

WELCOME TO

Connecting the Dots: Subcontractor Relationship Management

Samantha Torrez-Hidalgo, CSXF
Tandem Software Specialist
CoNetrix

DISCLAIMER

- **This presentation is for information only.**
Evaluate risks before acting on ideas from this session.
- **This presentation contains 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 © 2025 Tandem.

SESSION INFO



AUDIO / VIDEO

If you cannot hear sound or see the presentation now, adjust or change your settings.



SURVEY

At the end, fill out the survey for a chance to win an Amazon gift card.



RESOURCES

The slides, a recording, and certificate of attendance will be sent via email.



QUESTIONS

Use the "Questions" panel to chat with the presenters and Tandem team.

-  Audit Management
-  Business Continuity Plan
-  Compliance Management
-  Cybersecurity
-  Identity Theft Prevention
-  Incident Management
-  Internet Banking Security
-  Phishing
-  Policies
-  Risk Assessment
-  Vendor Management



Tandem™

A CoNetrix company

**SUBMIT YOUR
QUESTIONS!**

ABOUT THE PRESENTER



Samantha Torrez-Hidalgo
Tandem Software Specialist

- 10+ years IT / Service Industry XP
- 8 years with Tandem
- Thrives working with teammates
- Loves problem solving and helping others learn
- Conference speaker
- Published blog writer

[Linkedin.com/in/SamanthaTorrez](https://www.linkedin.com/in/SamanthaTorrez)



Subcontractor Definition



Identifying Subcontractors



Guidance & Regulations



Cautions & Considerations for Subcontractors



Reviewing Subcontractors

BONUS CONTENT
Vendor Management
Demo & Resources



What type of organization
do you work for?

What is your organization's
asset size?

Subcontractor Definition



Subcontractor

Individual or business that contracts to perform part (or all) of the obligations of another's contract

Managed Service
Provider (MSP)

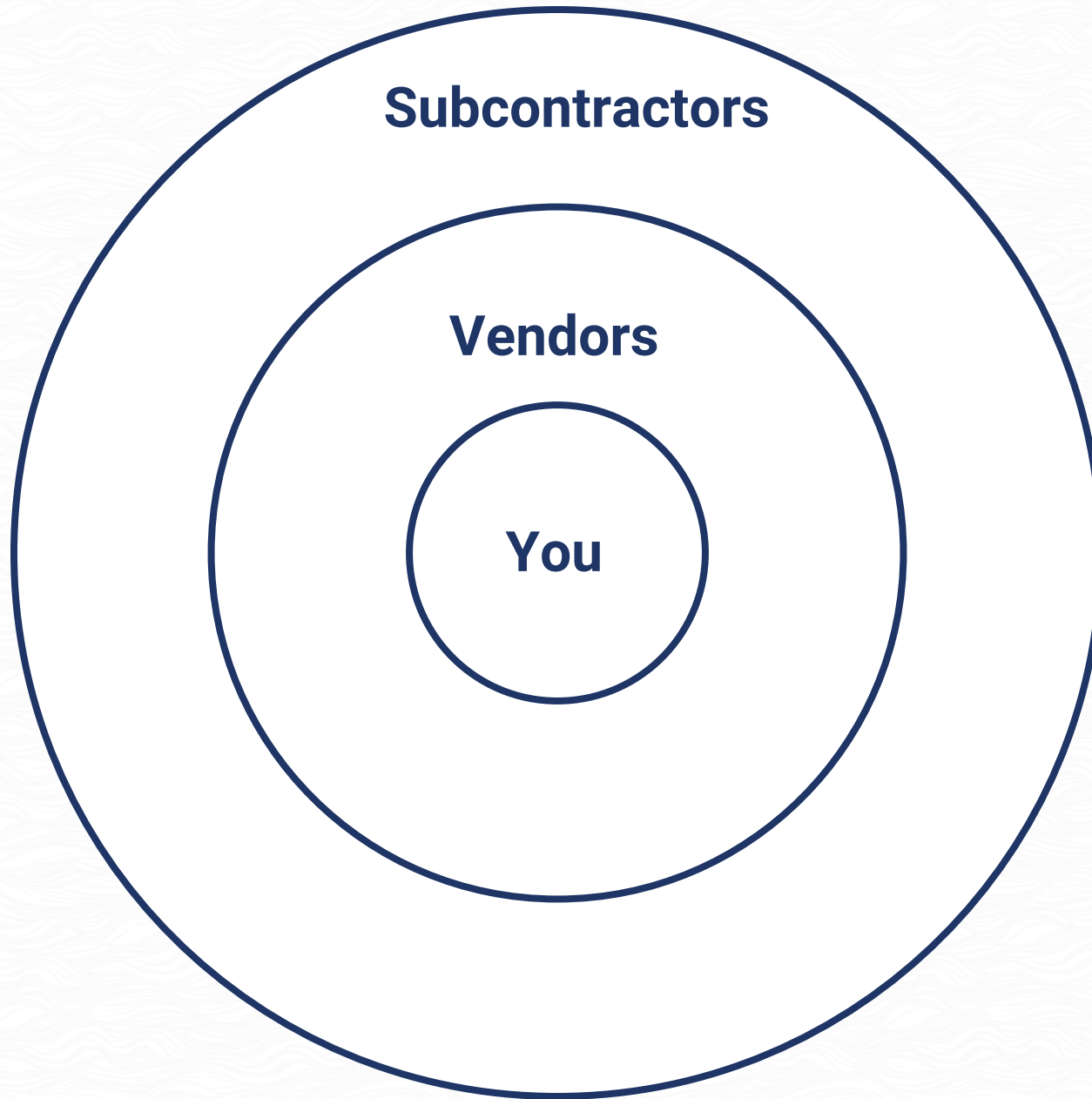


Subcontractor



Product
Licenses





Subcontractors

Vendors

You





Do Your
Research



Discuss Your
Options



Due Diligence
Matters

REMEMBER YOU KNOW





KEY TAKEAWAY

Finding out if your vendors are using subcontractors is always worth the time and effort.

Identifying Subcontractors

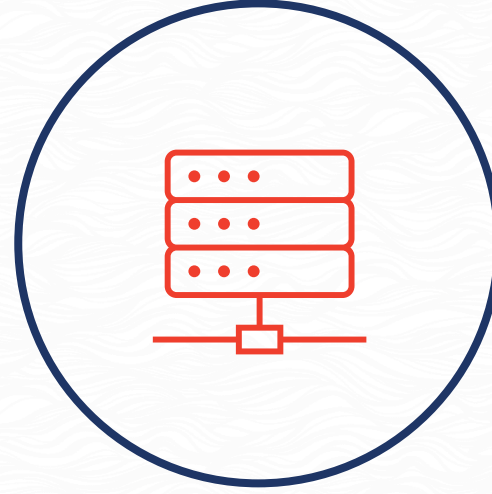
IDENTIFYING & TRACKING SUBCONTRACTORS



Ask Your
Vendors



Review
Contracts



Review SOC
Reports




Make a List

If / Then Method



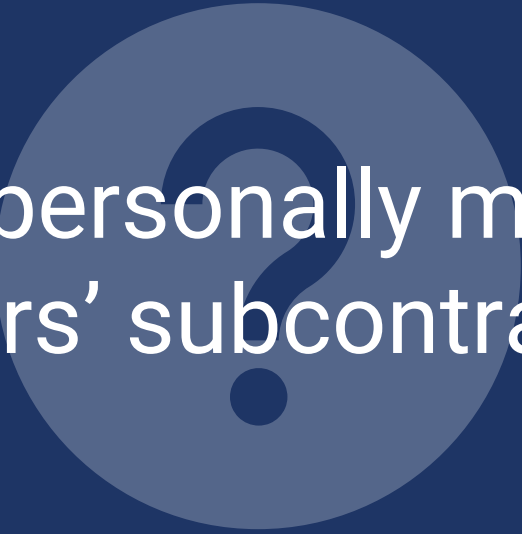
If a vendor stores
customer
information:



Then we
should get a
SOC report.

If the vendor uses subcontractors for critical functions,

Then ensure they manage their own vendors well.



Should I personally manage my vendors' subcontractors?



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

Why You Should Not Manage Your Vendors' Subcontractors

1

Inefficient

2

Poor Precedent

3

Legally
Questionable

How well do you know your vendors' subcontractor situation?

**You cannot manage your
vendors subcontractors,**

**but you *can* ensure your vendors
have a good third-party risk
management program.**



KEY TAKEAWAY

You can only manage your own expectations for your vendors – which can include them performing good due diligence on their subcontractors.

**SUBMIT YOUR
QUESTIONS!**

Guidance & Regulations

How familiar are you with guidance and regulation about subcontractors?

“The agencies acknowledge the risks and added complexity that may be involved with respect to a third party’s use of subcontractors. The agencies also recognize concerns by commenters interpreting the guidance to mean banking organizations are expected to assess or oversee all subcontractors of a third party. Accordingly, the agencies have revised the guidance, **focusing on a banking organization’s approach to evaluating its third party’s own processes for overseeing subcontractors and managing risks.**”

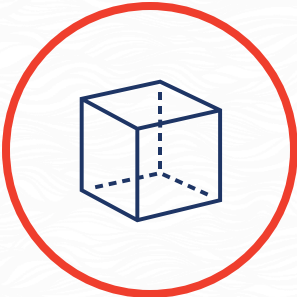
The agencies KNOW there is a lot of messiness and concern about subcontractors.

SAM's
version

But banks do NOT have to see or oversee their vendors' subcontractors.

Instead, banks need to focus on how their vendors oversee and manage their subcontractors.

SUBCONTRACTOR DUE DILIGENCE



Volume



Nature



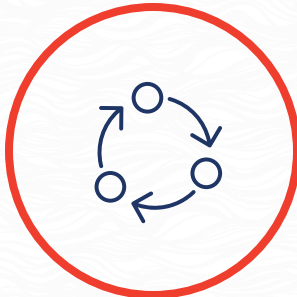
Reliance



Geography



Dependencies



Process



Not one piece of any guidance requires you to directly manage your vendors' subcontractors.

**Your third parties should be
managing their own third parties.**

Your job is to evaluate how well
you think they do that
and respond accordingly.

VENDOR CONTRACTS SHOULD INCLUDE

Notification of Subcontractor Use

Right to Audit & Remediation

Prohibit Use & Disclosure of Information

Indemnification & Liability

Third-Party Liability for Subcontractors

Prohibited Subcontractors

Prohibit Subcontracting without Consent

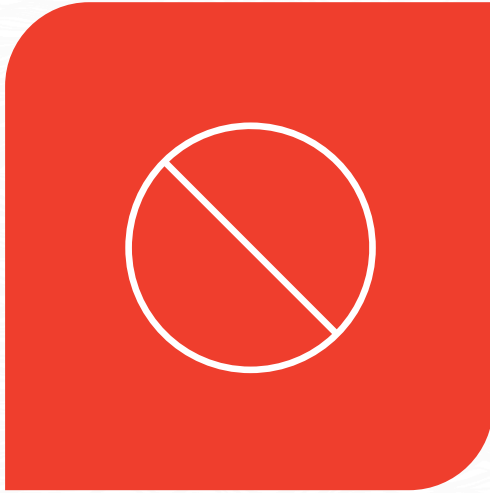
Subcontractor Performance Standards

Responsibility for Management Costs

Right to Terminate without Penalty

“We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best positioned to reduce risks for all of us.”

[White House National Cybersecurity Strategy Fact Sheet](#)



We Cannot Manage
Third Parties
Subcontractors



We Cannot Stop
Third- & Fourth-
Party Incidents



We Can Negotiate Strong
Contracts and Hold
Vendors Accountable



FFIEC Information Technology Examination Handbook

Architecture, Infrastructure, and Operations

JUNE 2021

FFIEC Information Technology Examination Handbook

Federal Financial Institutions Examination Council



3501 Fairfax Drive • Room 87081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • www.ffiec.gov

Joint Statement

Security in a Cloud Computing Environment

INTRODUCTION

The Federal Financial Institutions Examination Council (FFIEC) on behalf of its members¹ is issuing this statement to address the use of cloud computing² services and security risk management principles in the financial services sector. Financial institution management should engage in effective risk management for the safe and sound use of cloud computing services. Security breaches involving cloud computing services highlight the importance of sound security controls and management's understanding of the shared responsibilities between cloud service providers and their financial institution clients.

This statement does not contain new regulatory expectations; rather, this statement highlights examples of risk management practices for a financial institution's safe and sound use of cloud computing services and safeguards to protect customers' sensitive information from risks that pose potential consumer harm. Management should refer to the appropriate FFIEC member guidance referenced in the "Additional Resources" section of this statement for information regarding supervisory perspectives on effective information technology (IT) risk management practices. This statement also contains references to other resources, including the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Department of Homeland Security (DHS), International Organization for Standardization (ISO), Center for Internet Security (CIS), and other industry organizations (e.g., Cloud Security Alliance).

BACKGROUND

Due diligence and sound risk management practices over cloud service provider relationships help management verify that effective security, operations, and resiliency controls are in place and consistent with the financial institution's internal standards. Management should not assume that effective security and resilience controls exist simply because the technology systems are operating in a cloud computing

¹ The FFIEC comprises the principals of: the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

² NIST SP 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction.

FFIEC Joint Statement on Security in a Cloud Computing Environment

Conducting Due Diligence on Financial Technology Companies

A Guide for Community Banks

AUGUST 2021



Board of Governors of the Federal Reserve System

Federal Deposit Insurance Corporation

Office of the Comptroller of the Currency

Conducting Due Diligence On Financial Technology Companies

Supply Chain Risk Management (SCRM)

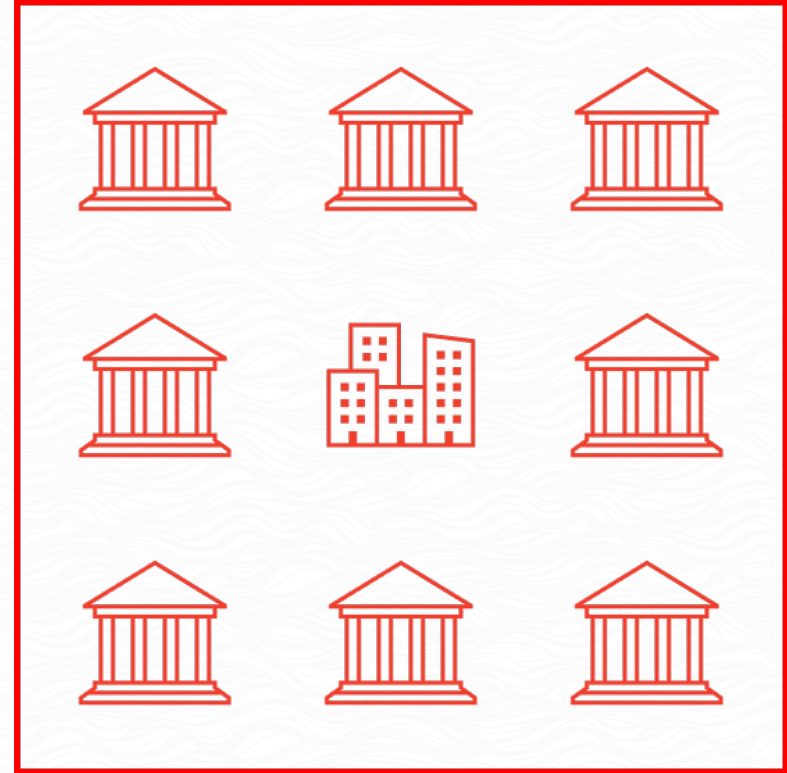
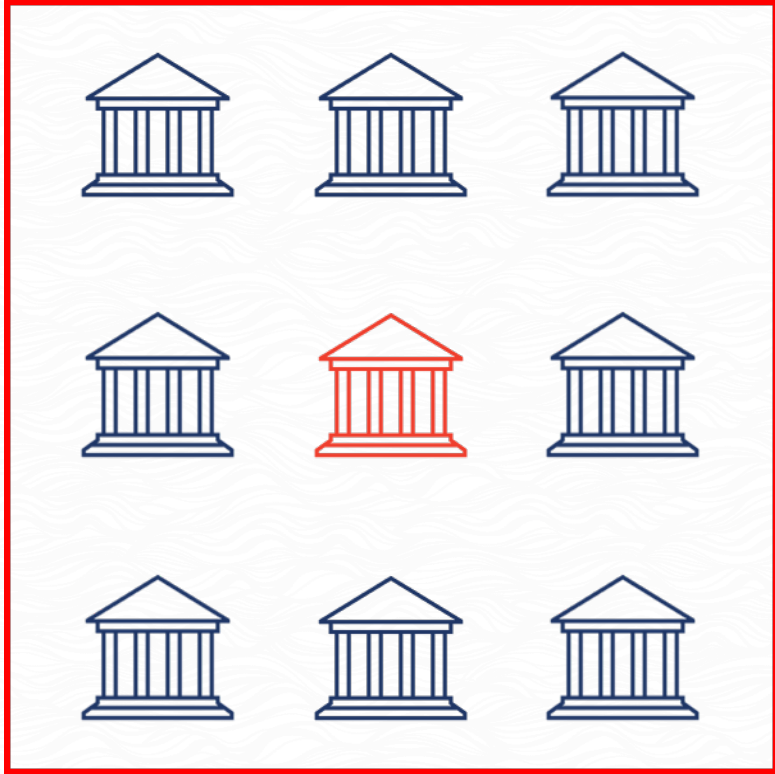


FFIEC Information Technology Examination Handbook

Development, Acquisition, and Maintenance

AUGUST 2024

How familiar are you with the concept of supply chain risk management?



“A system of organizations, people, activities, information, and resources, possibly international in scope, which provides products or services to consumers.”

“Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.”

NIST SP 800-161r1 Cybersecurity SCRM Practices for Systems and Organizations

SUPPLY CHAIN

SUBCONTRACTORS



Who They Depend On

THIRD PARTIES



Who You Depend On



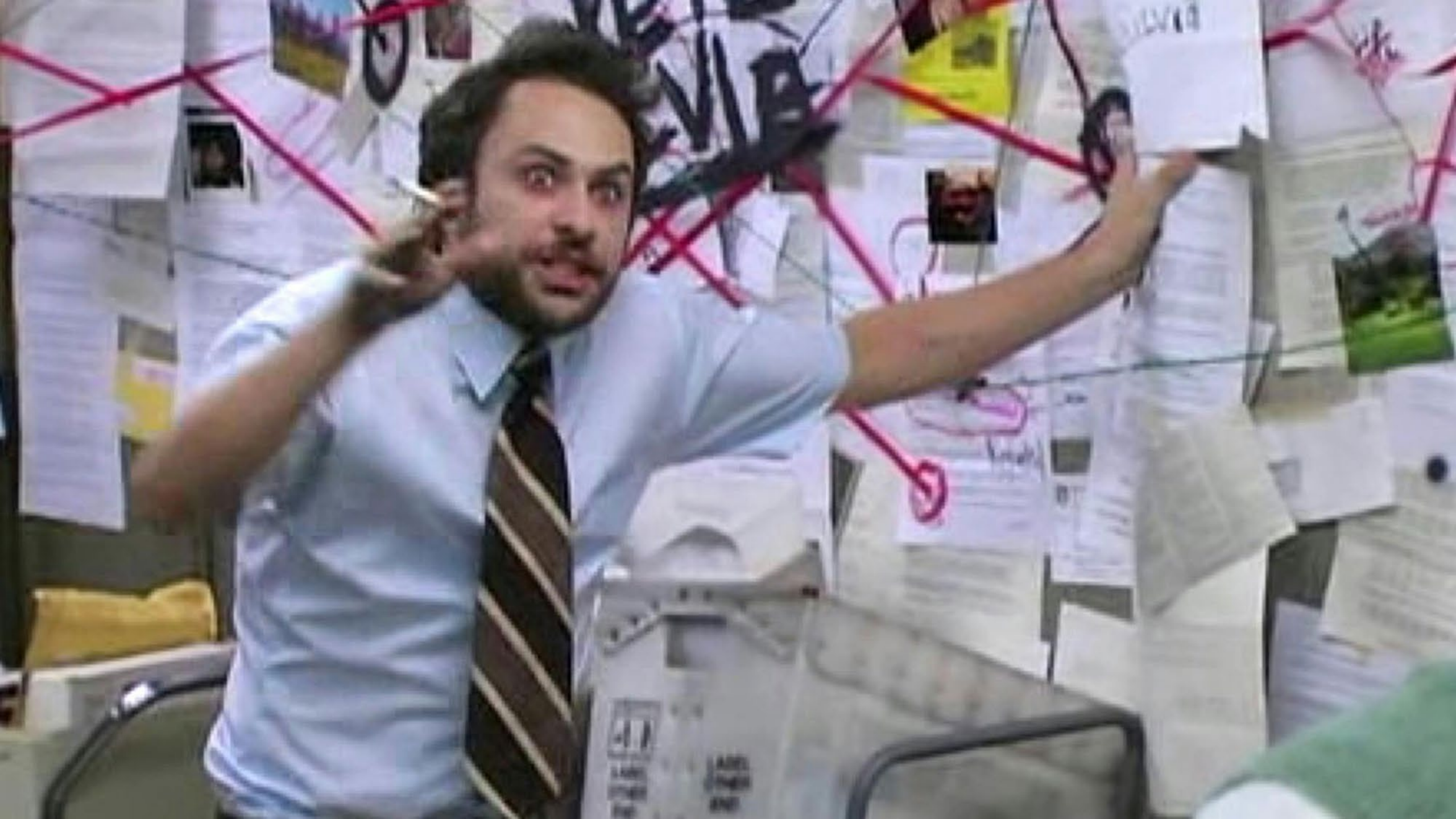
You Are Here

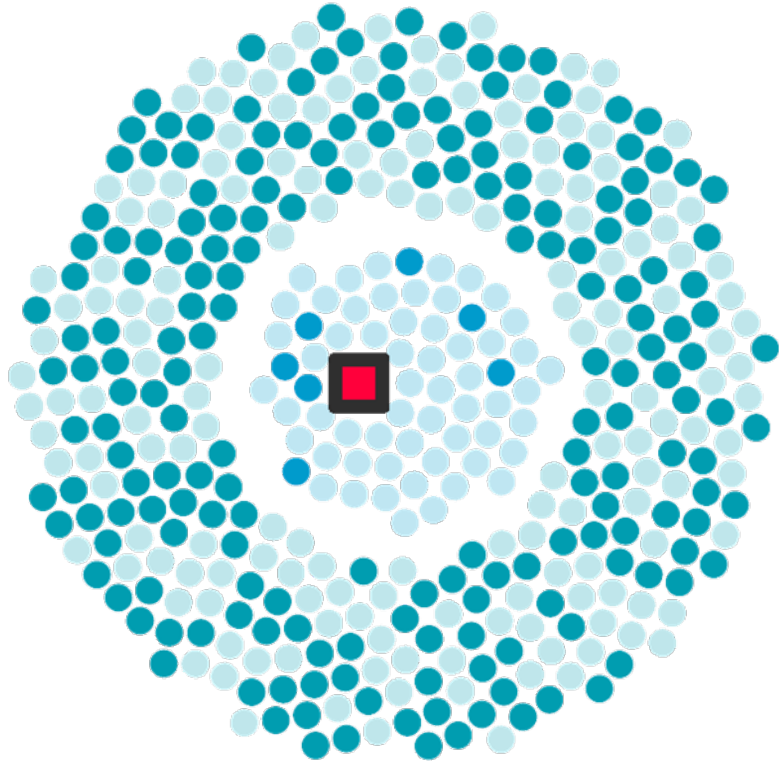
CUSTOMERS



Who Depends On You







“When a third party is relied on by multiple other 3rd parties, it is typically relied upon by nearly one-third – 29% – of those interconnected parties. Sometimes, as many as 40% of these third parties will all use the same other third party! If something goes wrong at that oft-used company, nearly half your business partners – and your company – could also suffer.”

Risk to the Nth Party Degree Report

<https://www.riskrecon.com/report-risk-to-the-nth-party-degree>

“To effectively manage supply chain risks, management should have a clear understanding of interconnectivity in the entity’s supply chain. To facilitate this understanding, management should consider using available information, such as that provided by third-party user groups and associations, which can augment ongoing monitoring and due diligence, threat intelligence, and security throughout the supply chain. A vulnerability to one system, component, or supply chain partner may pose a vulnerability to the entire supply chain.”

“The SCRM plan can be stand-alone but is often part of an entity’s information security program and third-party risk management program.”

FFIEC Development, Acquisition, and Maintenance Booklet, Section IV.Q.1 Supply Chain Risk Management



KEY TAKEAWAY

Guidance provides many recommendations for how you can effectively manage SCRM, and other risks related to third party relationships.

**SUBMIT YOUR
QUESTIONS!**

Cautions & Considerations for Subcontractors

What if there is language in the vendor contract I don't agree with?

What if I don't want my vendors working with certain subcontractors?

What authority do I have to make these types of changes with my vendors?

It's YOUR contract.

It's YOUR organization.

It's YOUR money.

YOU get to call the shots.





**IT'S MY MONEY AND
I NEED IT NOW!!!**



Bid for
contracts

2014

2014

Moving
Company
won Bid

Contract Terms Included



Moving Company will pick-up, transport, and decommission certain devices from data center.



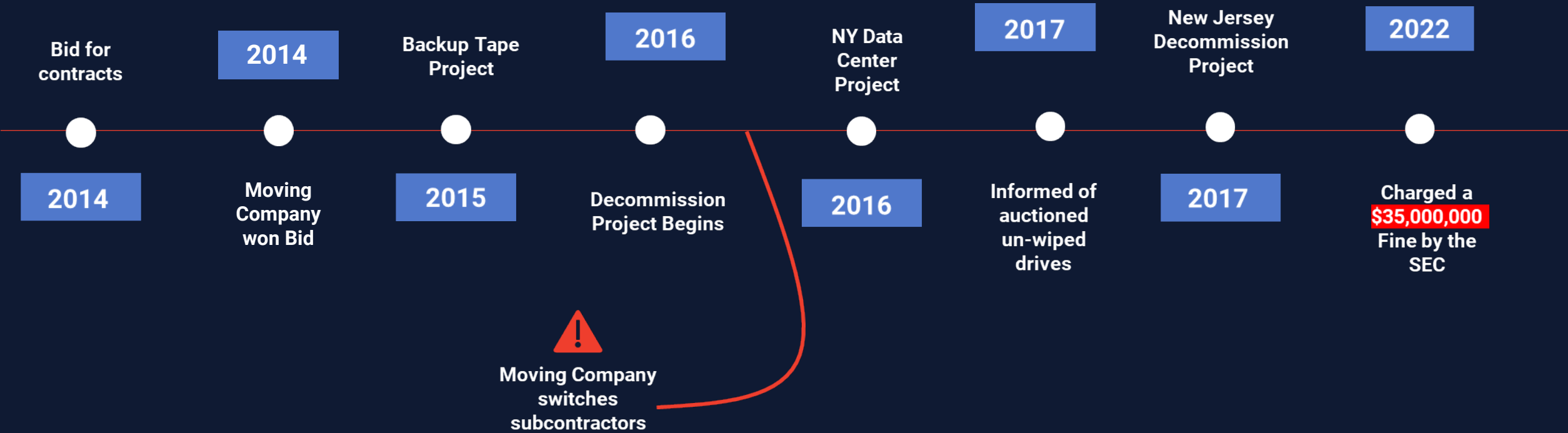
Devices will be wiped (or degaussed) by IT Corp A (subcontractor) and resold with 60-70% of the resale amount going to the bank.



Bank will receive an asset report and disposition report (inventory and whether they were returned to the bank, resold, or destroyed).



Bank will receive Certificates of Destruction (“CODs”) documenting the destruction of relevant devices.



“The vast majority of the hard drives from the 2016 Data Center Decommissioning remain missing.”

TRUST



but

VERIFY





Change Vendors



Termination
Contingency Plan



Test Your Controls



KEY TAKEAWAY

A detailed contract can mean the difference between a little more work now, or a *lot* of work down the road.

Reviewing Subcontractor Relationships

You are not reviewing the subcontractors.

You are reviewing your vendors' due diligence practices.



How much does the vendor subcontract?



What activities does the vendor subcontract?



What do the subcontractors have access to?



How reliant is the vendor on their subcontractors?



Are any of the subcontractors foreign-based?



Are subcontractors geographically dispersed?



Is the subcontractor used by several vendors?



How often does the vendor review their subcontractors?



Does the vendor do background checks?



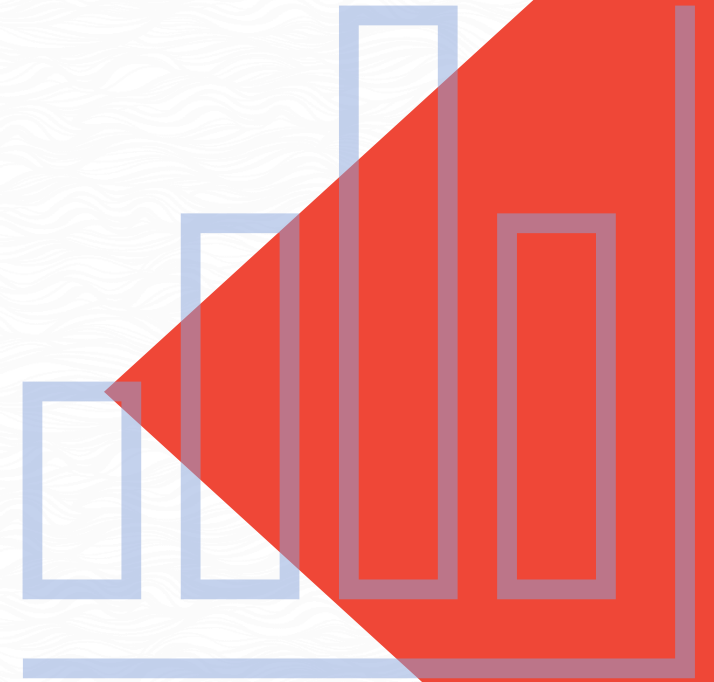
What documentation does the vendor review?



If the subcontractor is on the same infrastructure as you or your vendor, this will cause problems if that infrastructure goes down.



If the subcontractor has access to your sensitive data, this could put your organization in a compromising situation.



Third-Party Due Diligence of Subcontractors

Does the vendor use subcontractors?

What do they use them for?

How do they evaluate their subcontractors?



KEY TAKEAWAY

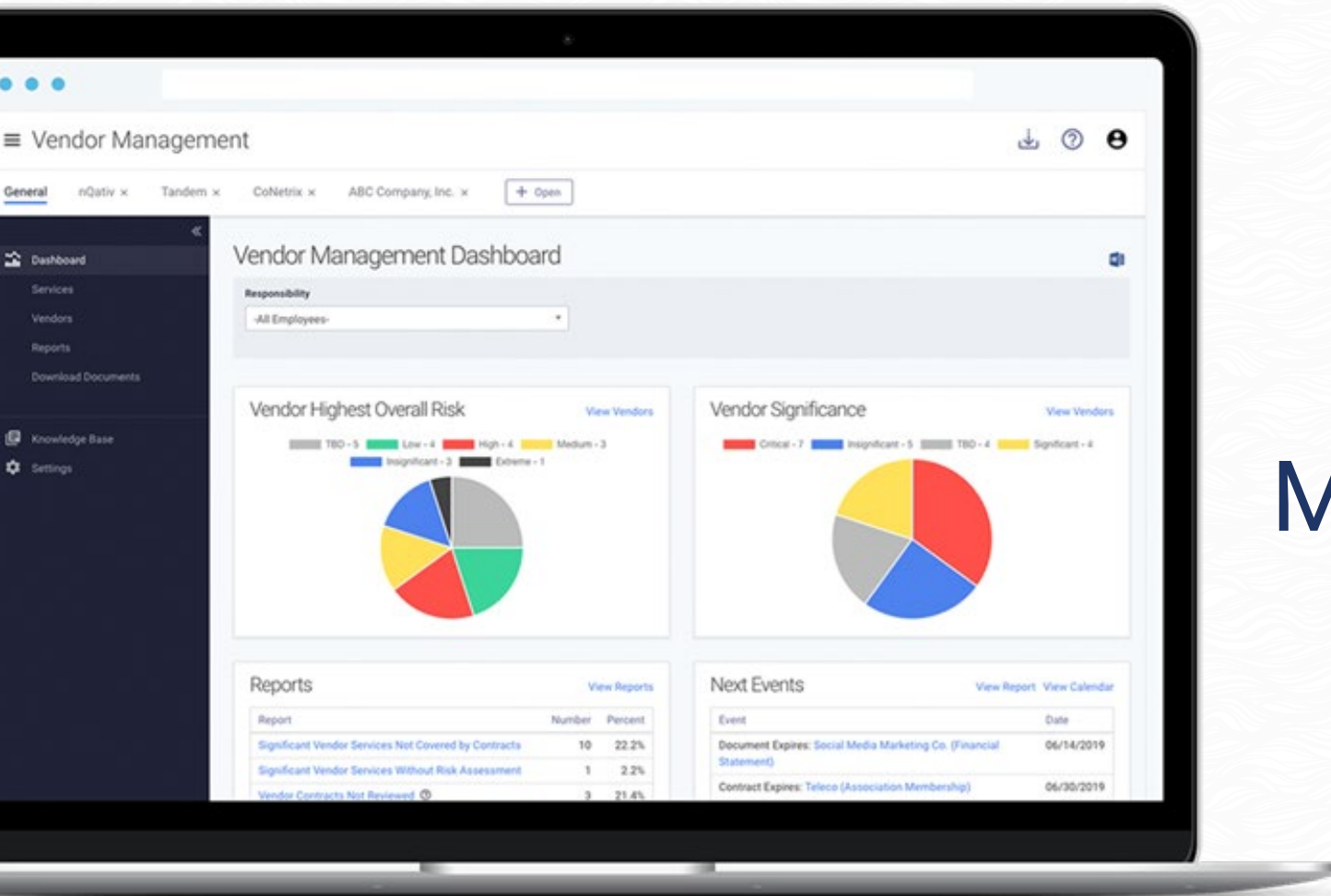
The best way you can be in the know about your vendors subcontractors is to review your own third parties closely and carefully.

Wrap Up & Bonus Content

DIGITAL VERSION

[Tandem.App/
Vendor-Management-
Workbook](https://Tandem.App/Vendor-Management-Workbook)





LEARN MORE

Tandem Vendor Management Software

Tandem.App/Vendor-Management-Software



Fill out the survey for
a chance to win!



**SUBMIT YOUR
QUESTIONS!**

THANKS FOR JOINING

Connecting the Dots: Subcontractor Relationship Management

Samantha Torrez-Hidalgo, CSXF

storrez@tandem.app

[LinkedIn.com/in/samanthatorrez](https://www.linkedin.com/in/samanthatorrez)



Remember to complete the survey!