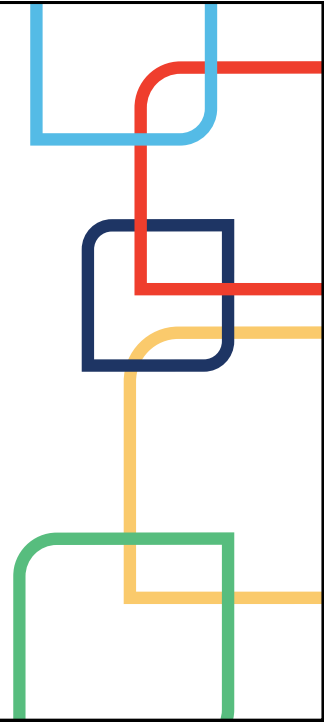


KEYS PRECONFERENCE

Savannah Richardson & Alyssa Pugh

# Third-Party Risk Management Workshop



1

## DISCLAIMER

- **This presentation is for information only.**  
Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**  
Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**  
Unauthorized release of this information is prohibited.  
Original material is copyright © 2024 Tandem.



2



## Savannah Richardson

ITRF  
Tandem Software Specialist



## Alyssa Pugh

CISM, Security+  
Tandem GRC Content Manager



4



DIGITAL VERSION  
[Tandem.App/](#)  
Vendor-Management-  
Workbook



5

# DISCUSSION TOPIC

## SMALL GROUPS

1. What is your name?
2. Where do you work?
3. How long have you been doing vendor management?
4. Why is this topic important to you?



6

# Agenda

## HERE'S THE PLAN

### Session 1

- **Identifying Vendors**
- **Governance, Risk, & Compliance (GRC)**
  - Why GRC?
  - Governance
  - Compliance
  - Risk Management
- **Due Diligence**
  - Due Diligence 101
  - Troubleshooting & Reviewing Due Diligence

### Session 2

- **Contract Management**
  - Contract Management 101
  - Contract Reviews
- **Practical Application**
  - Incidents
  - FinTechs
  - AI Service Providers



7

# Identifying Vendors

THIRD-PARTY RISK MANAGEMENT WORKSHOP

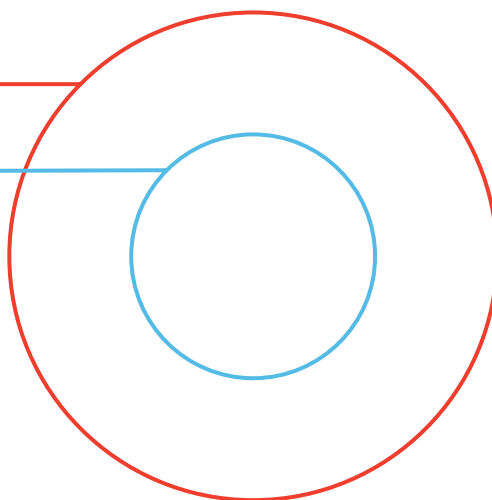


8

## Vendors vs. Third Parties (Page 6)

Third Parties

Vendors



9

DISCUSSION TOPIC

BIG GROUP TOPIC

What are some ways you identify or learn what vendors your organization uses?



10

# Finding Vendors

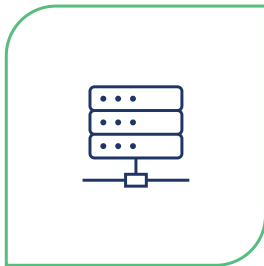
Employee Surveys



Accounts Payable



Business Impact Analysis (BIA)




Network Analysis



Procurement




11



**KEY TAKEAWAY**

# Find your vendors.



12

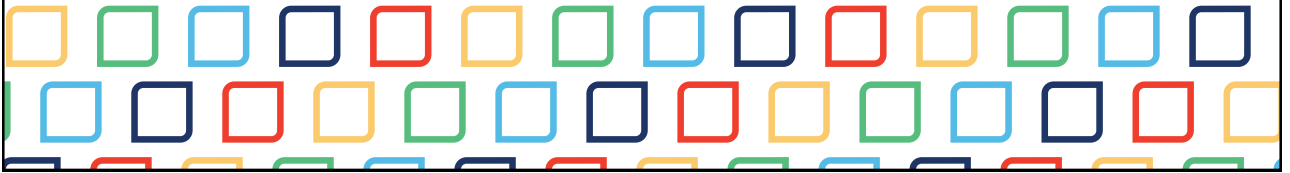
# Governance, Risk Management, & Compliance (GRC)

THIRD-PARTY RISK MANAGEMENT WORKSHOP



13

# Governance



14

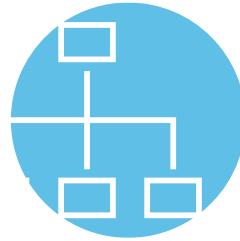


15

## Oversight & Accountability (Page 7)



Board of Directors



Senior Management



16

## Documentation & Reporting



Requirements & Expectations



Evidence of Effective Governance



Roles & Responsibilities



17



## Documentation & Reporting

**Policy**



**Program**



**Procedures**



18

## Independent Review

**1**

Strategic  
Alignment

**2**

Risk  
Management

**3**

Processes &  
Controls

**4**

Roles &  
Responsibilities

**5**

Conflicts of  
Interest




19



**KEY TAKEAWAY**

**Without governance,  
the vendor lifecycle is  
ineffective.**



20

# **Compliance**



21

# POLL QUESTION

SCALE OF 1 - 5

How familiar are you with  
vendor management laws, regulations,  
and guidance?



22



## Laws

Passed by Congress.  
U.S. Code. (USC)  
Legally enforceable.

### Examples

12 USC Ch. 18  
Bank Service Company Act (BSCA)

15 USC Ch. 94  
Gramm-Leach-Bliley Act (GLBA)



## Regulations

Enacted by Federal Agencies.  
Code of Federal Regulations (CFR)  
Legally enforceable.

### Examples

Interagency Guidelines Establishing  
Information Security Standards

Computer-Security / Cyber  
Incident Notification Rules



## Guidance

Published by Federal Agencies.  
**Not** legally enforceable on its own.

### Examples

FFIEC IT Examination Handbook:  
Outsourcing Technology Services (OTS) Booklet  
NCUA SL-07-01 Evaluating Third-Party Relationships

Interagency Guidance on Third-Party Relationships:  
Risk Management



23

# Bank Service Company Act (BSCA) (Page 5)

## THE REQUIREMENT

- **Who:** You notify the FDIC, OCC, or FRB
- **How:** "In Writing" | [Sample Form from FDIC](#)
- **When:** Within 30 Days
- **What:** Of signing a contract or beginning service with a bank service company.

## LEGAL REFERENCE

[12 USC Ch. 18 Bank Service Companies](#)

## BANK SERVICE COMPANIES

A service provider who 1) is solely owned by financial institutions and 2) provides one or more of the following services:

- Check and deposit sorting and posting;
- Computation and posting of interest and other credits and charges;
- Preparation and mailing of checks, statements, notices, and similar items; or
- Any other clerical, bookkeeping, accounting, statistical, or similar functions, including "data processing, internet banking, or mobile banking services" ([FIL-19-2019](#)).

LEARN MORE: [Read the Blog](#)



24

# Incident Notification Rules

## FOR BANKS

- 1
  - **Who:** You notify your federal regulator
    - FDIC ([FIL-12-2022](#))
    - FRB ([SR 22-4](#))
    - OCC ([Bulletin 2022-8](#))
  - **When:** ASAP and within 36 hours
  - **What:** A "notification incident"
- 2
  - **Who:** Bank service providers notify you
  - **When:** ASAP
  - **What:** An incident affecting service for 4+ hours

## FOR CREDIT UNIONS

- **Who:** You notify the NCUA ([23-CU-07](#))
- **When:** ASAP and within 72 hours
- **What:** A "reportable cyber incident"

## REGULATORY REFERENCES

- **FDIC:** [12 CFR Part 304, Subpart C](#)
- **FRB:** [12 CFR Part 225, Subpart N](#)
- **OCC:** [12 CFR Part 53](#)
- **NCUA:** [12 CFR Part 748.1](#)

WHEN IN DOUBT, REPORT IT.

FOR BANKS: [Watch the Webinar](#) | [Read the Blog](#)  
 FOR CREDIT UNIONS: [Watch the Webinar](#) | [Read the Blog](#)



25

# Interagency Guidelines (Page 5)

## THE REQUIREMENT

Each institution shall:

1. Exercise appropriate due diligence in selecting its service providers;
2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and
3. Where indicated by the institution's risk assessment, monitor its service providers to confirm that they have satisfied their obligations. As part of this monitoring, an institution should review audits, summaries of test results, or other equivalent evaluations of its service providers.

## SERVICE PROVIDERS

"Any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to the institution."

## REGULATORY REFERENCE

- **FDIC:** 12 CFR Part 364, Appendix B
- **FRB:** 12 CFR Part 208, Appendix D-2
- **OCC:** 12 CFR Part 30, Appendix B
- **NCUA:** 12 CFR Part 748, Appendix A



26

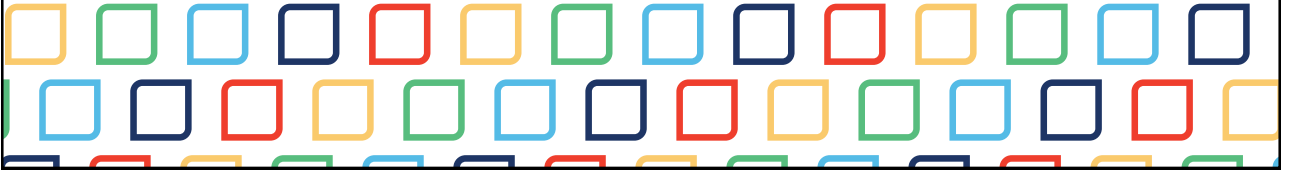
## KEY TAKEAWAY

Manage risk.  
Compliance will follow.



27

# Risk Management



28

## Significance vs. Risk



Significance

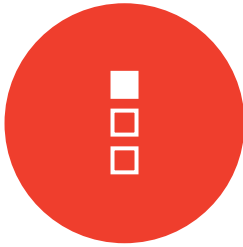


Risk



29

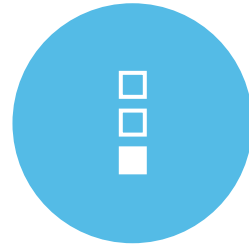
## Significance Levels



Critical



Significant



Insignificant



30

## DISCUSSION TOPIC

**SMALL GROUPS**

How do you determine what  
a “critical” vendor is?



31

## “Critical” Vendors

1

There are different types of critical.

2

There are different depths of critical.

3

There can be too many critical vendors.



32

“An activity that is critical for one banking organization **may not be critical** for another.”

Interagency Guidance on Third-Party Relationships: Risk Management



33



## Significance vs. Risk



Significance



Risk



34

## Vendor Risk Assessment (Page 9)



Identify the Risks



Understand the Impact



Show Your Work

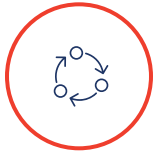


35

# Identify the Risks (Page 9)



Strategic



Operational



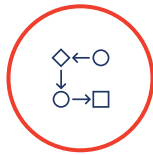
Reputational



Compliance



Credit



Subcontractor

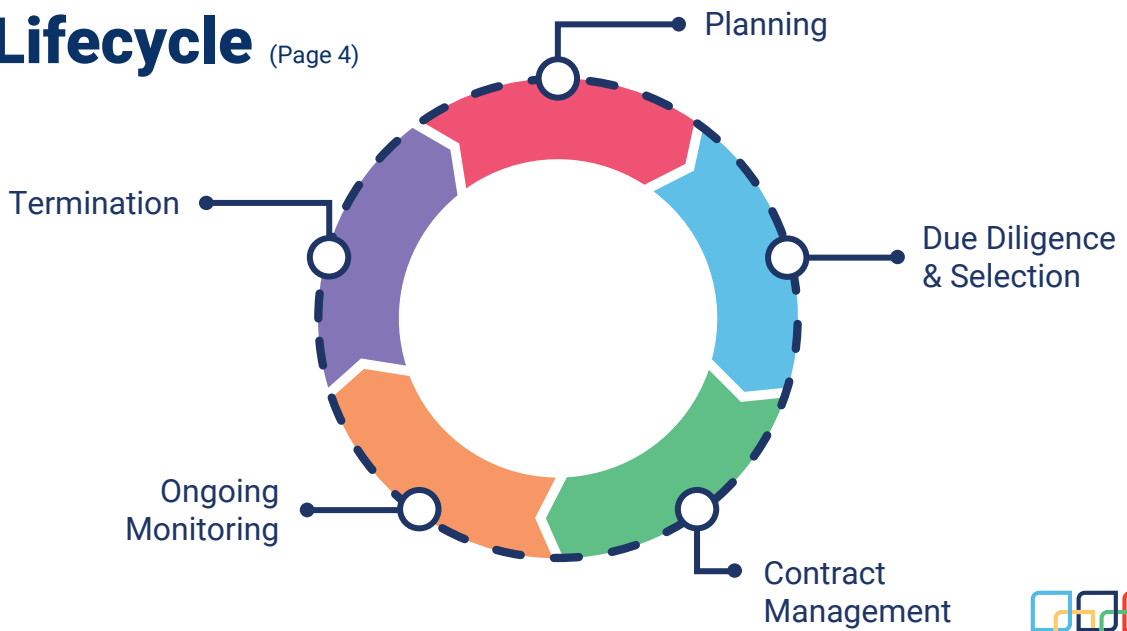


Country



36

# Lifecycle (Page 4)



37

“Risk assessments are a dynamic process, rather than a static process, and should be an ongoing part of a broader risk management strategy.”

NCUA Supervisory Letter 07-01: Evaluating Third Party Relationships

“Not all relationships present the same level of risk, and therefore not all relationships require the same level or type of oversight or risk management. [...] Periodically conducting risk assessments for each third-party relationship supports a banking organization’s determination of whether risks have changed over time and to update risk management practices accordingly.”

Interagency Guidance on Third-Party Relationships: Risk Management



38

KEY TAKEAWAY

Critical and high-risk vendors need more attention.



39

# Due Diligence

THIRD-PARTY RISK MANAGEMENT WORKSHOP



40

# Due Diligence 101



41

## Common Types of Due Diligence (Page 10)



Business Profile



SOC Report



Certificate of Insurance



Financial Statement



BCP Summary



Vendor Mgmt. Summary



42

## The If/Then Method

(Page 11)

IF

THEN



43

# Business Profile (Page 12)

If the vendor is going to provide services to you,

Then ensure they are qualified.



# Business Profile (Page 12)



Location & Contact Information



Business Experience



Staffing Qualifications



Compliance Requirements



# Insurance (Page 14)

If the vendor is going to provide services to you,

Then ensure they have insurance to withstand common losses.



46

# Insurance (Page 14)



General Liability



Errors & Omissions



Umbrella Liability



Workers' Compensation



Cyber Liability



47

# Business Continuity

(Page 16)

If a vendor service outage could impact your business,

Then assess the vendor's resilience and preparedness.



48

# Business Continuity (Page 16)

1

Written Plan

2

Review & Approval

3

Exercises & Tests

4

Service Level Agreements



49



# SOC Report (Page 18)

If the vendor stores information for you,

Then ensure their security is verified.



50

# SOC Report (Page 18)

## REPORTS

**SOC 1**  
Internal Controls Over  
Financial Reporting (ICFR)

**SOC 2**  
Trust Services Criteria

**SOC 3**  
Trust Services Criteria w/o  
Testing Details

## TYPE

**Type 1**  
Testing performed at a single point in time.

**Type 2**  
Testing performed over a period of time.



51

# Financial Statement

(Page 22)

If the vendor going out of business could impact you,

Then ensure the vendor is financially stable.



52

# Financial Statement (Page 22)

**Audited Financial Statements**



**Unaudited Financial Statements**



**Financial Stability Reports**



53

## Do Your Research

1

Credit Reports

2

References

3

Online Reviews



54

## Subcontractors (Page 26)

If the vendor uses subcontractors for critical functions,

Then ensure they manage their own vendors well.



55

## QUESTION

Should I personally manage my vendors' subcontractors?

## ANSWER

**No.** This is not a recommended practice and comes with several challenges.



56

## Why You Should Not Manage Your Vendors' Subcontractors

**1**

Inefficient

**2**

Poor Precedent

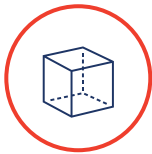
**3**

Legally Questionable



57

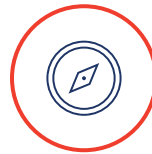
## Subcontractors (Page 26)



Volume



Nature



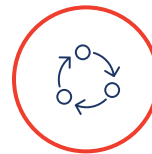
Reliance



Geography



Dependencies



Process



58

### KEY TAKEAWAY

While you should know who works with your data, systems, and processes, your vendors should be managing their own vendors.



59

## Other Types of Due Diligence

IF THE VENDOR IS A ...	THEN, LOOK AT ...
FinTech	Long-Term Business Plans
Software Developer	Software Development Procedures
Customer/Member-Facing Vendor	Complaint Handling Procedures
Bank Service Company	Examination Report
Real Estate Appraiser *	Consumer Compliance Practices
Payment Card Processor	PCI-DSS Compliance

\* <https://www.ffiec.gov/press/pr021224.htm>



60

### KEY TAKEAWAY

Due diligence is not about marking checkboxes. It's about managing risk.



61

# Troubleshooting & Reviewing Due Diligence



62

DISCUSSION TOPIC

**BIG GROUP TOPIC**

What do you do if the vendor won't respond to your requests?

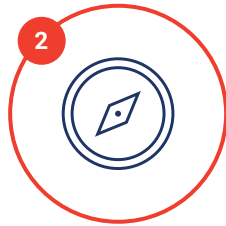


63

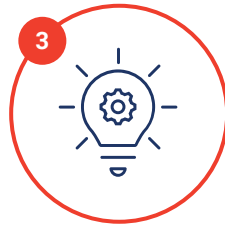
## Troubleshooting Due Diligence (Page 28)



**Communicate**  
with management



**Navigate**  
the risk carefully



**Validate**  
in another way



**Evaluate**  
your options



64

## Reviewing Due Diligence (Starts on Page 10)

1

Is it recent?

2

Does it seem reasonable?

3

Does it show any weaknesses?

4

Do I need to do anything in response?



65



**REPORT CARD**  
KEYS CLASSROOM

Name: M. Scott Year: 2024  
Address: D. Schulte Grading Period: Spring

SUBJECT	GRADE	FEEDBACK
Arts	A	
Computer	A+	
English	A	
History	B	Sign the following form
Math	A	
Music	A	
Science	A	
Social Studies	A+	
Physical Education	A	

**GRADING SCALE:**  
A+ = 90-100  
A = 80-90  
B = 70-80  
C = 60-70  
D = 50-60  
FNS = 00 and below


**TOTAL DAYS OF SCHOOL:**  
Days Absent: 0  
Days Absent:

66

# Reviewing Due Diligence (Starts on Page 10)


**Insurance Worksheet**  
**Business Continuity Worksheet**  
**SOC Report Worksheet**  
**Financial Statement Worksheet**  
**Subcontractors Worksheet**

67



**KEY TAKEAWAY**

# Review due diligence to learn about the vendor.



68



# Contract Management

THIRD-PARTY RISK MANAGEMENT WORKSHOP

69

**“The contract is the single  
most important control  
in the outsourcing process.”**

FFIEC Outsourcing Technology Services Booklet



70

# Contract Management 101



71

## What is Contract Management?



72

## Why Contracts?

**1**

Sets the Tone

**2**

Promotes  
Transparency

**3**

Cost Savings

**4**

Roles &  
Responsibilities



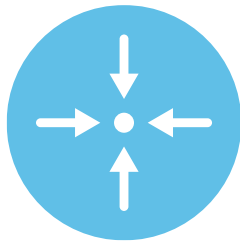
73

# Where are your contracts?

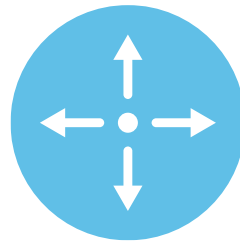


74

## Contract Responsibility (Page 7)



Centralized



Decentralized



75

## Types of Vendor Contracts (Page 30)



Software / Service Agreement



User Agreement



Terms of Service (TOS)  
Terms of Use



Nondisclosure Agreement (NDA)  
(Page 34)



Service Level Agreement (SLA)  
(Page 35)



76

**All contracts are legally binding.**  
Do you know what you just agreed to?



77

## GROUP DISCUSSION

Are some contracts more important than others?



78

## Risky Contracts (Page 30)

**1**

Long-Term  
Contracts

**2**

Highly Expensive  
Contracts

**3**

Critical Service  
Contracts



79

## Elements in a Vendor Contract (Page 32)

- Nature & Scope
- Performance Measures
- Information Responsibilities
- Right to Audit
- Compliance
- Cost & Compensation
- Ownership & License
- Confidentiality & Integrity
- Business Continuity & Resilience
- Indemnification Provisions
- Insurance
- Dispute Resolution
- Subcontracting
- Foreign-Based Vendors
- Default & Termination
- Regulatory Supervision



80

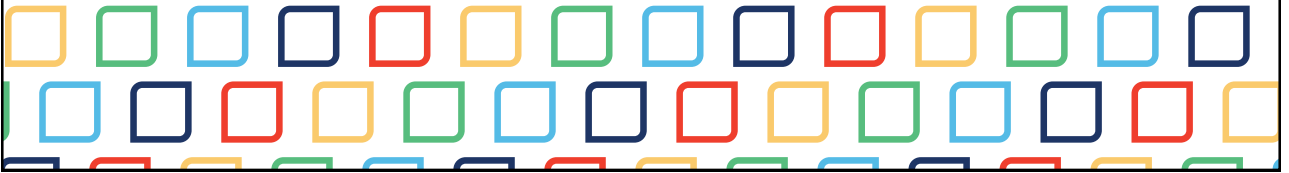
**Nothing is implied  
in contracts.**



81



# Contract Reviews



82

DISCUSSION TOPIC

SMALL GROUPS

Who is responsible for managing and reviewing contracts at your business?



83

## Contract Reviewers (Page 30)



Legal Professionals



Financial Experts



Subject Matter Experts



Senior Management



Risk Management Team



Compliance Officers



84

## Contract Reviews (Page 32)



85



“One of the greatest mistakes you can make in life is assuming all your thoughts are true.”



86

## Contract Reviews (Page 31)

**1**

Negotiate

**2**

Compensate

**3**

Evaluate



87

## Contract Reviews: Negotiate (Page 31)

### BAD SOUNDTRACK

"I have no control over what the contract says."

"We've already signed the contract, so there's nothing I can do to change it."

"The vendor will probably say no to my requests, so why would I bother asking?"

### GOOD SOUNDTRACK

"I have the right and the responsibility to ask for mutually beneficial changes."

"I can ask for an addendum or an amendment anytime one is needed."

"The vendor has the right to say no, but if I never ask, the answer is always no."

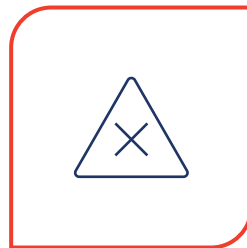


88

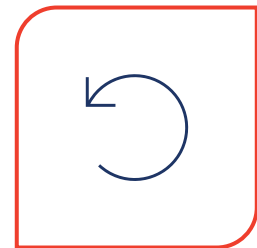
## Contract Reviews: Compensate (Page 31)



Enable Controls



Limit Access



Perform Backups



89

# Contract Reviews: Evaluate (Page 31)



90

## KEY TAKEAWAY

You have control over  
your contracts.



91

## DISCUSSION TOPIC

## GROUP DISCUSSION

How often should you review your vendors' contracts?



92



**Review before  
you sign.**



93

## Reassess Contract Adequacy (Page 36)



When You  
Change



When the  
Vendor Changes



Before  
Renewal Dates



If it is an  
Old Contract



94

### KEY TAKEAWAY

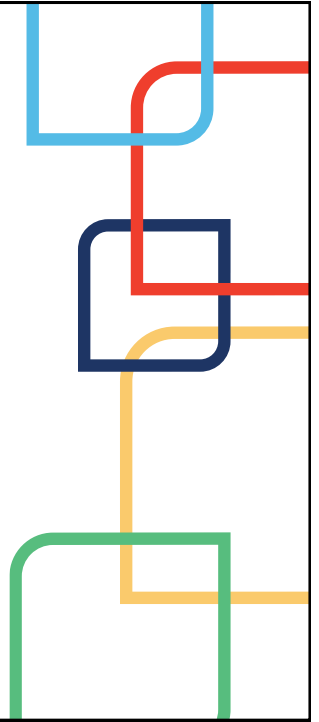
Assess contract  
adequacy periodically.



95

# Practical Application

THIRD-PARTY RISK MANAGEMENT WORKSHOP



96

## What if my vendor has an incident?



97



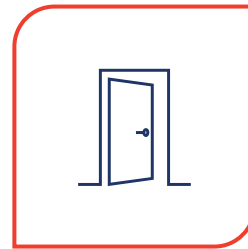
## Third-Party Incidents



Data Breach



Service Outage



Vulnerability Exploit



98

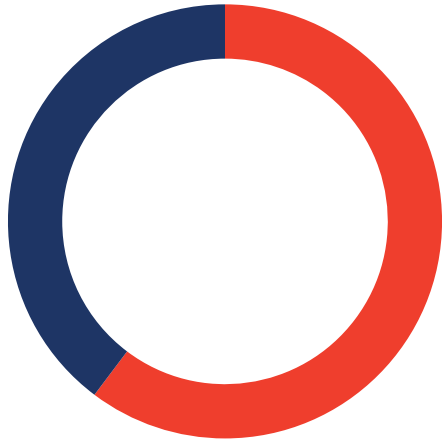
## DISCUSSION TOPIC

### SMALL GROUPS

Who are some of your vendors that experienced incidents in recent years?  
What was that like for you?



99

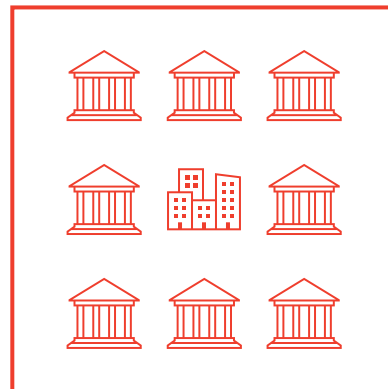
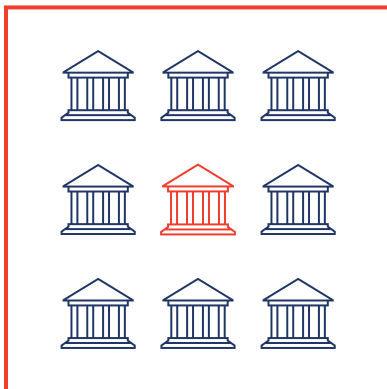


**NCUA BOARD UPDATE**  
“Over 60% of reported incidents were due to third-party compromises.”

<https://ncua.gov/files/agenda-items/cybersecurity-board-briefing-20231019.pdf>



100



101

## Preventing Third-Party Incidents



Due Diligence



Contract Management



102

## Detecting Third-Party Incidents



Negotiate  
Contract Terms



Subscribe to  
Email Lists



Participate in  
Information Sharing



Follow Reliable  
Sources



103

## Responding to Third-Party Incidents

- 1 Gather and review third-party statements about the incident.
- 2 Determine if the incident applies to you and assess the impact.
- 3 Reference SLAs, dispute resolution processes, termination options, etc.
- 4 Revoke third-party access to systems and data, if necessary.
- 5 Follow the third party's recommendations for remediating the incident.
- 6 Communicate with affected personnel and third parties (e.g., regulators, law enforcement, etc.).
- 7 Update the risk assessment and schedule more frequent reviews.



104

### KEY TAKEAWAY

Third-party incidents are **not your fault**, but it is your job to secure your data.



105

# Third-Party Incident Resources

- **Tandem Blog:** [Third-Party Incident Response Playbook](#)
- **Tandem Checklist:** [Third-Party Incident Checklist](#)
- **Tandem Knowledge Base Articles:**
  - [Incident Management Product Integrations](#)
  - [Vendor Management Product Integrations](#)



106

# What if my vendor is a FinTech company?



107

## DISCUSSION TOPIC

## SMALL GROUPS

What is a “FinTech” and have you worked with one?



108

“Partnerships with fintechs can provide community banks with [*access to new technologies*], enabling them to better serve their customers and deploy innovations that may be too costly to develop independently.”

Community Bank Access to Innovation through Partnerships



109

## Benefits of a FinTech Partnership



Easy Access



Cost Savings



Customer Experience



110

## What Are the Risks?



Financial Stability



Security & Privacy



Dependency



111

WHAT IF THE VENDOR

## Is a FinTech Company?

1

**Manage FinTechs**  
like any other vendor

2

**Get Creative**  
to fill in any gaps



112

## FinTech Resources

- **Regulatory Guidance:**
  - [Conducting Due Diligence on Financial Technology Companies](#)
  - [Community Bank Access to Innovation through Partnerships](#)
- **Tandem Blog:** [Creative Vendor Management: Managing FinTech Relationships](#)
- **Tandem Checklist:** [FinTech Due Diligence Checklist](#)
- **Tandem Knowledge Base Article:** [Review Template: FinTech](#)



113



# What if my vendor provides AI services?

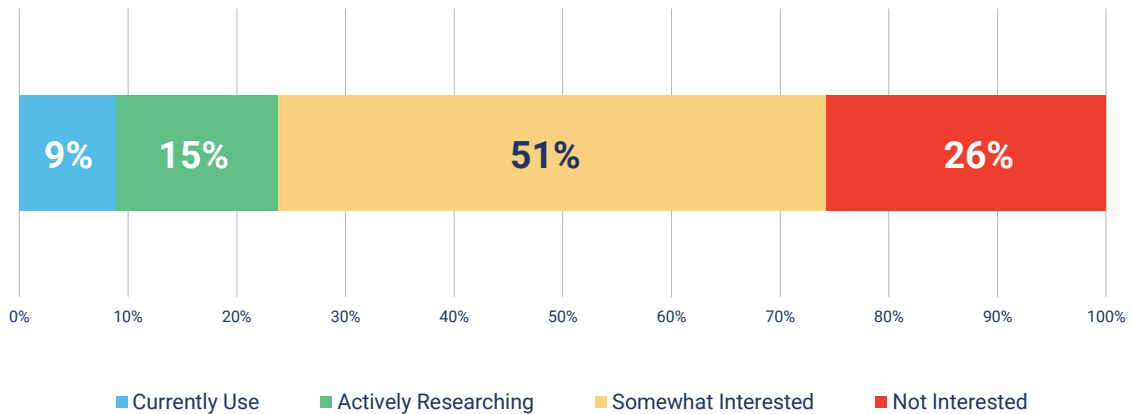


114

A collage of four overlapping report screenshots from the Tandem platform. From left to right: 1. 'Training' report showing a bar chart with red and blue bars and a table below. 2. 'Budget' report showing a bar chart with green and blue bars and two donut charts. 3. 'Board Oversight' report showing a horizontal bar chart with green and red bars and a table. 4. 'CYBER SECURITY REPORT' cover page with a dark background, colorful light trails, and the Tandem logo at the bottom right. The URL <https://tandem.app/state-of-cybersecurity-report> is visible at the bottom left of the collage.

115

## Use of AI Services



<https://tandem.app/state-of-cybersecurity-report>



116

## DISCUSSION TOPIC

### SMALL GROUPS

What are some ways you use  
(or are thinking about using)  
AI service providers?

