THIRD-PARTY RELATIONSHIP RISK MANAGEMENT

FIRMA NATIONAL RISK MANAGEMENT TRAINING CONFERENCE

NASHVILLE, TN – MAY 2, 2022

PRESENTED BY

JEFFREY KROPSCHOT – PRESIDENT, KROPSCHOT CONSULTING PARTNERS, LLC

DISCLAIMER

The views expressed today are solely those of the presenter and do not necessarily reflect those of Kropschot Consulting Partners, LLC.

THIRD-PARTY RELATIONSHIP DEFINITION

- The OCC defines a third-party relationship as a business arrangement between a bank and another entity, by contract or otherwise, which may exist despite a lack of a contract or remuneration.
- Third-party relationships include activities involving:
  - Outsourced products and services
  - Use of independent consultants
  - Networking arrangements
  - Services provided by affiliates and subsidiaries
  - Other business arrangements where the bank has an ongoing relationship

BACKGROUND

- When engaging in third-party relationships, banks are expected to practice effective risk management, whether activities are performed directly or through third parties.
- Banks are permitted to take a risk-based approach to managing third-party risks, where risk management practices reflect the risk and complexity of outsourced activities.
- When banks outsource certain activities to third parties, **including affiliates**, they are expected to verify those activities are performed prudently, consistent with laws, regulations and industry standards.
- OCC Bulletins 2013-29 and 2020-10 provide key guidance to financial institutions and examiners regarding risk management of third-party relationships.

OCC BULLETIN 2013-29 – THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE

- The bulletin provides guidance for assessing and managing risks associated with third-party relationships.
- Banks should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
- Banks should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process must evolve throughout the life cycle of each third-party relationship.

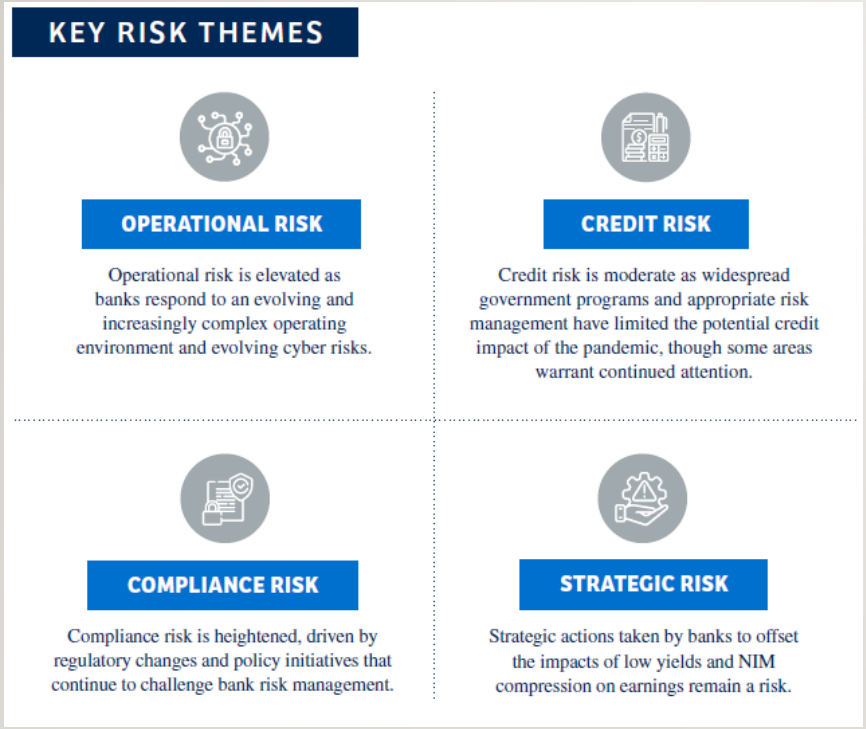
OCC BULLETIN 2020-10 – THIRD-PARTY RELATIONSHIPS: FAQs TO OCC BULLETIN 2013-29

- New bulletin rescinds OCC Bulletin 2017-21 (Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29)
- FAQs from OCC Bulletin 2017-21 have been incorporated unchanged into OCC Bulletin 2020-10 (except for question No. 24), which was updated to reflect current AICPA Service Organization Control report information
- FAQ numbers from OCC Bulletin 2017-21 are noted in parentheses throughout the bulletin

PROPOSED INTERAGENCY GUIDANCE ON THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT

- Published in the Federal Register 7/19/2021
- Offers a framework based on sound risk management principles to consider in developing risk management practices for all stages in the life cycle of third-party relationships, which considers the level of risk, complexity, and size of the organization and the nature of the third-party relationship.
- Sets forth considerations with respect to the management of risks arising from third-party relationships. The proposed guidance would replace each agency's existing guidance on this topic and would be directed to all banking organizations supervised by the agencies.

OCC SEMI-ANNUAL RISK PERSPECTIVE – FALL 2021



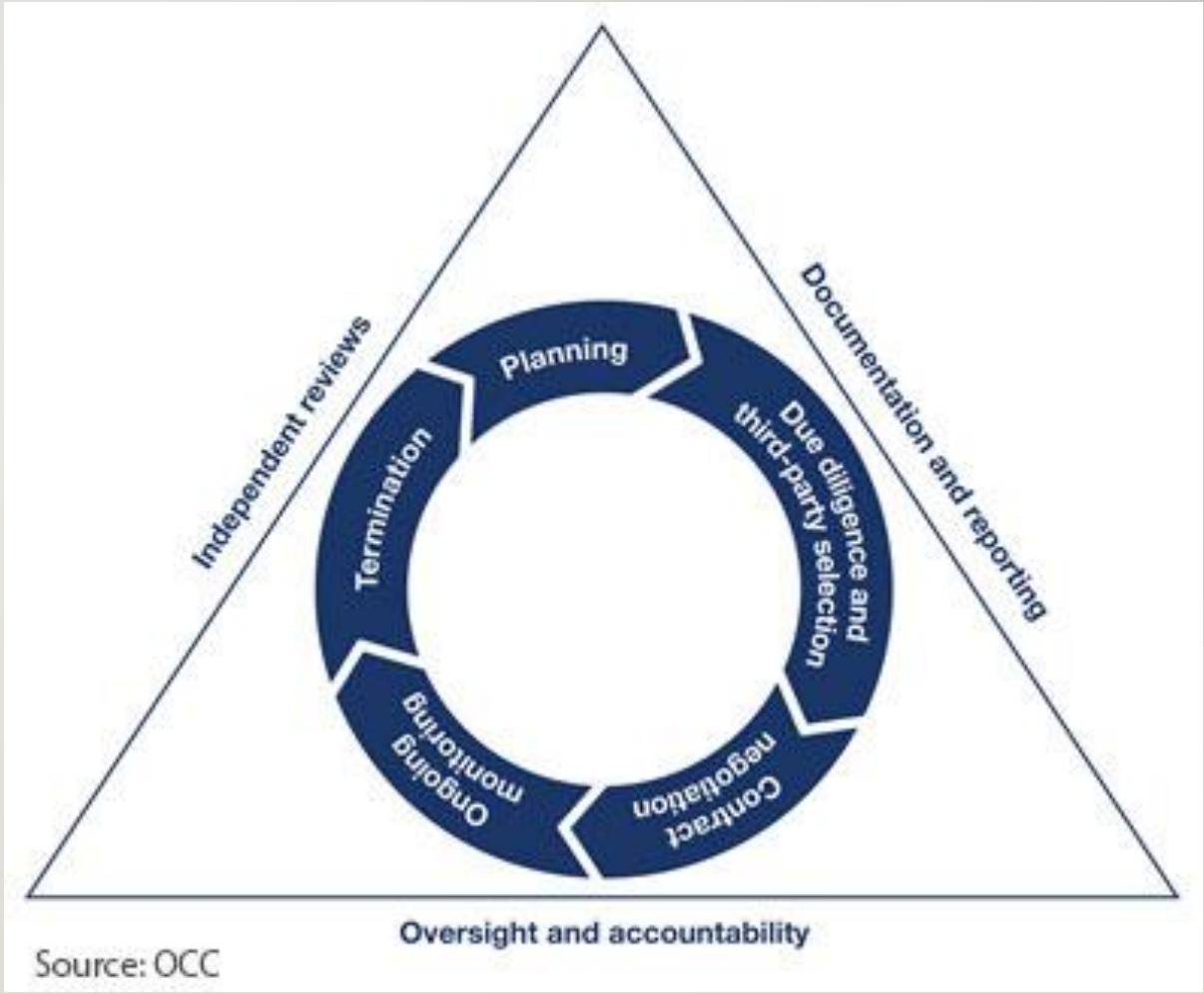
Third-Party Risk Management

- Continued area of supervisory focus
- Risk-based due diligence required, based on criticality of activities provided
- Must consider cyber and other risks
- Must know how third parties manage their risks
- Proposed interagency guidance on third-party relationship risk management dated 7/19/2021

RISK MANAGEMENT LIFE CYCLE

A third-party risk management process life cycle should include the following components:

- Planning
- Due Diligence and Third-Party Selection
- Contract Negotiation
- Ongoing Monitoring
- Termination



LIFE CYCLE PHASE - SUMMARY

Phase	Description	Guidance
Planning	Management planning is the first step in the life cycle, particularly when critical activities are involved	Discusses what the management plan should address
Due-Diligence and Third-Party Selection	In-depth review of potential third parties before final selection and contract negotiation	Discussed the key factors to consider when conducting third-party due diligence
Contract Negotiation	Established responsibilities and performance requirements	Discusses key factors the contract should address
Ongoing Monitoring	Monitoring of performance and compliance throughout the duration of the contract	Discusses key considerations in ongoing monitoring
Termination	Plans to cease activity, bring it in house, or move it to another third party at end of the contract or otherwise	Discusses what a termination plan should cover

LIFE CYCLE – PLANNING

- Banks should assess risks associated with prospective third-party relationships and develop formal plans to manage these relationships and risks.
- Plan scope should vary based on the unique risks and complexities associated with each relationship.
- Among other things, the bank plan should:
  - summarize strategic purposes for outsourcing
  - evaluate alignment with the bank's overall strategic objectives and risk appetite
  - assess the complexity of the arrangement and risks inherent with the outsourced activity
  - outline the process for selecting, assessing and monitoring the prospective third party

LIFE CYCLE – DUE DILIGENCE AND THIRD-PARTY SELECTION

- Banks must perform due-diligence on prospective third parties before entering into business relationships with them.
- The level of due-diligence performed should vary based on the unique risks and complexities associated with each relationship (e.g., relationships involving critical activities will require enhanced due diligence).
- A thorough, objective evaluation of each third party should be performed to verify that the third party can capably carry out its responsibilities, consistent with the needs of the bank and in compliance with regulatory expectations.
- Prior knowledge of or experience with a particular third party is not a substitute for a thorough analysis.

LIFE CYCLE – DUE DILIGENCE AND THIRD-PARTY SELECTION (CONT.)

- Factors to consider while performing due-diligence on prospective third-party service providers:
  - Strategies and goals (of the third party)
  - Legal and regulatory compliance program
  - Financial condition
  - Experience and reputation
  - Fee structure and incentives
  - Risk management program

LIFE CYCLE – DUE DILIGENCE AND THIRD-PARTY SELECTION (CONT.)

- Factors to consider while performing due-diligence on prospective third-party service providers include:
  - Information security program
  - Resilience to service disruptions
  - Physical security
  - Human resource management
  - Use of subcontractors
  - Insurance coverage

LIFE CYCLE – DUE DILIGENCE AND THIRD-PARTY SELECTION (CONT.)

- Leadership should review the results of the due diligence analysis to determine whether the third party is able to meet the bank's needs and expectations.
- If the results of the due diligence do not meet the bank's standards, management should:
  - recommend that the third party make appropriate changes,
  - find an alternate third party,
  - conduct the activity in-house, or
  - discontinue the activity.
- Management should communicate due diligence results to the board when recommending third parties, who may be hired to perform critical activities

LIFE CYCLE – CONTRACT NEGOTIATION

- When a bank decides to hire a third party, it should negotiate a contract outlining the roles, responsibilities and rights of all parties. Doing so can help the bank enforce the contract, limit liability and manage disputes with the third party.
- Leadership should obtain board approval of contracts where the third party will perform critical activities.
- Existing contracts should be reviewed periodically to verify they continue to serve the best interests of the bank and its clients.
- Banks should consider renegotiating contracts that no longer serve the best interests of the bank and its clients.

LIFE CYCLE – CONTRACT NEGOTIATION (CONT.)

- Contracts should have language addressing the following:
  - Nature and scope of the arrangement (e.g., service(s) and how they are to be provided)
  - Service level agreements, including performance measures/benchmarks
  - Reporting requirements and retention of records
  - Periodic audits by the third party's internal and external auditors (and bank personnel, if necessary) and prompt remediation of audit findings.
  - Compliance with laws, regulations and industry standards
  - Fees and other expenses
  - Confidentiality and protection of PII and other sensitive information

LIFE CYCLE – CONTRACT NEGOTIATION (CONT.)

- Contracts should have language addressing the following:
  - Resuming operations after a business interruption
  - Indemnification and insurance
  - Responses to and resolution of client complaints and disputes
  - Defaults and remedies
  - Termination of the relationship
  - Use and supervision of subcontractors
  - Choice of law and jurisdictional covenants for third parties in foreign countries
  - Performance of activities by external parties is subject to regulatory oversight/examination

LIFE CYCLE – ONGOING MONITORING

- Banks need to perform monitoring throughout the life of third-party relationships to properly assess and manage the risks associated with the outsourcing arrangement.
- Banks should compile a list of all third-party relationships and denote those where critical activities are performed. The scope and frequency of monitoring should vary directly with the complexity of the relationship and criticality of services provided.
- Monitoring should be performed by those with expertise and authority to monitor the third parties. Relationship owners should be assigned to and involved in monitoring.
- While banks can utilize reports and information provided by others to monitor third-party relationships, they may wish to schedule periodic onsite visits to gain direct knowledge of the vendor's operating practices and risk management capabilities.

LIFE CYCLE – ONGOING MONITORING (CONT.)

- Areas of consideration for ongoing monitoring of third parties include:
  - Business strategy
  - Reputation
  - Compliance with laws, regulations and industry standards
  - Financial condition (e.g., balance sheet, income statement, cash flow statement, etc.)
  - Insurance
  - Key personnel and their capabilities
  - Processes for proactively identifying, evaluating and managing evolving risks

LIFE CYCLE – ONGOING MONITORING (CONT.)

- Areas of consideration for ongoing monitoring of third parties include:
  - Processes for updating policies, procedures and controls as third-party operations evolve
  - Information technology and the management of information systems
  - Business continuity plans and business resumption capabilities
  - Management of risks related to the use of subcontractors
  - Conflicts of interest resulting from agreements with other entities
  - Safeguarding sensitive information
  - Consumer complaints and their remediation

LIFE CYCLE – ONGOING MONITORING (CONT.)

- Material concerns identified during ongoing monitoring should be escalated to leadership.
  - Increases in risk
  - Material weaknesses
  - Repeat audit findings
  - Deterioration in financial performance
  - Security and data breaches
  - System interruptions or degradations
  - Compliance violations
- Leadership should escalate significant concerns to the board, particularly when they relate to critical outsourced activities.

LIFE CYCLE – TERMINATION

- A bank may terminate third-party relationships for a variety of reasons.
  - Expiration or satisfaction of the contract
  - Appointing a new third party
  - Performing the activity directly
  - Discontinuing the activity
  - Breach of contract
  - Regulatory mandate to terminate the relationship
- Banks should have contingency plans to allow the efficient termination and/or transition of relationships with third parties.

FOUNDATIONS - INDEPENDENT REVIEW

- Leadership is responsible for seeing that independent reviews of third-party relationships are performed, particularly where critical activities are being performed.
  - Review list of considerations for independent reviews from OCC Bulletin 2013-29
- Leadership should evaluate independent review results to determine whether and how to adjust the bank's third-party risk management process.
- Independent review results should inform leadership of the effectiveness of the bank's third-party risk management process and support decisions about engaging in new (or maintaining existing) third-party relationships, performing outsourced activities directly, or ceasing activities altogether.
- Significant issues or concerns should be promptly and completely evaluated and addressed. The board should be advised of significant issues exceeding its risk appetite.

FOUNDATIONS – DOCUMENTATION & REPORTING

- Banks should maintain documentation supporting all phases of the five-step life cycle. Remember, if it was not documented, it never happened.
- Examples of documentation that should be maintained include:
  - Inventory of third-party relationships, organized by the criticality of activities performed
  - Planning documents supporting the onboarding of third parties
  - Contractual documents
  - Results and recommendations from due-diligence activities
  - Risk management and performance reports received from third parties
  - Reports to leadership and the board related to monitoring of third parties

FOUNDATIONS – OVERSIGHT & ACCOUNTABILITY

- The board and leadership are responsible for overall supervision of risk management processes.
- The board, leadership, and associates have individual and collective responsibilities for ensuring that risks related to outsourced activities are properly managed.
  - Review list of board, leadership and associate responsibilities from OCC Bulletin 2013-29
- Oversight of third-party activities should be risk-based and dependent on the complexity and criticality of each unique relationship.

EXAMPLES OF THIRD-PARTIES INVOLVED IN TRUST AND RELATED ACTIVITIES

- Technology system and data providers
- Outsourcing arrangements (general and specialized)
- Custodians/depositories
- Broker-dealers
- Automated trading platforms and trade portals
- Fiduciary audit
- Delegated fiduciary activities (e.g., investment management and account administration)
- Services provided to fiduciary accounts and beneficiaries

EXAMPLES OF TECHNOLOGY SERVICE PROVIDERS USED FOR TRUST ACTIVITIES

- Trust accounting systems
- Portfolio management and trade order entry systems
- IRS reporting/tax preparation
- Automated investment/administrative review systems
- Contact and document management systems
- Document management systems
- Corporate action notification systems

OUTSOURCING ARRANGEMENTS USED FOR TRUST ACTIVITIES

- Operations
- Specialized asset servicing (e.g., oil and gas interests)
- Client statement production and delivery
- Proxy processing and shareholder communications
- Asset valuation
- Tax reclamation
- Mutual fund processing

CUSTODIANS AND DEPOSITORIES

- OCC regulations permit banks to hold fiduciary assets off-premises if the bank maintains adequate safeguards and controls.
- Custodians and depositories also typically provide IT platforms that need to be properly controlled.

BROKER SELECTION

- Fiduciaries are required to seek "best execution" for client transactions.
- OCC regulations require that bank fiduciaries adopt and adhere to certain policies and procedures, including:
  - Brokerage selection
  - Brokerage allocation
  - Use of affiliated brokers
  - Soft-dollar arrangements

USE OF THIRD PARTIES TO PERFORM FIDUCIARY ACTIVITIES

- OCC regulations and guidance permit banks to use third parties to perform services related to the bank's exercise of fiduciary powers (12 CFR 9.4).
- Fiduciary activities, whether delegated or retained, are the board's responsibility.
- Fiduciaries are required to exercise reasonable care, skill, and caution when selecting agents and establishing the scope and terms of services performed by agents. The fiduciary must monitor third-party performance of the fiduciary activity and compliance with the contract.
- The use of third parties for fiduciary activities requires heightened oversight to ensure that the bank is fulfilling its fiduciary obligations and not engaging in impermissible conflicts of interests.

FIDUCIARY AUDIT

- OCC regulations require, under the direction of an audit committee of the board of directors, either an annual audit of all significant fiduciary activities, or a continuous audit system, consisting of discreet audits of each significant activity (12 CFR 9.9).
- Whether the fiduciary audit is performed internally or externally, the scope and coverage of fiduciary audits is the responsibility of the board. The board should base audit decisions on an appropriate assessment of fiduciary business risk and internal control systems.
- Whether internal or external, the auditors performing the fiduciary audit should have sufficient expertise in auditing fiduciary activities.

DELEGATION OF INVESTMENT MANAGEMENT TO THIRD PARTIES

- Decisions concerning the delegation of investment authority to a third party are matters of fiduciary judgement and discretion and require the exercise of care, skill, and caution.
- Some requirements overlap with OCC Bulletin 2013-29, but are more targeted to fiduciary investment requirements:
  - Investment methodology
  - Risk management process
  - Management personnel
  - Investment performance
  - Compensation and fees
  - Reporting capabilities

DELEGATION OF ACCOUNT ADMINISTRATION TO THIRD PARTIES

- If a trust requires special skills or expertise that a trustee does not possess, the trustee may delegate certain duties and powers to a third-party vendor if the power to delegate is authorized by applicable law.
- In addition to complying with OCC Bulletin 2013-29, a trustee must comply with applicable law when delegating a duty or power to a third-party vendor. Applicable law generally requires the trustee to use reasonable care, skill, and caution in:
  - Selecting an agent
  - Establishing the scope and terms of the delegation, consistent with trust purposes and terms
  - Periodically reviewing the agent's actions to monitor their performance
  - Compliance with the terms of the delegation.

CONFLICTS OF INTEREST

- When a bank delegates investment management to related parties or interests, such as an affiliate or an entity with which the bank has a business referral or other arrangement that benefits the bank or its affiliates, there is a conflict of interest. Before entering such arrangements, a bank should:
  - Ascertain that conflicts are authorized and disclosed in accordance with applicable law
  - Demonstrate that delegation is consistent with applicable law and best interest of the account
- Banks should apply the same standards for selection, continued use, and oversight of investment managers to whom it delegates investment discretion and who are related parties or interests that it applies to the selection, continued use, and oversight of other investment managers.

THIRD-PARTIES THAT PROVIDE SERVICES DIRECTLY TO FIDUCIARY ACCOUNTS AND BENEFICIARIES

- Bank fiduciaries may need to enter into business arrangements on behalf of an account or its beneficiaries, especially in the course of estate administration. Examples include:
  - Real estate agents
  - Insurance agents
  - Contractors
  - Care providers
- The duties of loyalty and care should dictate the selection of and use of service providers.
- Any conflicts must be authorized by and disclosed in accordance with applicable law, and the service provider selected based on the needs of the account.

SUPPLEMENTAL EXAMINATION PROCEDURES FOR RISK MANAGEMENT OF THIRD-PARTY RELATIONSHIPS

- Overview of OCC Bulletin 2017-7
  - Scope
  - Quantity of Risk
  - Quality of Risk
    - Policies
    - Processes
    - Personnel
    - Control Systems
    - Conclusions

QUESTIONS