SALTMARSH, CLEAVELAND & GUND

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

August 24, 2023

Third-Party Relationships & Risk Management: New Interagency Final Guidance

J. Michael Maricelli, CIA, AAP

Saltmarsh, Cleaveland & Gund

ABOUT THE FIRM

Saltmarsh is one of the largest locally-owned CPA and business advisory firms in the Southeast, serving clients throughout the U.S. and worldwide from offices across Florida and in Nashville, Tennessee.

SIZE OF FIRM

OFFICE LOCATIONS

5

FLORIDA
Destin
Orlando
Pensacola
Tampa

TENNESSEE
Nashville

AFFILIATIONS

SALTMARSH FINANCIAL ADVISORS, LLC
Saltmarsh
Financial Advisors, LLC
AN AFFILIATE OF SALTMARSH, CLEAVELAND & GUND

THE BDO ALLIANCE USA
AN INDEPENDENT MEMBER OF
BDO
ALLIANCE USA

CELEBRATING 75 YEARS
Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

SERVICES OFFERED

Audit & Assurance | Business Valuation | Financial Institution Consulting | Financial Planning | Flexible Spending Plan Administration | Healthcare Consulting | Human Resources Consulting | Information Technology Consulting | Investment Management | Litigation & Dispute Advisory | Managed IT Services | Outsourced Accounting Solutions | Research & Development Tax Credits | Retirement Plan Administration | Tax Compliance & Consulting

OUR CLIENTS

Community Banks | Construction & Real Estate Development | Credit Unions | Governments, Municipalities, Special Districts & Pension Plans | High Net Worth Individuals | Hospitality | Manufacturing & Distribution | Non-Profit Organizations | Post-Acute Healthcare | Professional Employer Organizations | Technology & Emerging Growth

accountingTODAY 2022 Best Firms to Work For
People's Choice 2021 Best of the Best Tampa Bay Times
Inside Public Accounting Top 300 Firms 2022
Inweekly's Best of the Coast 2021
2021 Best of the Bay Pensacola News Journal Finalist
We AAM to Serve

saltmarshcpa.com | (800) 477-7458

New Interagency Guidance

Issued June 6, 2023, and currently in effect, by the following agencies:

- The Board of Governors of the Federal Reserve System (Board),
- The Federal Deposit Insurance Corporate (FDIC),
- The Office of the Comptroller of the Currency

Replaces each agency's existing general guidance on this topic.

Supervisory guidance does not have the force and effect of law and does not impose new requirements on banking organizations.

- Banks should consider the degree to which examiners will review third-party risk management practices through the lens of this guidance.

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Purpose

Provides consistency in the agencies' supervisory approach to third-party risk management,

Outlines the third-party risk management life cycle and identifies risk management principles applicable to each stage of the life cycle,

Clarifies that not all third-party relationships present the same level of risk or criticality to a Bank's operations,

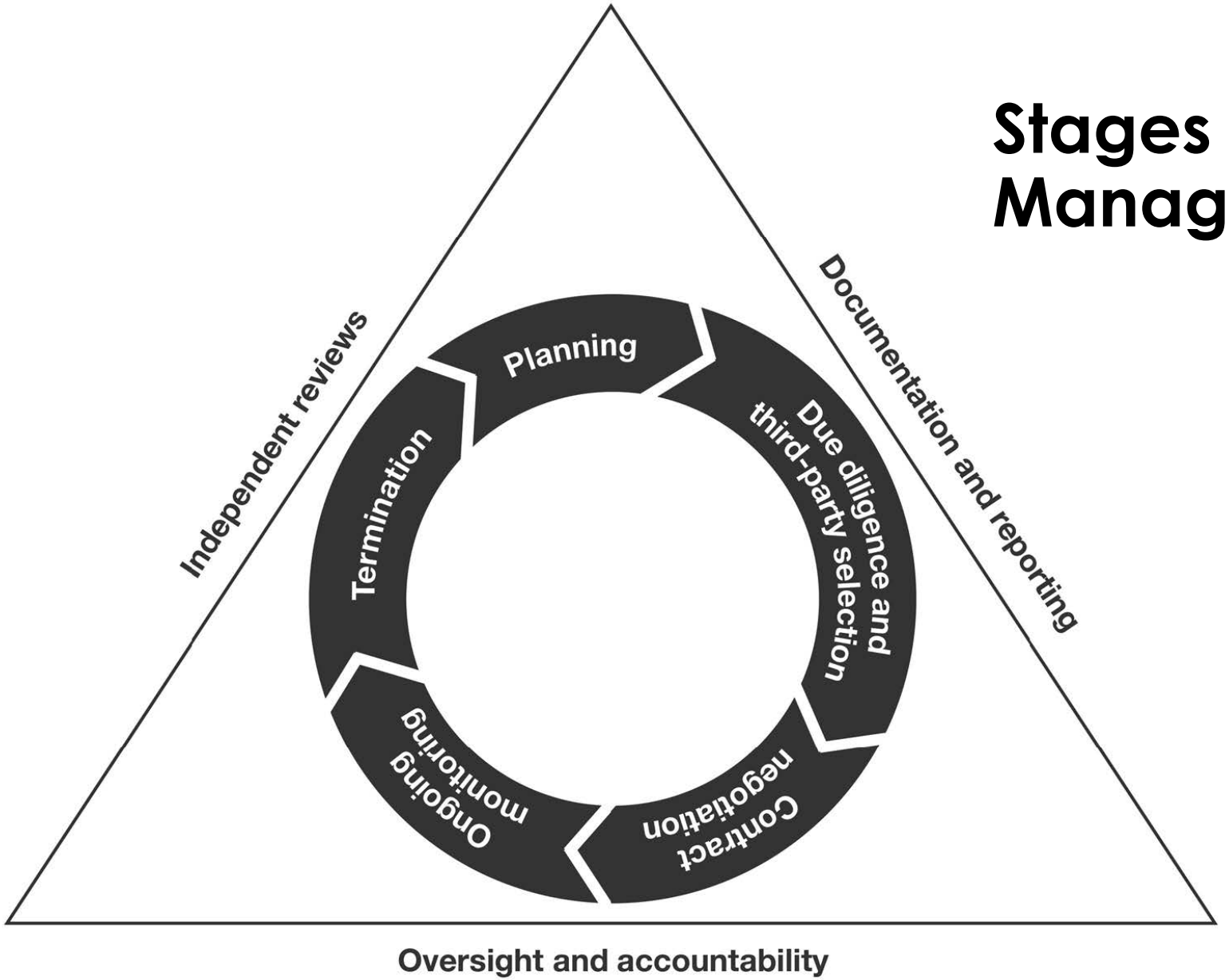
Describes sound risk management principles to consider when developing and implementing third-party risk management practices, commensurate with the Bank's risk profile and complexity as well as the criticality of the activity supported by the third party.

Key Details

Breaks down the Third-Party Relationship Life Cycle in five phases:

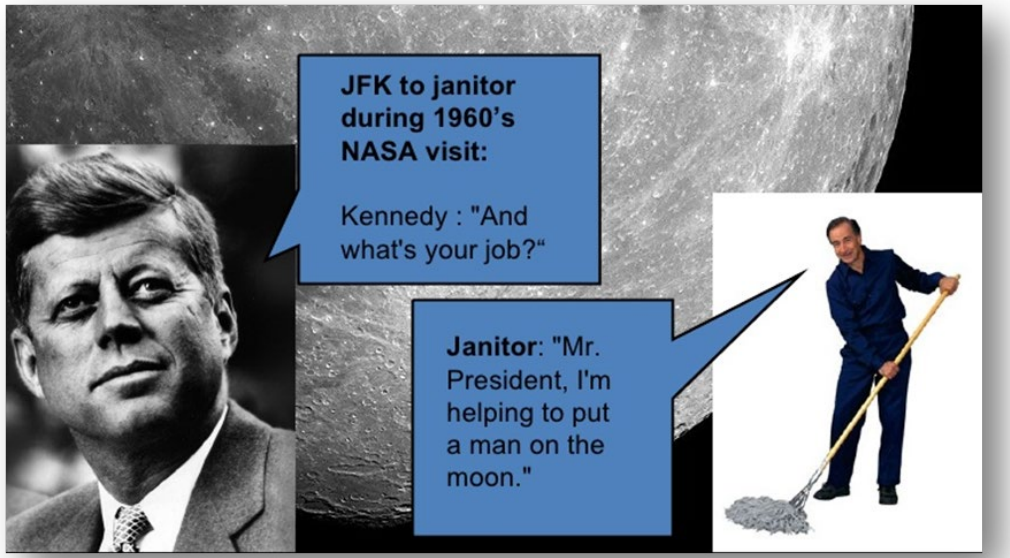
- Planning
  - Why are we outsourcing the activity? What are the risks? Can we control the risks?
- Due Diligence and third-party selection
  - Can the third party deliver quality products on time and comply with laws and regulations?
- Contract Negotiation
  - Does the contract contain clearly defined performance metrics?
  - Does the contact contain acceptable language regarding third party's use of subcontractors?
- Ongoing Monitoring
  - Monitoring of a third party's performance and controls should be performed on a periodic OR **continuous** basis depending on the activity supported by the third party (i.e., higher-risk activities)
  - Banks should have an escalation process for new risks identified.
- Termination
  - Terms and conditions for ending a third-party relationship should be outlined in the contract and include cause for termination, costs, and how data and intellectual property will be handled.

Stages of the Risk Management Life Cycle



Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Changes to Third-Party Risk Management



New definitions:

- A consistent, definitive definition of third-party relationship: Any business arrangement between a Bank and another entity by contract *or otherwise*
  - The word "vendor" is not used anywhere in the guidance
  - How do you identify third parties?
- "Critical activities" are activities that may:
  - Cause a Bank to face significant risk if the third party fails to meet expectations
  - Have a significant impact on customers
  - Have a significant financial impact on a Bank's financial condition or operations

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Changes to Third-Party Risk Management

A Sound Methodology

- An activity that is critical for one Bank may not be critical for another.
- Criticality or risk levels may be assigned to each third-party relationship or to identified critical activities and those third parties that support such activities.
- Sound methodology will be required to designate activities and third-party relationships requiring a more comprehensive oversight.

Changes to Third-Party Risk Management

Increased expectation Bank's will involve staff and outside experts with the requisite knowledge and skills in each stage of the risk management life cycle.

- Experts may be needed across disciplines such as:
  1. Compliance
  2. Risk Management
  3. Technology
  4. Legal

Third-party risk management is no longer the exclusive purview of the IT Department.

- Gone are the days we could look at insurance certificates and SOC reports once per year.
- Many of today's third parties perform functions on behalf of the Bank in real or near real-time.
- Does your Bank utilize social media? Who is responsible for posting on social media? Who monitors for complaints received on social media?

Changes to Third-Party Risk Management

Expansion of due diligence requirements -- OCC, FDIC, and Fed supervised Banks will need to address:

1. Strategies and goals
2. Legal and regulatory compliance
3. Financial condition
4. Business experience
5. Qualifications and backgrounds of key personnel and other human resource considerations
6. Risk management
7. Information Security
8. Management of information systems
9. Operational resilience
10. Incident reporting and management processes
11. Physical security
12. Reliance on subcontractors
13. Insurance Coverage
14. Contractual arrangements with other parties

Old School:
-Strategic
-Reputation
-Operational
-Transactional
-Credit
-Compliance

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Changes to Third-Party Risk Management

Increased emphasis on contracts as a control measure

- Compliance responsibilities
  - Does the contract require compliance with laws and regulations specific to the activity being performed by the third party?
  - Does the contract include the right to monitor and be informed about the third party's compliance with laws and regulations?
- Customer complaints
  - Does the third party interact with Bank customers?
  - Who receives complaints and inquires from Bank customers?
  - Does the contract specify the timeframe complaints must be processed by?
  - Does the contract contain provisions to receive from the third party, timely notification of any complaints or inquires?

Changes to Third-Party Risk Management

Integration of Third-Party risk management with the Bank's overall risk management processes

- Third-party risk management should be linked to other elements of the Bank's risk management program.
  - Reputation
  - Compliance
  - Strategic
  - Information Security
  - Business continuity and resiliency
- The actions of third parties can have an impact in each of these areas.

Third-Party Risk Management vs. Enterprise Resource Management

Third-Party Risk Management

- The ongoing process of overseeing third-party vendor and fintech relationships to weigh, assess and limit the potential risks of these relationships and decide whether a relationship falls within the Bank's risk tolerance.

Enterprise Resource Management (ERM)

- A system for managing risks holistically throughout the Bank to create value.
- ERM includes identifying, assessing, mitigating, measuring, monitoring, and communicating risks.

Third-Party Risk Management vs. Enterprise Resource Management

ERM addresses full span of risks including:

1. Operational Risk
2. Transaction Risk
3. Compliance Risk
4. **Third-Party Risk**
5. Credit Risk
6. Strategic Risk
7. Reputation Risk
8. Cyber Risk
9. Concentration Risk

Other Takeaways

No published examination procedures

- The scope of the supervisory review depends on the degree of risk and the complexity associated with the Bank's activities and third-party relationships.

No checklist to follow to ensure compliance

- Boards will need to risk tolerances for their respective Banks and management will need to develop procedures to carry out third-party risk management practices within Board approved risk tolerances.
- While the guidance applies to all banking organizations under the supervision of the Board, FDIC, and OCC, it is not expected to be put into practice in the same way from Bank to Bank.
- Recognizing that a third-party may present a different degree of risk from Bank to Bank, Banks are encouraged to tailor their respective risk management practices.

Other Takeaways

Oversight

- Banks should have a process for escalating significant issues or concerns identified during the initial due diligence or ongoing monitoring phases of the third-party lifecycle.
- Periodic reporting on the Bank's third-party relationships, including the results of management's planning, due diligence, contract negotiation, and ongoing monitoring activities.

Questions?

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

CONTACT

J. Michael Maricelli, CIA, AAP

Senior Consultant, Financial Institutions

michael.maricelli@saltmarshcpa.com

(225)-571-6255

(800) 477-7458

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS