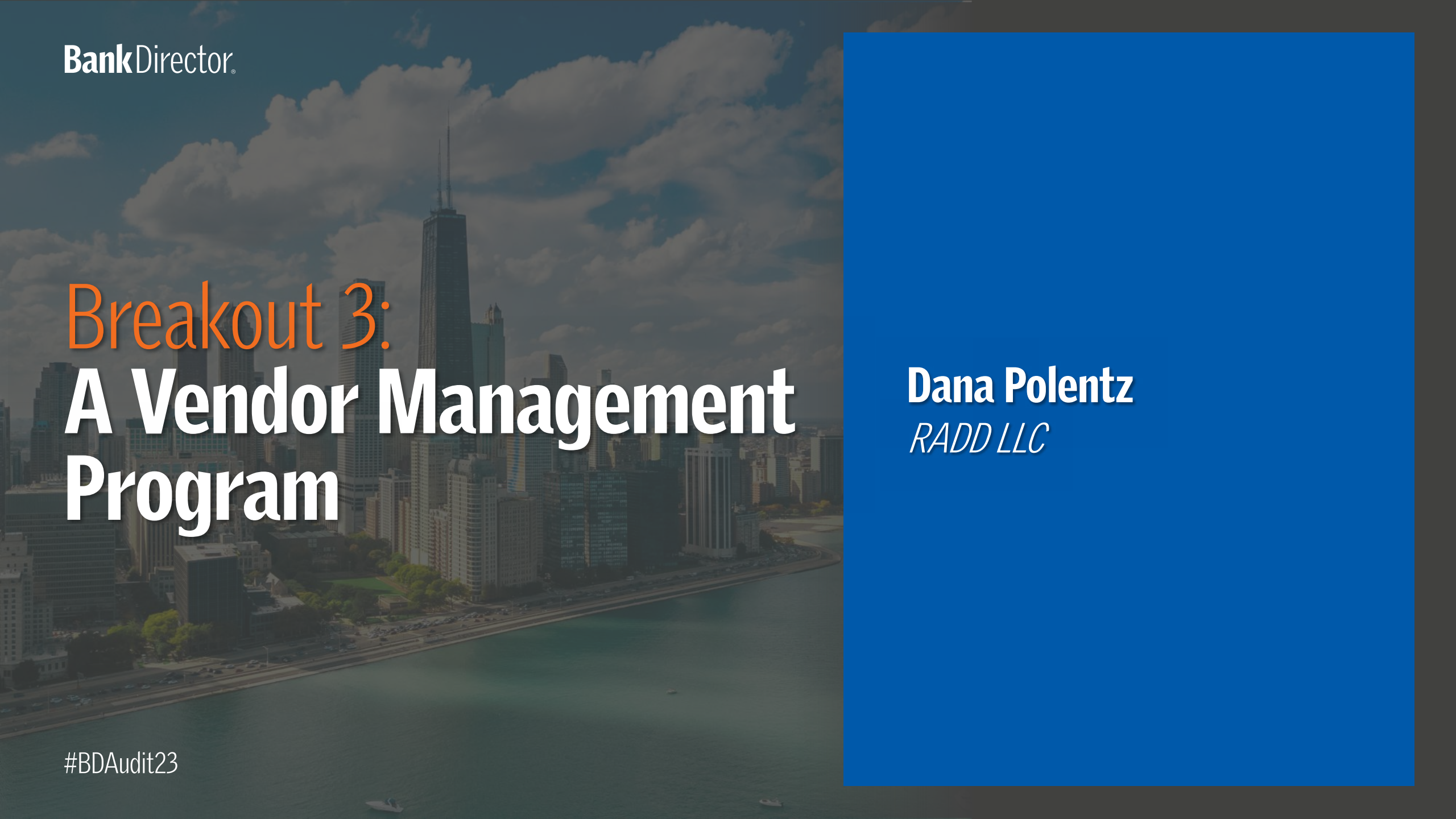


Bank Director

Breakout 3: A Vendor Management Program

Dana Polentz
RADD LLC

#BDAudit23

EFFECTIVE THIRD-PARTY VENDOR MANAGEMENT AND MONITORING

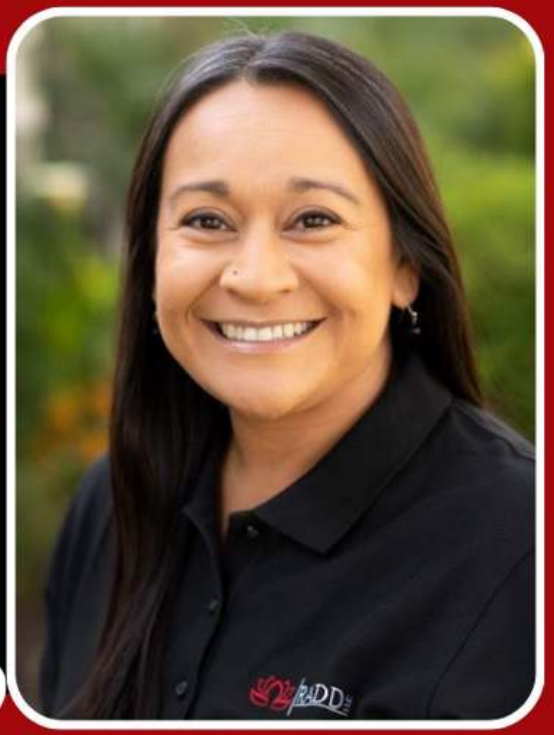
RADD LLC VENDOR MANAGEMENT PRESENTATION

Thank you Bank Director

Introduction

Meet The Speaker

Dana Polentz is a Director within the Audit & Advisory group at RADD LLC. She has a broad background in accounting, lending (consumer, commercial, and SBA loans), deposit and lending operations, auditing, and finance. She has spent the previous 19 years focused on operational and technology driven audits for a variety of companies ranging from $400M - $50B in assets. Dana has worked closely with many companies to establish and assist with internal controls and continuous monitoring for the purpose of simplifying SOX 404 attestations along with reducing cost for audit and compliance. Lastly, Dana is a Certified Information Systems Auditor, Certified Data Privacy Solutions Engineer and ISO 270001 Lead Auditor.



DANA POLENTZ

Director, Audit & Advisory

Table of Contents

What is a Third-Party Vendor?

Third-Party Vendor Definition:

A third-party vendor is an external entity that provides goods, services, or both, which are related to the institution's operation. They are not part of the financial institution itself (the first party) or its customers (the second party). These relationships are typically governed by a contractual agreement.

Third-Party Vendor Relationships

Vendors can be classified into various levels based on their potential impimpact on the financial institution's operations, objectives, compliance and risk exposure

- Critical
- High Impact
- Moderate Impact
- Low Impact

Fourth-Party Vendor Relationships

What is a Fourth-Party Vendor?

A fourth-party vendor refers to a subcontractor or a vendor to the third party.

Why should you care?

Although an institution has no direct relationship with the fourth-party vendor, it can still be exposed to risk through that relationship. As such, the institution must ensure that the third-party vendor is effectively managing its relationship with the fourth-party vendor to mitigate this risk as the institution is ultimately responsible for the consequences.

Why is Third-Party Vendor Risk Management Important?

Vendor risk management is crucial for several reasons at the inception and continuous monitoring:

- Data Integrity; Security and Privacy
- Regulatory Compliance
- Financial Risk
- Operational Risk
- Reputational Risk
- Legal Risk
- Business Continuity

Regulatory Guidance
On Third-Party Management

Risk Management Process:

1. Risk Assessment
2. Due Diligence in Selecting a Third-Party
3. Contract Structuring and Review
4. Oversight

Regulatory Environment and Compliance

- OCC Bulletin 2013-29
- FRB SR 13-19/CA 13-21
- CFPB Bulletin 2012-03
- FINRA
- FFIEC
- NCUA SL No. 07-01
- Sarbanes-Oxley Act (SOX)

Components of Third-Party Vendor Management Program

A comprehensive vendor risk management program includes several key components that help manage the risks associated with third-party vendors:

- Policies and Procedures
- Vendor Selection and Due Diligence
- Risk Assessment
- Contract Management
- Ongoing Monitoring and Review
- Incident Management and Contingency Planning

Due Diligence Process

An effective due diligence process for potential vendors entails multiple steps including:

- Understanding the Vendor's Business Model
- Evaluating Vendor Financials
- Assessing Vendor Reputation
- Checking Information Security Practices
- Reviewing Legal and Regulatory Compliance
- Analyzing Business Continuity and Disaster Recovery Plans
- Verifying Insurance and Bonding Coverage
- Verification of SOC 1 and SOC 2 compliance – initially and continuously

Risk Assessment

Conducting a risk assessment on a potential vendors is crucial in vendor risk management to allow the institution to proactively identify and manage potential risks before they become problems. This can protect the institution from disruptions, financial loss, reputational damage, and regulatory penalties.

The risk assessment process involves:

1. Risk Identification
2. Risk Analysis
3. Risk Evaluation

Contract Negotiation

Effective contract negotiations are central to managing third-party vendor risk by establishing clear expectations, set performance standards, and detail the right sand obligations of each party.

The contract can be a critical tool for risk mitigation. By including specific provisions, the institution can ensure risks are appropriately managed. These may include:

- Scope of Services
- Minimum Performance Standards and Penalties
- Indemnification Clauses
- Use of the Institution's Intellectual Property
- Data Protection and Security
- Contract Modification Capabilities
- Service Level Agreements (SLAs)
- Legal Aspects
- Audit requirements
- Business Continuity and Incident Management
- Subcontracting Relationships
- Costs and Service Fees
- Duration of Contract
- Termination Rights

Ongoing Monitoring and Performance Management

Ongoing monitoring of third-party vendors is crucial to ensure compliance with contractual obligations, identify potential risks, and ensure delivery of expected service levels. Monitoring provides the following benefits:

- Risk Mitigation
- Contract Compliance
- Service Quality Assurance

To establish effective vendor monitoring mechanisms, consider the following:

- Performance Dashboards
- Regular Audits – including SOC Report review and CUECs considerations
- Frequent Communication

Tools and Technologies for Vendor Risk Management

Institutions should consider using vendor management tools to help mitigate vendor risk. Vendor management tools offer multiple benefits including streamlining and enhancing the process of managing and monitoring third-party vendor relationships.

01

Efficiency

Automated vendor management tools can handle repetitive tasks such as data entry, tracking due dates, and generating reports. This saves time and reduces the chances of human error.

02

Centralized Information

These tools offer a centralized location for all vendor-related information, including contracts, performance data, compliance documents, etc. This makes it easier to access and manage the data, especially for organizations dealing with multiple vendors.

03

Risk Management

Advanced vendor management technologies can provide real-time visibility into vendor performance and risks, helping organizations proactively mitigate potential issues. Some tools also have predictive capabilities, using AI and machine learning to forecast potential future risks.

04

Compliance Management

Vendor management tools often include features to help ensure compliance with relevant regulations, industry standards, and contractual obligations. These features may include automated reminders for due diligence reviews or compliance checks.

05

Performance Tracking

These tools can track key performance indicators (KPIs) and service level agreement (SLA) metrics to ensure vendors meet their contractual obligations. Regular reports and dashboards provide clear insights into vendor performance.

Key Takeaways

01

Importance of Effective Third-Party Vendor Risk Management

02

Comprehensive Vendor Risk Management Framework

03

Use of Vendor Management Tools and Technologies

Conclusion

To conclude, effective third-party vendor risk management is crucial for financial institutions to ensure regulatory compliance, mitigate risks, and maintain operational resilience. By implementing robust risk management frameworks, leveraging vendor management tools, and fostering a culture of continuous improvement, we can safeguard our organization and enhance our vendor relationships for long-term success. Thank you for your participation, and we welcome your questions and further discussions.

THANK YOU

Contact Information

Website: https://www.raddllc.com/
E-mail: Radhika@raddllc.com or Dana@raddllc.com
Phone: 833-RADD-LLC or 714-624-8222

Social Media: