elliott davis

Interagency Guidance on Third-Party Relationships Risk Management

Brody Ledbetter, CPA, CISA, CRCM
Audit Senior Manager
Brody.Ledbetter@elliottdavis.com

Bob Balzano, CPA
Audit Senior Manager
Bob.Balzano@elliottdavis.com

elliott davis

Disclaimer

This material was used by Elliott Davis during an oral presentation; it is not a complete record of the discussion. This presentation is for informational purposes and does not contain or convey specific advice. It should not be used or relied upon regarding any situation or circumstances without first consulting the appropriate advisor. No part of the presentation may be circulated, quoted, or reproduced for distribution without prior written approval from Elliott Davis.

elliott davis

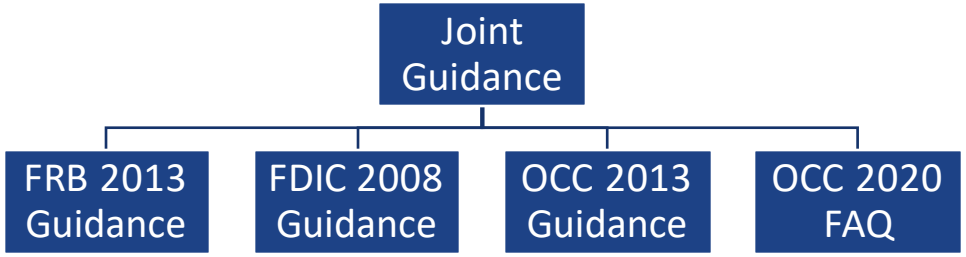
Agenda

- Overview
- Third-Party Relationship Life Cycle
  - Planning
  - Due Diligence and Third-Party Selection
  - Contract Negotiation
  - Ongoing Monitoring
  - Termination
- Governance
- Supervisory Reviews of Third-Party Relationships
- Comment Period Clarifications

Overview

Overview

- The FRB, FDIC, and OCC have jointly released comprehensive interagency guidance for managing third-party relationship risks.
    - Assist institutions in developing and implementing effective risk management practices throughout the entire life cycle of third-party relationships.
    - Finalized on June 6, 2023
    - Not adopted by NCUA



Overview, *continued*

- Institutions use third parties for quicker and more efficient access to technologies, capital, products, services, and markets.
  - Third parties, especially those utilizing innovative technologies, can present elevated risks to institutions and their customers.
    - Operational risk
    - Compliance risk
    - Strategic risk
  - The use of third parties does not remove or diminish our responsibility to manage risk.
    - “You can’t outsource risk.”

Overview, *continued*

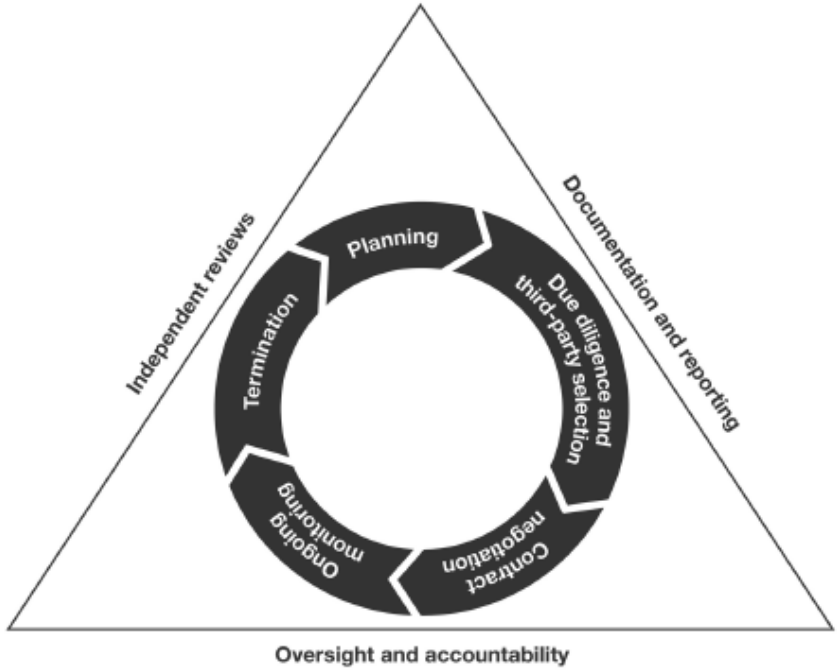
- Risk Management
  - Not all relationships pose same level of risk.
    - Varying degrees of required oversight
  - Institutions should maintain a complete inventory of its third-party relationships.
    - Periodically conduct risk assessments for each third party.
  - Allows tracking of whether risks have changed over time.

Overview, *continued*

- Risk Management, *continued*
  - More comprehensive oversight and management of higher-risk activities, including critical activities.
    - Critical activities including:
      - Significant risk if third party were to fail to meet expectations.
      - Significant customer impact
      - Significant impact on an institution's operations or financial condition

Third-Party Relationship Lifecycle

Third-Party Relationship Lifecycle



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

Third-Party Relationship Lifecycle, *continued*

- Staff with requisite knowledge and skills should be involved in each stage of the risk management lifecycle:
  - May involve experts from
    - Compliance
    - Risk
    - Technology
    - Legal Counsel
    - External Support

Third-Party Relationship Lifecycle

Planning

elliott davis

Planning

- Consider the following factors before entering a third-party relationship
  - Alignment with institution's strategic goals, risk appetite, and corporate policies.
  - Assess benefits and risks, plan risk management.
  - Consider arrangement details: activity volume, subcontractors, tech, customer interaction, foreign-based third parties.

Planning, *continued*

- Consider the following factors before entering a third-party relationship
  - Estimated costs: Contractual and indirect costs.
  - Impact on our employees:
    - What happens when we outsource these activities?
  - Impact on our customers.
  - Implications for physical security.
  - Our ability to maintain adequate, ongoing oversight and management of the relationship.
  - Contingency plans.

Third-Party Relationship Lifecycle

Due Diligence and Third-Party Selection

Due Diligence and Third-Party Selection

- The interagency guidance provides fourteen factors to consider in performing due diligence of a third-party, as follows:

  - Strategy and Goals
  - Legal and Regulatory Compliance
  - Financial Condition
  - Business Experience
  - Qualifications and Backgrounds of Key Personnel and Other Human Resources
  - Risk Management
  - Information Security
  - Management of Information Systems
  - Operational Resilience
  - Incident Reporting and Management Programs
  - Physical Security
  - Reliance on Subcontractors
  - Insurance Coverage
  - Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Review the third party's business strategy – is there M&A risks that may affect the service?
- Does the service provider have a service philosophy, quality standards, employment practices that align with our policies?

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Evaluation of ownership structure, including beneficial ownership
- OFAC concerns over owners or third party itself.
- Does the third party have the expertise, process, and controls to remain compliance with regulation.
- Responsiveness to compliance issues
- Process to mitigate risk of potential consumer harm

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Evaluate a third party's financial condition using audited statements, SEC filings, and other relevant sources to assess capability and stability.
- Consider additional factors, such as access to funds, growth, earnings, litigation, and debt ratings (when available) to gain a comprehensive understanding of the third party's overall financial health.

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Evaluate the third party's:
  - Resources (including staffing)
  - Previous experience
  - History of addressing complaints or litigation outcomes
- Consider any changes in activities or business model and review marketing materials for accuracy in representing capabilities.

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Evaluate third party qualifications and experience of key personnel related to the activity.
  - Consider periodic background checks for those with access to sensitive information.
  - Ensure procedures for identifying and removing unsuitable employees.
  - Verify employee training on duties, regulations, and risk factors.
- Assess third party's succession and redundancy planning for key personnel.
- Evaluate processes for holding employees accountable for compliance with policies and procedures.

Due Diligence and Third-Party Selection, *continued*

- Assess the third party's risk management effectiveness, including policies, processes, and internal controls. This involves:
  - Evaluating governance processes, roles, responsibilities, and segregation of duties.
  - Reviewing audit assessments and escalation/remediation processes for adequacy.
- Consider reports and certifications by independent third parties, such as SOC reports, in relation to the activity and the need for additional scrutiny

Due Diligence and Third-Party Selection, *continued*

- Assess the third party's information security program and its alignment with the institution's program.
- Identify and address gaps that could pose risks.
- Consider access controls, threat awareness, and vulnerability management.

Due Diligence and Third-Party Selection, *continued*

- Review and understand third party's business processes and information systems.
  - Evaluate gaps in:
    - service-level expectations, business processes and interoperability.
- Understand the third party's performance assessment measures for information systems.

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Evaluate disaster recovery and business continuity plans, including resumption timeframes and data recovery.
- Review resilience testing outcomes, telecommunications redundancy, and readiness for known and emerging threats.
- Examine risks related to provider dependencies and technology end-of-life issues.

Due Diligence and Third-Party Selection, *continued*

- Evaluate the incident reporting and management processes of the third party.
- Verify the presence of documented procedures, timelines, and clear accountability for incident identification, reporting, investigation, and escalation.

Due Diligence and Third-Party Selection, *continued*

- Ensure safety of people, facilities, technology, and data.
- Review on and off-boarding procedures for managing physical access rights.

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Due Diligence and Third-Party Selection, *continued*

- Evaluate the volume and types of subcontracted activities and their impact on risk.
  - Assess the third party's ability to identify, manage, and mitigate subcontracting risks.
  - Consider subcontractor selection, oversight, and control implementation.
  - Examine geographic location and provider dependencies.

Due Diligence and Third-Party Selection, *continued*

- Determine coverage extent.
- Assess coverage for various risks like dishonesty, natural disasters, data loss, and specialty areas (e.g., cybersecurity, intellectual property).

Due Diligence and Third-Party Selection, *continued*

- Evaluate third party's commitments to subcontractors or other parties.
- Assess if these commitments may introduce legal, financial, or operational implications and transfer risks to the institution or its customers.

Strategy and Goals

Legal and Regulatory Compliance

Financial Condition

Business Experience

Qualifications and Backgrounds of Key Personnel and Other Human Resources

Risk Management

Information Security

Management of Information Systems

Operational Resilience

Incident Reporting and Management Programs

Physical Security

Reliance on Subcontractors

Insurance Coverage

Contractual Arrangements with Other Parties

Third-Party Relationship Lifecycle

Contract Negotiation

elliott davis

Contract Negotiation

- The interagency guidance provides seventeen factors to consider during contract negotiations:

  - Nature and Scope of the Arrangement
  - Performance Measures or Benchmarks
  - Responsibilities for Providing, Receiving, and Retaining Information
  - The Right to Audit and Require Remediation
  - Responsibility for Compliance with Applicable Laws and Regulations
  - Cost of Compensation
  - Ownership and License
  - Confidentiality and Integrity
  - Operational Resilience and Business Continuity
  - Indemnification and Limits on Liability
  - Insurance
  - Dispute Resolution
  - Customer Complaints
  - Subcontracting
  - Foreign-Based Third Parties
  - Default and Termination
  - Regulatory Supervision

Contract Negotiation, *continued*

- Clearly define rights and responsibilities in the contract, including:
  - Nature and scope of the business arrangement.
  - Description of ancillary services, activities, and terms governing resource use.
  - Address dual employees' roles and reporting lines.
  - Consider potential contract termination or renegotiation in response to changing circumstances.

Contract Negotiation, *continued*

- Establish clear performance measures for evaluating third-party performance.
  - Utilize service-level agreements to define expectations and responsibilities.
  - Monitor conformance with policies, procedures, and regulatory compliance.
  - Use measures to enforce accountability and potentially reward excellence.
  - Ensure measures encourage responsible performance without compromising quality or compliance.

Contract Negotiation, *continued*

- Contract provisions should address:
  - Institutions timely data access.
  - Access to third-party data and documentation.
  - Data sharing with regulators for supervision.

Contract Negotiation, *continued*

- Provisions should outline the frequency and types of audit reports the institution is entitled to receive from the third party.
- Consider reserving the right for the institution to conduct its own audits or engage an independent party for audits based on the relationship's risk and complexity.

Contract Negotiation, *continued*

- Contracts must outline obligations for legal compliance.
  - Both the third party and the institution are responsible.
  - Enable monitoring of third party's compliance and timely issue resolution.

Contract Negotiation, *continued*

- Contracts should define costs and compensation:
  - Describe fees, including volume-based or special requests.
  - Specify conditions for cost structure changes.
  - Avoid incentives for risky behavior.
  - Clarify legal and audit fee responsibilities.

Contract Negotiation, *continued*

- Contracts must define ownership and licensing rights:
  - Specify the third party's use of the institution's property (name, logo, trademark).
  - Clarify data ownership and third-party intellectual property warranties.
  - Include provisions for software escrow agreements, ensuring access in specific conditions.

Contract Negotiation, *continued*

- Contracts must address risks related to sensitive information and infrastructure:
  - Prohibit unauthorized use or disclosure of sensitive data.
  - Mandate security measures for personally identifiable information.
  - Specify breach disclosure procedures.
  - Specify joint incident management exercise frequency.

Contract Negotiation, *continued*

- Contracts should ensure operational resilience and business continuity:
  - Address the third party's responsibility for controls and operational resilience measures.
  - Require business resumption and continuity plans.
  - Specify recovery time and objectives, along with procedures (RPO and RTO).

Nature and Scope of the Arrangement

Performance Measures or Benchmarks

Responsibilities for Providing, Receiving, and Retaining Information

The Right to Audit and Require Remediation

Responsibility for Compliance with Applicable Laws and Regulations

Cost of Compensation

Ownership and License

Confidentiality and Integrity

Operational Resilience and Business Continuity

Indemnification and Limits on Liability

Insurance

Dispute Resolution

Customer Complaints

Subcontracting

Foreign-Based Third Parties

Default and Termination

Regulatory Supervision

Contract Negotiation, *continued*

- Specify liability extent and reimbursement for third-party failures.
- Ensure limits on liability align with potential losses.
- Avoid holding the third party harmless from liability.

Contract Negotiation, *continued*

- Require the third party to maintain insurance (and name institution as insured)
  - And notify the institution of changes in insurance coverage.

Nature and Scope of the Arrangement

Performance Measures or Benchmarks

Responsibilities for Providing, Receiving, and Retaining Information

The Right to Audit and Require Remediation

Responsibility for Compliance with Applicable Laws and Regulations

Cost of Compensation

Ownership and License

Confidentiality and Integrity

Operational Resilience and Business Continuity

Indemnification and Limits on Liability

Insurance

Dispute Resolution

Customer Complaints

Subcontracting

Foreign-Based Third Parties

Default and Termination

Regulatory Supervision

Contract Negotiation, *continued*

- Disputes can impact third-party activities and the institution negatively.
- Consider establishing a dispute resolution process in the contract for timely issue resolution.
    - Evaluate whether third party should continue activities during dispute resolution.
- Assess contract provisions that affect dispute resolution, such as arbitration or forum selection.

Contract Negotiation, *continued*

- Specify responsibility for responding to complaints or inquiries.
  - For third-party responsibility, ensure timely responses and data provision.
  - For the institution's responsibility, mandate prompt notification of complaints or inquiries by the third party.

Contract Negotiation, *continued*

- Specify notification and approval requirements for subcontractors.
- Consider prohibitions on specific subcontractors.
- Define liability for subcontractor actions.
- Include a termination clause without penalties for non-compliance with subcontracting obligations.

Contract Negotiation, *continued*

- Contracts with foreign-based third parties should specify choice-of-law and jurisdiction.
- Be aware of foreign court interpretation and jurisdiction laws' impact.
- Seek legal advice for contract enforceability and potential legal implications, including privacy laws in cross-border agreements.

Contract Negotiation, *continued*

- Contracts should allow flexibility to change third parties.
  - Specify orderly transition requirements.
  - Address data and resource return.
  - Assign transition and termination costs.
  - Allow termination with regulator-directed notice and no penalties.

Contract Negotiation, *continued*

- Contracts should state that third-party performance is subject to regulatory examination.
- Specify retention and access to relevant documentation.

Third-Party Relationship Lifecycle

Ongoing Monitoring

Ongoing Monitoring

- Ongoing monitoring ensures the quality and sustainability of a third party's controls and compliance with contractual obligations.
  - It allows for the escalation and response to significant issues, such as audit findings, financial deterioration, security breaches, or compliance lapses.
- Monitoring activities may include:
  - Reviewing performance reports
  - Meetings with third-party representatives.
  - Regular testing of the institution's controls that manage risks from its third party.

Ongoing Monitoring, *continued*

- Intuitions may need dedicated staffing with the expertise for ongoing monitoring
  - Factors for ongoing monitoring include:
    - Assessing the overall effectiveness of the relationship
    - Changes in the third party's business
    - Financial condition
    - Compliance with laws and regulations
    - Personnel
    - Subcontractors
    - Training
    - Response to incidents

Third-Party Relationship Lifecycle

Termination

elliott davis

Termination

- Institutions can terminate third-party contracts for various reasons, including contract expiration or dissatisfaction with services.
  - Ensure efficient termination to minimize disruptions in daily operations.
  - Consider risks tied to transitioning service providers, operational impacts, and handling sensitive information.

Governance

Governance

- Oversight and Accountability:
  - The board of directors holds ultimate responsibility for overseeing third-party risk and ensures that appropriate policies and procedures are established.
  - Management develops and implements policies, procedures, and practices for third-party risk management in line with the institutions risk appetite and relationship complexity.
    - Management integrates third-party risk management into the institution's overall risk management processes, directs key activities, reports to the board, establishes organizational structures and staffing, implements internal controls, assesses compliance management, ensures access to third-party data, escalates issues to the board, and terminates arrangements that no longer align with strategic goals or risk appetite.

Governance, continued

- Independent Reviews:
  - Independent reviews play a crucial role in assessing the adequacy of an institution's third-party risk management processes.
    - The reviews evaluate whether third-party relationships align with the organization's business strategy and internal policies and standards.
    - They also assess the identification, measurement, monitoring, and control of risks associated with third-party relationships.
    - They ensure that conflicts of interest or the appearance of conflicts of interest are avoided when selecting or overseeing third parties.
  - The results of these reviews help the organization adjust its third-party risk management process, including policies, reporting, resources, expertise, and controls.

Governance, continued

- Documentation and Reporting:
  - Documentation and reporting depend on the risk and complexity of third-party relationships.
    - Key elements include an inventory of all third-party relationships, with a focus on higher-risk activities, including critical activities.
      - Documentation encompasses planning, risk assessments, due diligence results, executed contracts.
  - Periodic board reports, especially concerning dependency on a single provider for multiple activities.

Supervisory Reviews of Third-Party Relationships

Supervisory Reviews of Third-Party Relationships

- Supervisory Reviews of Third-Party Relationships:
  - Examiners may intensify their review of third-party risk management following the finalized interagency guidance.
    - Institutions should be prepared for potential examinations of their third parties.
  - Ultimate responsibility for compliance with applicable laws and regulations lies with the institution.
  - Management teams should assess their current third-party risk management practices in light of the finalized interagency guidance to identify any gaps or needed changes.

Comment Period Clarifications

Comment Period Clarifications

- Important Terminology:
  - Business arrangement – meant to capture the full range of third-party relationships.
    - Purposely broad given how these relationships have evolved and continue to evolve.
  - Critical activities – activities that may cause significant impact to customers or the institutions if the third party fails to meet expectations.
    - Institutions should have a methodology to designate which activities and 3rd party relationships should receive more comprehensive oversight.

Comment Period Clarifications, *continued*

- While commentors suggested adjusting requirements based on institution size, the agencies reiterated that the guidance is relevant to all institutions.
  - Not all third parties require the same extent of oversight, but all institutions have the responsibility to analyze risk.

Comment Period Clarifications, *continued*

- Agencies stated it would not be appropriate to assume lower levels of risk based solely on type of third party.
  - For example, just because the third party is an affiliate, or is regulated itself, does not lessen your due diligence requirements.

Comment Period Clarifications, *continued*

- Regarding circumstances in which institutions would have difficulty gathering information for due diligence, the agencies recommend:
  - If certain information cannot be gathered, institutions should consider alternative steps to mitigate the risks; or
    - If risks cannot be mitigated, determine if residual risk is acceptable.
- Consider information available from various sources like public regulatory disclosures.

STAY IN TOUCH

Brody Ledbetter, CPA, CISA, CRCM

Audit Senior Manager

Brody.Ledbetter@elliottdavis.com

Bob Balzano, CPA

Audit Senior Manager

Bob.Balzano@elliottdavis.com

500 E. Morehead Street | Suite 700

Charlotte, NC | 28202

elliottdavis.com

Thank You!

elliott davis