Supplemental Examination Procedures for Risk Management of Third-Party Relationships

Scope

These procedures are designed to help examiners tailor the examinations of national banks and federal savings associations (collectively, banks) and determine the scope of the third-party risk management examination. This determination should consider work performed in related areas by internal and external auditors, risk and compliance functions, and examiners. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objectives. Seldom will every objective or step of the expanded procedures be necessary.

Objective: To determine the scope of the examination of the bank's third-party risk management process and identify examination objectives and activities necessary to meet the supervisory strategy for the bank.

1. Review the following sources of information related to the bank's third-party risk management process that require follow-up:

   - Supervisory strategy
   - Examiner-in-charge's scope memorandum
   - Previous reports of examination, supervisory correspondence, comments within the supervisory information system, and work papers
   - Outstanding enforcement actions or matters requiring attention and status of corrective action
   - Risk assessments developed by the bank or the Office of the Comptroller of the Currency (OCC) that indicate the use of a third party in connection with a product or service

2. Through discussions with management, determine if there are any material changes (actual or planned) in third-party relationships or the third-party risk management process.

3. Obtain and review the following sources of information related to the bank's third-party risk management process:

   - List of key persons, organizational charts, committees, and governance structures supporting the third-party risk management process
   - Policies and procedures
   - Board of directors or designated board committee meeting minutes
   - Inventory or database of third-party relationships (and related subcontractors) that indicates risk ranking (e.g., low, high, or critical) of each third-party relationship

- A listing of each product, process, system, and service supported by a third-party relationship that shows which of these products, processes, systems, and services support critical activities
- Sample[1] of contracts or written agreements with third parties
- Complaint log, and responses to complaints, related to third-party products, processes, systems, and services
- Internally prepared reports (e.g., risk reports and incident reports)
- Internal or external audit reports
- Independent reviews of the bank's third-party risk management process
- Quality assurance, monitoring plans, testing plans, and related reports
- Sample of independent reports on third parties involved in critical activities
- Project plans and timelines
- Training and awareness activities

4. Review findings from other examination areas and identify issues relating to the third-party risk management process; third-party relationships; or the products, processes, systems, and services supported by third parties.

5. Based on an analysis of information obtained in the previous steps, as well as input from the examiner-in-charge, determine the scope of the review of the bank's third-party risk management process.

[1] A "sample" should be based on examiner-in-charge (EIC) judgment (with reference to the "Sampling Methodologies" booklet of the *Comptroller's Handbook)* with consideration given to major lines of business, third parties that support critical activities, or technology service providers.

Quantity of Risk

Conclusion: The quantity of each associated risk is (low, moderate, or high).

Objective: To determine the quantity of risks associated with the bank's third-party relationships.

1. Does the bank have a full inventory of its third-party relationships,[2] including[3]

   - services provided by or to affiliates and subsidiaries?
   - services provided by or to other banks?
   - arrangements with financial market utilities?[4]
   - debt originators (e.g., mortgage or auto dealers)?
   - debt collectors?
   - mortgage government-sponsored entities (e.g., Fannie Mae and Freddie Mac)?
   - critical application software providers?
   - entities that support the bank's human resource functions, such as payroll or benefits administration?
   - attorneys, appraisers, and consultants?
   - entities with whom the bank engages in referral arrangements?
   - entities to which the bank has delegated fiduciary activities?

[2] "Third-party relationship" is defined as any business arrangement between a bank and another entity, by contract or otherwise. Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements in which the bank has an ongoing relationship or may have responsibility for the associated records. Third-party relationships generally do not include customer relationships.

[3] This list is not all inclusive. This list includes some third-party relationships that banks may mistakenly fail to consider when developing their inventory of third-party relationships.

[4] The term "financial market utility" is defined in Title VIII of the Dodd–Frank Wall Street Reform and Consumer Protection Act as "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person." Examples of financial market utilities include the Clearing House Interbank Payments System, Options Clearing Corporation, Depository Trust Company, National Securities Clearing Corporation, Chicago Mercantile Exchange, Fixed Income Clearing Corporation, Fedwire Funds Service, Society for Worldwide Interbank Financial Telecommunication, FedACH Service, Electronic Payments Network, Visa, MasterCard, and Fedwire Securities Service.

2. In its inventory of third-party relationships, does the bank identify those that

    - involve critical activities?[5]
    - involve the use of subcontractors[6]?
    - are with affiliates?
    - are with foreign-based entities?
    - are with domestic-based entities that engage in foreign transactions?
    - are technology-based services storing bank data?

Objective: To determine the quantity of operational risk associated with the use of third parties.

1. Determine whether there are any concentrations[7] among third-party relationships.

    - Review the bank's methodology for identifying concentrations among third-party relationships.
    - Determine whether there are concentrations due to the bank's reliance on a single third party for multiple activities, particularly when several of the activities are critical to one or more lines of business.
    - Determine whether there are geographic concentrations where the bank's own operations, the operations of its third parties, or the operations of third parties' subcontractors are located in the same region or are dependent on the same critical power and telecommunications infrastructures.

2. Determine whether any third-party relationships are foreign-based.

    - Review the bank's policies and procedures regarding offshore outsourcing of bank services or operations.
    - Review the bank's method for determining whether the bank's third parties or the third parties' subcontractors are foreign-based.
    - Determine if the bank's database or inventory distinguishes third parties that are foreign-based and if the database or inventory notes the geographic location (country, city, or region).

[5] "Critical activities" is a term used in OCC Bulletin 2013-29. The term refers to significant bank functions (e.g., payments, clearing, settlements, and custody) or significant shared services (e.g., information technology), or other activities that could cause a bank to face significant risk if the third party fails to meet expectations; could have significant customer impacts; require significant investment in resources to implement the third-party relationship and manage the risk; or could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

[6] The term "subcontractor" refers to any entity with which the third-party service provider itself has chosen to enter into a third-party relationship. Another term for subcontractor is "fourth party."

[7] Concentrations may arise when a bank relies on a single third party for multiple activities, particularly when several of the activities are critical to bank operations. Additionally, geographic concentrations can arise when a bank's own operations, and that of its third parties and subcontractors, are located in the same region or are dependent on the same critical power and telecommunications infrastructures.

- Determine if the bank has obtained legal advice regarding the enforceability of foreign-based third-party contracts or how to adjudicate disputes with foreign-based third parties. The lack of legal advice or advice that discloses potential problems increases the bank's risk.
- Determine if the bank obtained and reviewed research regarding the stability of the country, the country's government structure, legal structure, applicable law, or economic situation. Does the bank obtain and review, on an ongoing basis, research on these issues? The lack of research or the existence of research that discloses potential problems increases the bank's risk.
- Determine if the bank obtained and reviewed research of the possibility of natural disasters or disasters of human origin in the country where third parties are based. Does the bank obtain and review, on an ongoing basis, research on these issues? The lack of research or the existence of research that discloses potential problems increases the bank's risk.
- Determine if the bank has obtained legal advice regarding the coverage of privacy and information security laws in the country where third parties are based. The lack of legal advice or the existence of advice that discloses potential problems increases the bank's risk.

3. Determine whether any third-party relationships involve the use of subcontractors.

    - Review the bank's methodology for determining whether third parties use subcontractors.
    - Determine if the bank maintains a database or inventory that can distinguish all third parties that use subcontractors.

4. Determine if the bank is a member of or receives services from a financial market utility. If so, what is the bank's due diligence and ongoing monitoring process for these third parties? Consider

    - how the bank monitors risk related to each of these third parties.
    - whether the bank complies with the third parties' operating agreements.

5. Determine if the bank has contracted with third-party lenders (e.g., marketplace lenders)[8] to perform some, if not all, operational functions, including processing, underwriting, closing, funding, delivering, and servicing of loans. Does the bank have sufficient support systems, controls, and personnel to adequately support the volume of planned loan origination, servicing, or collections activities?

[8] There is no single or universally accepted definition for "marketplace lender." Generally, marketplace lenders are companies engaged in Internet-based lending businesses (other than payday lending). Marketplace lenders may offer a wide variety of financial products, including small business loans, consumer loans, student loans, and real estate loans. Marketplace lenders may fund their loans through various means, including equity capital, commercial lines of credit, sale of whole loans to institutional investors, securitizations, and pass-through note programs.

6. Determine if there is a limitation on the third party's liability in the contract or other documentation. If so, has the bank documented any analysis showing whether the limitation is proportional to the amount of loss or increased legal, reputational, or compliance risk the bank might experience because of the third party's failure to perform or comply with applicable law?

Objective: To determine the quantity of compliance risk associated with the use of third parties.

1. Determine if any of the bank's third-party relationships are with affiliates. If so, determine if the bank has a process to maintain compliance with sections 23A and 23B of the Federal Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223).

2. Determine whether any concerns are identified in a report of internal audit or independent third party that regularly reviews the bank's products, services, transactions, or systems associated with third-party relationships for compliance with

   - all applicable laws and regulations, including U.S. economic sanction laws administered by the Office of Foreign Assets Control (OFAC), the Bank Secrecy Act/anti-money laundering (BSA/AML), and consumer protection laws and regulations.
   - the bank's policies and procedures.

3. Determine if the bank conducts sufficient research to assess that a license or technology that the bank uses does not violate third parties' intellectual property rights.

4. Determine if and how often the bank reviews third parties' policies, procedures, and independent audit reports for compliance with all applicable laws and regulations, including consumer protection laws and OFAC and BSA/AML requirements, if appropriate to the services provided.

5. Determine if the bank has identified and appropriately managed potential conflicts of interest that the bank has with its third-party relationships.

6. Determine if the bank has conducted adequate due diligence to verify whether third parties or their subcontractors have publicly known outstanding issues with regulatory entities or law enforcement agencies.

7. Determine if the bank reviews third parties' programs or processes that identify and track necessary implementation steps designed to ensure that third parties can comply with new consumer compliance, OFAC, and BSA/AML requirements by a stated effective date. Does the bank review third parties' policies, procedures, and training materials to determine if third parties can comply with new consumer compliance, OFAC, and BSA/AML requirements by a stated effective date?

8. Determine if the bank has contingency or termination plans if services provided to the bank by third parties cannot meet new consumer compliance, OFAC, or BSA/AML requirements by a stated effective date.

Objective: To determine the quantity of reputation risk associated with the use of third parties.

1. Determine if the bank has contracts specifying that third parties are responsible for responding to customer complaints. If so, do the contracts include provisions requiring third parties to promptly respond and adequately address the complaints? Do the contracts include provisions for third parties to provide regular reports to the bank about the complaints received and how the complaints were addressed?

2. Determine if the bank obtains customer complaints or regular reports regarding consumer complaints from third parties and their subcontractors.

3. Assess the adequacy of the bank's process for periodically receiving and analyzing customer complaints (or regular reports) related to third parties and their subcontractors (or the products or services that third parties support) for incidents of poor services, frequent or prolonged service disruptions, significant or repetitive security lapses, inappropriate sales recommendations, or violations of consumer protection laws and regulations.

4. Determine if the bank periodically reviews online activity, publicity, public reports, or social media for adverse events involving third parties and their subcontractors. If so, assess to what extent bank management incorporates this information into its ongoing monitoring.

Objective: To determine the quantity of strategic risk associated with the use of third parties.

1. Determine if the bank conducted sufficient planning before contracting with third parties.

    - Are the banking functions, products, and services associated with or performed by third parties compatible with the bank's strategic goals?
    - Can the bank effectively monitor and manage bank functions, products, and services associated with or performed by third parties?
    - Does the bank compare the cost of providing these bank functions, products, and services internally with the cost of outsourcing?
    - Does the bank estimate that these bank functions, products, and services provide adequate return on investment in relation to risk?
    - If the bank has third-party relationships with affiliates, how did the bank determine that the cost of services provided by the affiliates was reasonable compared with the cost of outsourcing to unaffiliated third parties?

2. Determine if the bank has enough staff with adequate experience and expertise to properly oversee third-party relationships and the bank's third-party risk management process.

Objective: To determine the quantity of credit risk associated with the use of third parties.

1. Determine to what extent the bank uses third parties for real estate lending, credit card lending, installment lending, student lending, debt reconciliation, subprime lending, payday lending, or other types of lending. If the bank uses third parties for a material amount of lending in these or any other portfolio segment(s),

   - has the bank determined if the loans meet its underwriting standards?
   - does the bank adequately monitor performance of loans underwritten or originated by third parties?
   - are there controls in place to maintain the volume of lending within the parameters of the bank's business plans?

2. Determine if third parties perform any of the following types of functions on the bank's behalf.

   - Marketing or originating loans
   - Account management, customer service, servicing, or collection activities
   - Customer solicitation and referral
   - Underwriting analysis
   - Closing loans
   - Creating and distributing disclosures

   If so, are the bank's due diligence and ongoing monitoring processes for these third parties adequate?

3. Determine if the bank is a member of a financial market utility or a number of financial market utilities to which it has direct or potential credit exposure. If so, assess how the bank monitors, manages, and limits these exposures.

4. Determine if the bank has contracted with marketplace lenders to originate or purchase loans. Do the marketplace lenders use underwriting methods that are new, nontraditional, or different from the bank's underwriting standards? Is the bank subject to any recourse or participation arrangements as part of originating marketplace loans? What remedies are available to the bank if a third party does not meet the terms of the contract?

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, insufficient, or weak).

The conclusion on the quality of risk management considers all risks associated with third-party relationships.

Policies

Policies are statements of actions adopted by a bank to pursue certain objectives. Policies guide decisions, often set standards (on risk limits, for example), and should be consistent with the bank's underlying mission, risk appetite, and core values. Policies should be reviewed periodically for effectiveness and approved by the board or designated board committee.

Objective: To determine whether the board has adopted effective policies that are consistent with safe and sound banking practices and are appropriate to the size, nature, and scope of the bank's third-party relationships.

1. Determine the adequacy of the bank's policies regarding its third-party relationships. Consider if the policies

   - establish responsibilities and accountability.
   - establish risk limits and outline actions to be taken if limits are breached.
   - establish criteria for defining critical third parties.
   - require the board to approve all critical third-party contracts.
   - include the methodology to be used for risk-assessing third parties.

2. Determine if policies are appropriately communicated to persons with supervisory responsibility for third-party relationships.

3. Verify that the board or designated board committee periodically reviews and approves third-party relationship policies.

Processes

Processes are the procedures, programs, and practices that impose order on a bank's pursuit of its objectives. Processes define how activities are carried out and help manage risk. Effective processes are consistent with the underlying policies and are governed by appropriate checks and balances (such as internal controls).

Objective: To determine whether the bank has processes in place to manage the risk of its third-party relationships.

1. Determine the method or process the bank uses to identify all of its third-party relationships and to include all of its third-party relationships in the bank's inventory or database.

2. Review the bank's methodology for risk ranking each third-party relationship. Some relationships may be low risk, others may be high risk, and others may be critical.

3. Determine how often the bank reviews the risk ranking of third-party relationships.

4. Determine whether management has a process for escalating significant issues or concerns to the board.

5. Determine whether management has appropriately integrated the third-party risk management process into the bank's enterprise risk management framework.

6. Determine if the bank has an effective third-party risk management process throughout the life cycle of each third-party relationship.

7. Determine if the bank

   - buys bonds, whole loans, or notes from third-party lenders (e.g., marketplace lenders).
   - has a written agreement with third-party lenders to purchase loans or pool(s) of loans on a future date that meet predetermined criteria, such as interest rate, average loan amount, weighted average credit score, and weighted average life.
   - is acting as an issuer of securities backed by loans originated through third-party lending.
   - is investing directly or indirectly in a third-party lender.
   - is providing warehouse lines or other credit facilities to third-party lenders.

   If so,

   - has the bank performed robust counterparty credit risk analysis of the third-party lenders?
   - has the bank determined if the loans meet the bank's underwriting standards?
   - does the bank have a process to determine whether the third-party arrangement meets OCC regulatory investment and lending limits?
   - does the bank have a process for ensuring that the bank properly records revenue and expenses associated with third-party lending activities in the bank's financial reports?

Life Cycle Phase 1—Planning

1. Before the bank enters into third-party relationships, determine whether management develops plans to manage the relationships. Determine the adequacy of these plans based on the risk associated with the third-party relationships. Depending on the risk associated with the third-party relationships, consider whether each plan

- discusses the risks inherent in the arrangement.
- outlines compliance and audit oversight.
- discusses how the arrangement aligns with the bank's overall strategic goals, objectives, and risk appetite.
- assesses the arrangement's complexity, such as the volume of activity, use of subcontractors, technology needed, and whether the third party is foreign-based.
- determines whether the potential financial benefits outweigh the estimated costs to control the risks.
- considers how the third-party relationship could affect other strategic bank initiatives, such as large technology projects, organizational changes, mergers, acquisitions, or divestitures.
- considers how the third-party relationship could affect bank employees and what transition steps are needed to manage the impact when the activities currently conducted internally are outsourced.
- assesses the nature of customer interaction with the third party and the potential impact the relationship will have on the bank's customers—including access to or use of those customers' confidential information, joint marketing or franchising arrangements, complying with consumer protection laws, and handling of customer complaints—and outlines plans to manage these impacts.
- assesses potential information security implications, including access to the bank's systems and to its confidential information.
- considers the bank's contingency plans if the bank needs to transition the activity to another third party or bring it in-house.
- assesses the extent to which the activities are subject to specific laws and regulations, including BSA/AML and OFAC.
- considers whether the selection of the third party is consistent with corporate policies and practices.
- details how the bank will select and oversee the third party, including monitoring the third party's compliance with the contract.
- is presented to and approved by the bank's board of directors when critical activities are involved.

Life Cycle Phase 2—Due Diligence and Third-Party Selection

1. Determine whether the bank conducts appropriate due diligence on all potential third parties before selecting and entering into contracts or relationships.

2. Determine whether there is appropriate staffing and expertise involved in due diligence activities.

3. Determine the scope and assessment method(s) of due diligence performed and evaluate whether the due diligence activities are commensurate with the level of risk of the third-party relationship. Consider management's assessment of the third party's

- compliance management system. Does the assessment ensure that the third party has the appropriate licenses and expertise, processes, and controls to provide bank services that are compliant with applicable laws and regulations?
- financial condition, including reviews of the third party's audited financial statements. Also determine whether the assessment evaluates growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability.
- business experience and reputation, including history of customer complaints and litigation.
- fee structure and incentives.
- fraud prevention processes.
- thoroughness of background checks on senior management, employees, and subcontractors who have access to critical systems or confidential information.
- risk management program effectiveness. Management's assessment should include reviewing samples of Service Organization Control 2, information security control questionnaire, industry Standardized Information Gathering, or other similar reports. Management should consider whether these reports contain sufficient information to assess the third party's risk management program or whether additional scrutiny is required.
- information security program to determine whether the third party has sufficient expertise in identifying, assessing, and mitigating known and emerging threats and vulnerabilities.
- information systems to determine whether the information system can identify gaps in service-level expectations, technology, business process, and management or interoperability issues.
- resilience, including the third party's ability to respond to service disruptions from natural disasters, human error, physical attacks, or cyber attacks.
- incident reporting and management programs.
- physical security and environmental controls.
- program to train and hold employees accountable for compliance with policies and procedures.
- reliance on subcontractors and geographic locations of subcontractors.
- verification of fidelity bond, liability, and hazard insurance coverage.

Life Cycle Phase 3—Contract Negotiation

1. Determine whether management appropriately reviews, or has legal counsel review, contracts before execution and periodically reviews contracts thereafter to check whether the contracts continue to address pertinent risk controls and legal protections.

2. Determine whether only authorized individuals execute third-party contracts.

3. Review a sample of contracts and determine their adequacy, particularly those that involve critical activities. Consider whether contracts adequately

- address the nature and scope of the third-party relationship.
- address cost and compensation.
- specify performance measures or benchmarks that define the expectations and responsibilities of both parties.
- include specific language regarding the type and frequency of reporting on third parties' and their subcontractors'
  - conformance with performance measures or benchmarks.
  - audit results.
  - business resumption testing.
  - compliance with laws and regulations.
  - customer complaints.
  - other contractual obligations.
- address the bank's right to audit, monitor performance, and require remediation when issues are identified.
- require third parties and subcontractors to comply with the laws, regulations, and self-regulatory standards applicable to the contracted service, including those related to intellectual property rights.
- address how and when the third party must notify the bank of its intent to use a subcontractor.
- address activities that cannot be subcontracted, or whether the bank prohibits the third party from subcontracting to certain locations or specific subcontractors.
- address requirements for subcontractor conformance with contractual obligations (e.g., conformance with performance measurements, periodic audit requirements, compliance with applicable laws and regulations, and other contractual obligations).
- reserve the bank's right to terminate contracts without penalty if third parties or their subcontractors do not comply with contractual terms.
- specify what actions or procedures third parties are obligated to take upon termination of the contract.
- require third parties and their subcontractors to implement and maintain appropriate security measures to comply with privacy regulations and refrain from using or disclosing the bank's or the bank customers' information, except to provide contracted services or to comply with legal requirements.
- address confidentiality and integrity of data and compliance with laws and regulations regarding the protection of confidential consumer information.
- address prompt notification of information security or cyber incidents.
- specify how third parties or their subcontractors should disclose, in a timely manner, information security breaches that result in unauthorized intrusions or access that may materially affect the bank or its customers.
- stipulate that material information security breach notifications include corrective actions to be taken by third parties and their subcontractors.
- stipulate whether and how often the bank, its third parties, or the third parties' subcontractors jointly practice incident management plans involving information security breaches.
- require third parties to provide the bank with current business resumption and disaster recovery plans that include operating procedures and address integrity of service.

- require third parties to maintain appropriate insurance, notify the bank of material changes to coverage, and provide evidence of coverage.

Life Cycle Phase 4—Ongoing Monitoring

1. Assess whether management periodically reviews third-party relationships to determine if the nature of the activities is critical.

2. Determine whether management has dedicated sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party in a manner commensurate with the level of risk and complexity of the relationship. Consider whether there is sufficient monitoring of the

   - quality and sustainability of the third party's controls.
   - third party's ability to meet service-level agreements, performance metrics, and other contractual terms, and to comply with legal and regulatory requirements.

3. Determine whether on-site visits are performed for a third party involved in critical activities. Analyze whether someone with the necessary authority and expertise conducts the visits and how information gathered during the visits is used for ongoing monitoring purposes.

4. Select a sample of independent reports on third parties involved in critical activities and determine the adequacy, frequency, and types of reports used to monitor third-party relationships.

5. Determine if processes include having the bank contact the OCC to determine if an Interagency Examination of a Service Provider examination report is available. If an examination report is available, did the bank request the report from the OCC? How was this information used in the bank's ongoing monitoring of the third party?

6. Determine if ongoing monitoring includes assessing changes to third parties'

   - business strategies and reputation that may pose conflicts of interest and affect third parties' ability to meet contractual obligations and service-level agreements.
   - compliance with legal and regulatory requirements in providing services to the bank.
   - financial condition.
   - insurance coverage.
   - key personnel and ability to retain essential knowledge in support of the services provided to the bank.
   - ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.
   - process for adjusting policies, procedures, and controls in response to changing threats, new vulnerabilities, and material breaches or other serious incidents.
   - information technology used or the management of information systems.

- ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.
- reliance on, exposure to, or quality of performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.
- agreements with other entities that may pose conflicts of interest or introduce reputation, operational, or other risks to the bank.
- ability to maintain the confidentiality and integrity of the bank's information systems.
- volume, nature, and trends of customer complaints, in particular those that indicate compliance or risk management problems.
- ability to appropriately address customer complaints.

7. Assess the bank's process for escalating significant issues identified during ongoing monitoring. Are significant issues escalated to senior management (and the board, if necessary)?

Life Cycle Phase 5—Termination and Contingency Planning

1. Determine whether management has adequate contingency plans that address steps to be taken in the event of contract default or termination. Specifically, does the plan cover

   - capabilities, resources, and the time frame required to transition activities provided by third parties while still managing legal, regulatory, and customer responsibilities?
   - risks associated with data retention and destruction, information system connections, access control issues, or other control concerns?
   - handling of intellectual property jointly developed during the course of the third-party relationship or intellectual property that belongs solely to the third party?
   - reputation risks to the bank if the termination happens as a result of the third party's inability to meet expectations?

Personnel

Personnel are the bank staff and managers who execute or oversee processes. Personnel should be qualified and competent, have clearly defined responsibilities, and be held accountable for their actions. They should understand the bank's mission, risk appetite, core values, policies, and processes. Banks should design compensation programs to attract and retain qualified personnel, align with strategy, and appropriately balance risk-taking and reward.

Objective: To determine management's ability to supervise third-party relationships in a safe and sound manner.

Board Responsibilities

1. Determine whether the board (or designated board committee) has adopted a risk-based process that, at a minimum, establishes policies, operating standards, and procedures

throughout the third-party risk management life cycle, including documentation and reporting, oversight and accountability, and independent reviews. Is the process reviewed and periodically updated?

2. Do board minutes indicate that the board reviews and approves the following?

   - The methodology for determining critical activities
   - Management's plans for using third parties involved in critical activities
   - Summary of due diligence results
   - Contracts with third parties involved in critical activities
   - Results of management's ongoing monitoring of third parties involved in critical activities
   - Results of periodic internal audit or independent third-party reviews of the bank's third-party risk management process

3. Do board minutes show that the board oversees management's efforts to remedy deterioration in performance, material issues, or changing risks identified through internal audit or independent third-party reviews?

Management Responsibilities

1. Determine whether management properly documents and reports on the bank's third-party risk management process. Consider whether management has developed and periodically reviews and updates

   - a current inventory or database of all third-party relationships that indicates the risk ranking of each third-party relationship.
   - the methodology for determining the risk ranking assigned to each third-party relationship, particularly for relationships involving critical activities.
   - approved plans for the use of third-party relationships.
   - due diligence results, findings, and recommendations.
   - analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the bank.
   - executed contracts.
   - required risk management and performance reports received from third parties (e.g., audit reports, security reviews, consumer complaints, and reports indicating compliance with contracts or service-level agreements).

2. Determine whether management has an effective process to escalate significant issues or concerns to the board (e.g., events that result in material adverse consequences to the bank and its customers, including data breaches and compromise of customer information).

3. Determine whether management provides satisfactory reports to the board regarding the following:

- Results of ongoing monitoring of third parties involved in critical activities.
- Results of internal audit or independent third-party reviews of the bank's third-party risk management process.

4. Determine how management holds the employees in business lines who manage relationships with third parties accountable for

   - adhering to the bank's policies, procedures, and processes regarding third-party management.
   - conducting due diligence and ongoing monitoring of third parties.
   - escalating significant issues to senior management.
   - responding to material weaknesses identified by independent reviews.
   - maintaining appropriate documentation throughout the life cycle of the third-party relationship.

Control Systems

Control systems are the functions (such as internal and external audits, and quality assurance) and information systems that bank managers use to measure performance, make decisions about risk, and assess the effectiveness of processes and personnel. Control functions should have clear reporting lines, sufficient resources, and appropriate access and authority. Management information systems should provide timely, accurate, and relevant feedback.

Objective: To determine whether the bank has systems in place to provide accurate and timely assessments of the risks associated with its third-party relationships.

1. Determine whether internal audit or a third party conducts periodic independent reviews of the bank's third-party risk management process. Determine whether these reviews thoroughly assess the adequacy of the bank's process for

   - verifying whether third-party relationships align with the bank's business strategy.
   - identifying, assessing, managing, and reporting on risks of third-party relationships.
   - responding to material breaches, service disruptions, or other material issues.
   - identifying and managing risks associated with third-party relationships, including foreign-based third parties and subcontractors.
   - involving multiple business lines across the bank as appropriate during each phase of the third-party risk management life cycle.
   - maintaining appropriate staffing and expertise to perform due diligence and ongoing monitoring of third parties.
   - administering oversight and accountability for managing third-party relationships (e.g., whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority).
   - preventing conflicts of interest or appearances of conflicts of interest when selecting or overseeing a third party.

- identifying and managing concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentrations of business due to either direct contracting or subcontracting agreements in the same locations.

2. Determine whether management analyzes the results of independent reviews and responds promptly and appropriately to significant issues or concerns. Determine whether management escalates significant issues or concerns to the board.

3. Evaluate the effectiveness of monitoring systems to identify, measure, and track exceptions to policies and established risk limits.

4. Determine whether management information systems provide timely, accurate, and useful information to evaluate risk levels and trends in the bank's third-party relationships.

5. Assess the effectiveness of risk functions overseeing the bank's third-party relationships.

Conclusions

Conclusion: The aggregate level of each associated risk is (low, moderate, or high). The direction of each associated risk is (increasing, stable, or decreasing).

Objective: To determine, document, and communicate overall findings and conclusions regarding the examination of the bank's third-party risk management process.

1. Determine preliminary examination findings and conclusions and discuss the following with the examiner-in-charge:

   - Adequacy of the bank's methodology for determining risk ranking of each third-party relationship
   - Quantity of associated risks
   - Quality of the risk management process
   - Overall risk from the bank's third-party relationships
   - Adequacy of the board and management's oversight over its third-party risk management process
   - Inconsistencies with OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," or other concerns

Summary of Risks Associated With Third-Party Relationships				
Risk category	**Quantity of risk**	**Quality of risk management**	**Aggregate level of risk**	**Direction of risk**
	(Low, moderate, high)	(Weak, insufficient, satisfactory, strong)	(Low, moderate, high)	(Increasing, stable, decreasing)
Credit				
Operational				
Compliance				
Strategic				
Reputation				

2. Discuss examination findings with bank management, including concerns, recommendations, and conclusions about risks and risk management practices. If necessary, obtain commitments for corrective action.

3. Compose conclusion comments, highlighting any issues that should be included in the report of examination or supervisory correspondence. If necessary, compose matters requiring attention.

4. Update the OCC supervisory information system.

5. Update the supervisory strategy to include steps that the OCC should take to effectively supervise the risk management of third-party relationships, including time frames, staffing, and workdays required.

6. Update, organize, and reference work papers in accordance with OCC policy.

7. Ensure that any paper or electronic media that contain sensitive bank or customer information are appropriately disposed of or secured in accordance with OCC policy.