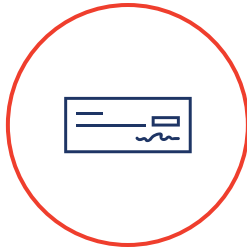


117

# AI Service Use Cases



Security Applications



Fraud Detection



Credit Underwriting



Support

<https://home.treasury.gov/news/press-releases/jy2134>



118

# AI Service Risks

Privacy Risks



Accuracy Risks



Security Risks



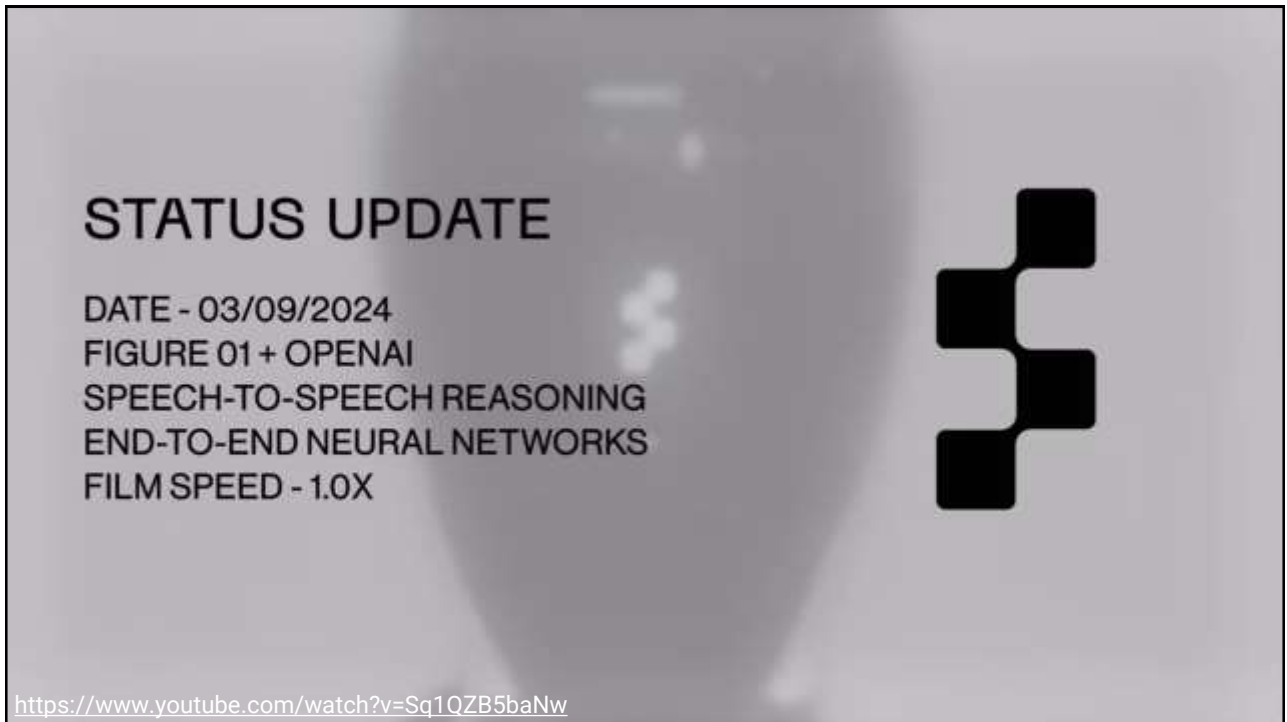
Legal Risks



Bias & Fairness Risks



119



120

ChatGPT

chat.openai.com

Clear chat

Chat History is off for this browser.

When history is turned off, new chats on this browser won't appear in your history on any of your devices, be used to train our models, or stored for longer than 30 days. This setting does not sync across browsers or devices. [Learn more](#)

Enable chat history

Upgrade plan  
Get GPT-4, DALL·E, and more

Alyssa Pugh

ChatGPT 3.5

You  
what due diligence should i do before selecting an AI/ML service provider?

ChatGPT  
Selecting an AI/ML service provider requires thorough due diligence to ensure that they meet your business needs and standards. Here's a comprehensive list of steps you can take:

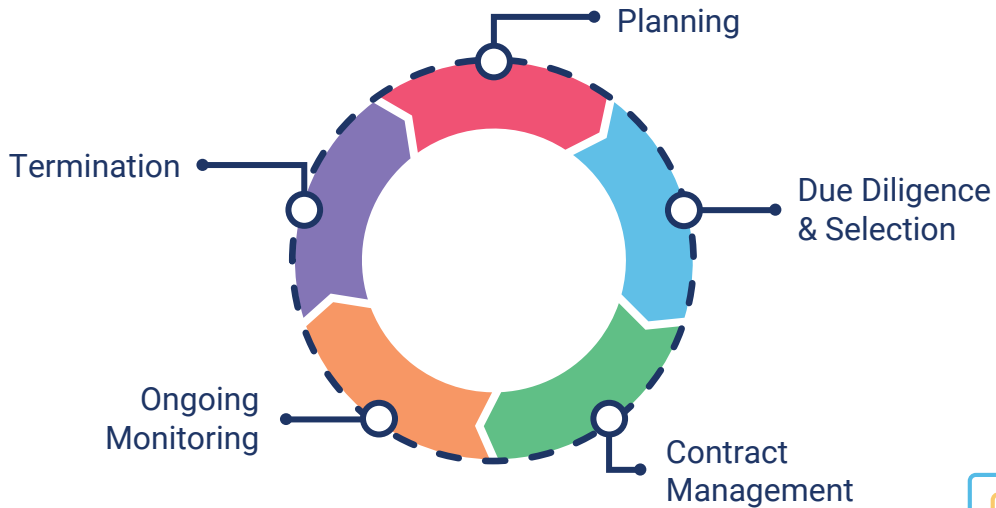
- Define Your Requirements:** Clearly outline your business objectives, project scope, budget, and timeline. Understand the specific AI/ML capabilities you need.
- Research Providers:** Look for AI/ML service providers through online research, referrals, industry events, and directories. Consider factors such as reputation, expertise, experience, and client testimonials.
- Evaluate Expertise:** Assess the provider's expertise in your industry and the specific AI/ML techniques and technologies you require. Look for case studies or projects similar to yours.
- Check Track Record:** Review the provider's track record of delivering successful AI/ML projects. Verify their experience with relevant use cases and their ability to meet deadlines and budgets.

Message ChatGPT...

ChatGPT can make mistakes. Consider checking important information.

121

# AI Service Risk Management



122

# AI Risk Management Resources



NIST AI Risk Management Framework



CISA / Joint Guidance on Engaging with Artificial Intelligence (AI)




Use of Artificial Intelligence Systems by Insurers



Treasury Department Report on Managing AI Risks in the Financial Services Sector




123



**KEY TAKEAWAY**

**AI is an emerging topic.  
Manage the risk accordingly.**



124



**Wrap Up**

THIRD-PARTY RISK MANAGEMENT WORKSHOP

125

THANKS FOR JOINING!

# Third-Party Risk Management Workshop

**Savannah Richardson**  
Software Specialist  
Tandem, LLC  
ITRF  
[srichardson@tandem.app](mailto:srichardson@tandem.app)

**Alyssa Pugh**  
GRC Content Manager  
Tandem, LLC  
CISM, Security+  
[apugh@tandem.app](mailto:apugh@tandem.app)

