, of a third party and to assess whether the third party can help the bank achieve its strategic goals. Banks should conduct appropriate due diligence before selecting a third party and at appropriate intervals thereafter.

Due diligence should involve a thorough evaluation of all available information about the third party, and may include:

- Experience in implementing and supporting the proposed activity, possibly to include requiring a written proposal;
- Audited financial statements of the third party and its significant principals (the analysis should normally be as comprehensive as the bank would undertake if extending credit to the party);
- Business reputation, complaints, and litigation (by checking references, the Better Business Bureau, state attorneys general offices, state consumers affairs offices, and, when appropriate, audit reports and regulatory reports);
- Qualifications, backgrounds, and reputations of company principals, to include criminal background checks, when appropriate;
- Internal controls environment and audit coverage;
- Adequacy of management information systems;
- Business resumption, continuity, recovery, and contingency plans;
- Technology recovery testing efforts;
- Cost of development, implementation, and support;
- Reliance on and success in dealing with sub-contractors (the bank may need to consider whether to conduct similar due-diligence activities for material subcontractors);
- Insurance coverage.

Other important elements of due diligence include probing for information on intangibles, such as the third party's business strategies and goals, human resources policies, service philosophies, quality initiatives, and policies for managing costs and improving efficiency. The third party's culture, values, and business styles should fit the bank's.

The due diligence process that a bank uses to select a third party will depend on the complexity of the service to be performed. How formal the process is may depend on the nature of the service and the bank's familiarity with the prospective providers. When selecting third parties, banks may find expert consultants helpful.

Contract Issues

The board and management should ensure that the expectations and obligations of each party are clearly defined, understood, and enforceable. The following topics should normally be considered when entering into a binding contract or agreement (some points may not apply in every circumstance).[6]

Scope of arrangement. The contract should specify the scope of the relationship. For example, outsourcing contracts should specifically identify the frequency, content, and format of the service or product to be provided. The contract should also include, as applicable, such services to be performed by the service provider as software support and maintenance, training of employees, and customer service. Contracts should detail which activities the third party is permitted to conduct, whether on or off the bank's premises, and should describe the terms governing the use of the bank's space, personnel, and equipment. When dual employees are used, their duties and responsibilities should be clearly articulated. The agreement should also indicate whether the service provider is prohibited from assigning any portions of the contract to subcontractors or other entities.

Performance measures or benchmarks. When clearly specified, performance measures define the expectations and responsibilities for both parties. This understanding is the basis for monitoring ongoing performance and measuring the success of the arrangement. Such measures can also be used to motivate third-party performance, especially if poor performance is penalized or outstanding performance rewarded. Industry standards for service-level agreements may provide a reference point for commodity-like services, such as payroll processing. For more customized services, there may be no standard measures. Instead, the bank and service provider should agree upon a range of measures.

Responsibilities for providing and receiving information. Management information reports received from the third party should be timely, accurate, and comprehensive enough to allow the bank to adequately assess performance, service levels, and risks. The contract should discuss the frequency and type of reports received (e.g., performance reports, control audits, financial statements, security reports, and business resumption testing reports). The bank should consider materiality thresholds and procedures to be used to notify the bank when service disruptions, security breaches, and other events pose a material risk to the bank. Banks should consider requiring the third party to notify them in the event of financial difficulty, catastrophic events, material change in strategic goals, and significant staffing changes, all of which might result in a serious impact to service.

The right to audit. Banks should make certain that they have the right to audit third parties (and their subcontractors) as needed to monitor performance under the contract. Generally, in an outsourcing contract, banks should ensure that periodic independent internal and/or external audits are conducted at intervals and scopes consistent with in-house functions. Banks should

[6] The OCC recognizes that some existing contracts may not establish clear and specific responsibilities and obligations of both parties. In this situation, the OCC recommends that banks renegotiate the contracts at the earliest opportunity to address pertinent risk controls and legal protections.

generally include in the contract the types and frequency of audit reports the bank is entitled to receive from the service provider (e.g., financial, internal control, and security reviews). The bank may reserve the right to conduct its own audits of the function, or it may engage an independent auditor. The bank should consider whether to accept independent internal audits conducted by the third-party provider's audit staff or external audits and reviews (e.g., SAS 70 reviews)[7]. In any event, audit reports should include a review of the third party's internal control environment as it relates to the service or product being provided to the bank. Reports should also include a review of the third party's security program and business continuity program.

Cost and compensation. For both the bank and the third party, the contract should fully describe compensation, fees, and calculations for base services, as well as any charges based upon volume of activity and fees for special requests. It should indicate which party is responsible for payment of legal, audit, and examination fees associated with the activity. Cost and responsibility for purchasing and maintaining hardware and software may also need to be addressed. Any conditions under which the cost structure may be changed should be addressed in detail, including any limits on any cost increases.

Ownership and license. The contract should state whether and how the third party has the right to use the bank's data, hardware and software, system documentation, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material. It should indicate whether any records generated by the third party are the property of the bank. If the bank purchases software, management should also consider establishing escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the vendor), documentation of programming and systems, and verification of updated source code.

Confidentiality and security. Service providers must do all they can to keep information confidential and secure. The agreement should prohibit the third party and its agents from using or disclosing the bank's information, except as necessary to provide the contracted services. If the third party receives nonpublic personal information regarding the bank's customers, the bank should notify the third party to assess the applicability of the privacy regulations, and the third party must implement appropriate security measures designed to meet the objectives of regulatory guidelines with which the bank must comply. Banks should require the third party to fully disclose breaches in security resulting in unauthorized intrusions that may materially affect the bank or its customers. The third party should report to the bank when material intrusions occur, should estimate the intrusion's effect on the bank, and should specify the corrective action taken. Arrangements should address the powers of each party to change security procedures and requirements, and should resolve any confidentiality/security issues arising out of shared use of facilities owned by a third party.

Business resumption and contingency plans. The contract should provide for continuation of the business function in the event of problems affecting the third party's operations, including system breakdown and natural (or man-made) disaster. The contract should address the third

---

[7] AICPA Statement of Auditing Standards 70, "Reports of Processing of Transactions by Service Organizations," known as SAS 70 Reports, are one form of external review. Type II SAS 70 reports review the service provider's policies and procedures and provide tests of actual controls against policies and procedures.

party's responsibility for backing up and otherwise protecting program and data files, for protecting equipment, and for maintaining disaster recovery and contingency plans. Responsibilities should include testing of the plans and providing results to the bank. The bank also should consider requiring the third party to provide the bank with operating procedures that are to be carried out in the event business resumption contingency plans are implemented. Contracts should include specific time frames for business resumption and recovery that meet the bank's business requirements. Further, the bank's own contingency plan should address potential financial problems or insolvency of the third party.

Indemnification. Indemnification provisions would require the bank to hold the third party harmless from liability for the negligence of the bank, and vice versa. These provisions should be reviewed to reduce the likelihood that the bank will be held liable for claims citing failure of the third party.

Insurance. The third party should maintain adequate insurance and should notify the bank of material changes to coverage.

Dispute resolution. The bank should consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) for the purpose of resolving problems between the bank and the third party in an expeditious manner, and whether it should provide that the third party continue to perform during the dispute resolution period.

Limits on liability. Some standard contracts with service providers may limit the third party's liability. If the bank is considering such a contract, management should determine whether the proposed limit is in proper proportion to the amount of loss the bank might experience as a result of the third party's failure to perform.

Default and termination. There can be significant risks associated with contract default and/or termination. Therefore, the contract should stipulate what constitutes default, it should identify remedies, and it should allow for opportunities to cure defaults. The extent and flexibility of termination rights sought vary with the type of service. Termination rights may be sought for a variety of eventualities, including change in control, merger or acquisition, convenience, substantial increase in cost, repeated failure to meet service standards, failure to provide critical services and required notices, failure to prevent violations of law or unfair and deceptive practices, bankruptcy, company closure, and insolvency. In addition, the contract should include a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally objects to the particular third-party arrangement. Management should consider whether the contract permits the bank to terminate the relationship in a timely manner without prohibitive expense. The contract should state termination and notification requirements with time frames to allow for the orderly conversion to another third party. The contract should provide for the timely return of the bank's data and other bank resources. Any costs and servicer's obligations associated with transition assistance should be clearly stated.

Customer Complaints. The third party should forward to the bank any complaints it receives from the bank's customers. The contract should specify whether the bank or third party is

responsible for responding to the complaints. If the third party responds, a copy of the response should be forwarded to the bank.

Foreign-based service providers. Banks entering into contracts with foreign-based service providers should carefully consider including in those contracts choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. Such contracts and covenants, however, may be subject to the interpretation of foreign courts relying on local laws. These local laws may substantially differ from U.S. laws in how they apply and enforce choice of law covenants, what they require of banks, and how they protect bank customers. Therefore, a bank should seek legal advice regarding the enforceability of all aspects of a proposed contract with a foreign-based service provider and the other legal ramifications of each such arrangement.

OCC Supervision. As discussed earlier, the performance of services by external parties for the bank is subject to OCC examination oversight. This fact should be included in all contracts when services are performed for the bank.

Oversight of Third-Party Relationships

After entering into a contract or agreement with a third party, management should monitor the third party with respect to its activities and performance. Management should dedicate sufficient staff with the necessary expertise to oversee the third party. While the extent of a bank's oversight activities will vary depending on the nature of the activity, the oversight program should monitor the third party's financial condition, its controls, and the quality of its service and support. Performance monitoring may include, as appropriate, the following:

Monitor Financial Condition

- Evaluate the third party's financial condition at least annually, and more frequently when risk is high or moderate and increasing. This analysis should be as comprehensive as the ongoing credit analysis the bank would conduct of its borrowers. Audited financial statements should be required for significant relationships with third parties.

- If applicable, ensure that the third party's financial obligations to subcontractors are being met in a timely manner.

- Review the adequacy of the third party's insurance coverage.

- Compare actual earnings/costs with projections.

Monitor Controls

- Review audit reports (e.g., internal audits, external audits, SAS 70 reviews, security reviews), as well as examination reports, if available.[8] Follow up on any deficiencies noted.
- Review the third party's policies relating to internal controls and security to ensure that they continue to meet the bank's minimum guidelines and contract requirements.
- Perform on-site quality assurance reviews, targeting adherence to specified policies and procedures, where practicable and necessary.
- Sponsor coordinated audits and reviews with user groups, as applicable.
- Review compliance with the Bank Secrecy Act, fair lending, and other consumer protection laws and regulations, as applicable.
- Review the third party's business resumption contingency planning and testing to ensure that all bank services can be restored within an acceptable time. For many critical services, annual or more frequent tests of the contingency plan are typical. Review any results of those tests and ensure that recovery times meet bank requirements.
- Monitor changes in key third-party personnel allocated to the bank.

Assess Quality of Service and Support

- Regularly review reports documenting the third party's performance relative to service level agreements. Determine whether contractual terms and conditions are being met, and whether any revisions to service-level agreements or other terms are needed.
- Document and follow up on performance problems in a timely manner.
- Evaluate the third party's ongoing ability to support and enhance the bank's strategic plan and goals.
- Determine the adequacy of training provided to bank employees.
- Review customer complaints on the products and services provided by the third party and the resolution of these complaints.
- Administer mystery shopper, customer call-back, or customer satisfaction programs.
- Periodically meet with contract parties to discuss performance and operational issues.

---

[8] Some services provided to national banks by service providers are examined by the FFIEC member agencies. Regulatory examination reports, which are only available to client financial institutions of the service provider, may contain information regarding a service provider's operations. However, regulatory reports are not a substitute for a bank's due diligence, audit, or oversight of the service provider.

- Maintain documents and records regarding contract compliance, revision, and dispute resolution.

Documentation

If a bank is to manage third-party relationships successfully, it must properly document its oversight program. Proper documentation will facilitate the monitoring and management of the risks associated with third-party relationships. Proper documentation typically includes:

- A list of significant vendors or other third parties, i.e., those for which management spends substantial amounts of money, or those deemed critical to the operation[9];
- Valid, current, and complete contracts;
- Business plans for new lines of business or products that identify management's planning process, decision making, and due diligence in selecting a third party;
- Regular risk management and performance reports received from the third party (for example, audit reports, security reviews, reports indicating compliance with service-level agreements); and
- Regular reports to the board, or delegated committee, of the results of the ongoing oversight activities.

CONCLUSION

The OCC supports and encourages national banks' use of third parties to take advantage of the many legitimate and safe opportunities to enhance product offerings, improve earnings, and diversify assets and revenues. To maximize benefits from third-party relationships, banks should have an effective process for managing the associated risks. The value a bank will derive from its use of third-party business relationships is directly proportional to the quality of management's strategic planning, due diligence and ongoing oversight activities, and sensitivity to customer expectations and understandings with regard to the services and products offered by the third parties.

Questions regarding this bulletin should be addressed to Core Policy Development at (202) 874-5190.

Emory W. Rushton
Chief National Bank Examiner

[9] Under 12 USC 1867(c)(2), national banks are required to notify the OCC of the existence of a servicing relationship within 30 days after the making of a contract or the performance of the services, whichever occurs first.

REFERENCES

More guidance about third-party relationships can be found in the following documents.

Issuance	Date	Subject	Applicability
OCC 2001-31	July 3, 2001	Weblinking	Highlights the risks and provides risk management guidance concerning banks' weblinking relationships with third parties.
OCC 2001-28	June 22, 2001	Assessment of Fees	Describes the factors the OCC will consider in determining whether imposition of a fee for the examination of a third-party servicer is warranted.
OCC 2001-12	February 28, 2001	Bank Provided Account Aggregation Services	Includes guidance for banks that offer aggregation services through third-party service providers.
AL 2001-8	February 15, 2001	Guidelines Establishing Standards for Safeguarding Customer Information	Alerts banks that oversight program of service providers should include confirmation that the providers have implemented appropriate measures designed to meet the objectives of the guidelines.
AL 2001-5	May 11, 2001	Interagency Advisory on Brokered and Rate-Sensitive Deposits	Includes guidance that banks should implement adequate due diligence procedures before entering any business relationship with a deposit broker.
AL 2001-4	April 24, 2001	Network Securities Vulnerabilities	Alerts banks to review contracts with service providers to ensure that security maintenance and reporting responsibilities are clearly described.
AL 2001-2	January 22, 2001	Privacy Preparedness	Includes guidance for banks to evaluate agreements with nonaffiliated third parties that involve the disclosure of consumer information.
Comptroller's Corporate Manual	January 2001	The Internet and the National Bank Charter	Includes guidance on the use of vendors/outsourcing.
Comptroller's Handbook	December 2000	Asset Management	Includes guidance on vendor management.
AL 2000-12	November 28, 2000	Interagency Guidance on Risk Management of Outsourcing Technology Services	Transmits detailed guidance on risk mitigation practices when outsourcing technology services, including information and transaction processing and internet banking activities.
AL 2000-11	November 27, 2000	Title Loan Programs	Alerts national banks to OCC concerns over title loan programs, including the involvement of third-party vendors.
AL 2000-10	November 27, 2000	Payday Lending	Alerts national banks to OCC concerns over payday lending programs, including the involvement of third-party vendors.
OCC 2000-25	September 8, 2000	Privacy Laws and Regulations	Includes guidance for banks to evaluate agreements with third parties that involved the disclosure of consumer information.
AL 2000-9	August 29, 2000	Third-Party Risk	Alerts national banks to potential credit risks arising from arrangements with third parties.
Comptroller's Handbook	July 2000	Internal and External Audits	Provides guidelines for banks that outsource internal audit.

OCC 2000-14	May 15, 2000	Infrastructure Threats -- Intrusion Risks	Provides guidance on how to prevent, detect, and respond to intrusions into bank computer systems, including outsourced systems.
Comptroller's Handbook	October 1999	Internet Banking	Includes a discussion of the pros and cons of conducting internet activities in-house or of outsourcing them. Examination procedures include a section on vendor management.
AL 99-6	May 4, 1999	Guidance to National Banks on Website Privacy Statements	Provides guidance on privacy policies regarding customers who access bank Internet sites.
OCC 99-9	March 5, 1999	Infrastructure Threats from Cyber-Terrorists	Identifies the threats and vulnerabilities created by cyber-terrorism.
OCC 98-38	August 24, 1998	PC Banking	Includes information on risk controls for banks that rely on service providers and software vendors for PC banking.
OCC 98-31	July 30, 1998	FFIEC Guidance on Electronic Financial Services and Consumer Compliance	Provides guidance on federal consumer protection laws as they apply to electronic financial services and operations.
OCC 98-3	March 17, 1998	Technology Risk Management	Includes a short description of a bank's responsibility with regard to outsourcing its technology products and services.
OCC 98-1	January 7, 1998	Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing	Includes specific guidance on the use of outsourcing the internal audit function. (Note: A revision is pending.)
OCC 97-23	May 16, 1997	Interagency Statement on Corporate Business Resumption and Contingency Planning	Alerts national banks to assess the business resumption and contingency planning of service providers.
AL 96-8	October 6, 1996	Insurance and Annuity Sales Activities	Includes guidance on third-party arrangements involving bank sales of insurance products and annuities.
FFIEC Information Systems 1996 Examination Handbook	September 1996	Information Systems Operations	Provides guidance for regulatory examiners in the examination of information systems operations in financial institutions and independent service bureaus. It also includes an overview of information systems concepts and practices, examples of sound information systems controls, and FFIEC examination work programs.
OCC 94-13	February 24, 1994	Nondeposit Investment Sales Examination Procedures (temporary insert - *Comptroller's Handbook*)	Includes a section on board oversight of third-party vendors.
BC 260	July 14, 1992	Interagency Statement on EDP Service Contracts	Alerts banks to risks involved in outsourcing information technology services.
BC 187	January 18, 1985	Financial Information on Data Processing Servicers	Alerts national banks to the importance of performing financial reviews of organizations providing data processing services.
BC 181	August 2, 1984	Purchases Of Loans In Whole Or In Part - Participations	Describes prudent purchases of loans and loan participations.