### Connecting the Dots: Subcontractor Relationship Management

Samantha Torrez-Hidalgo, CSXF Tandem Software Specialist CoNetrix



- 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.





















Risk Assessment

Vendor Management





# 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

<u>Linkedin.com/in/SamanthaTorrez</u>



### AGENDA

Subcontractor Definition

**Identifying Subcontractors** 

BONUS CONTENT
Vendor Management
Demo & Resources



Guidance & Regulations

Cautions & Considerations for Subcontractors

Reviewing Subcontractors



### What type of organization do you work for?



### What is your organization's asset size?



## Subcontractor Definition





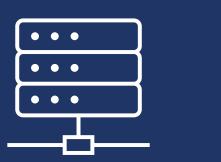




Managed Service Provider (MSP)

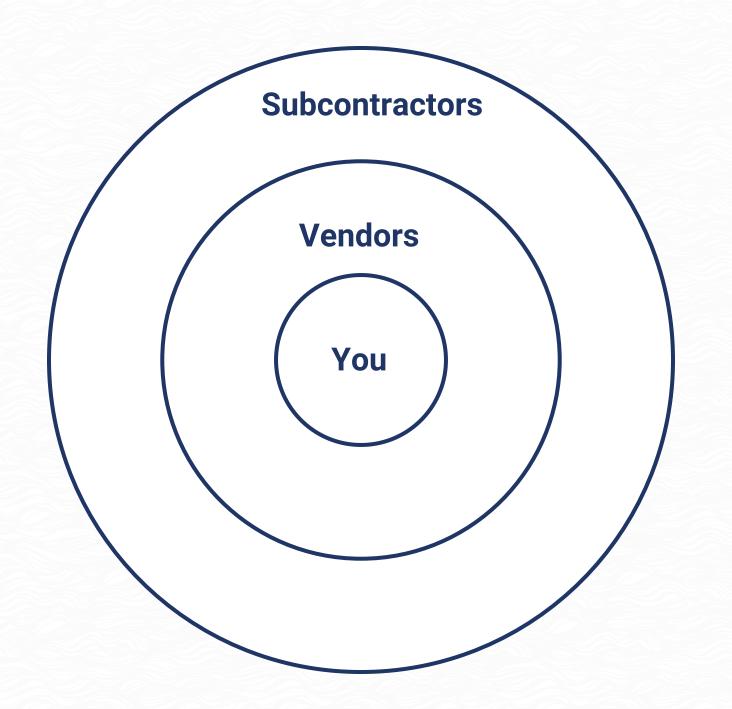
Subcontractor

Product Licenses















Do Your Research

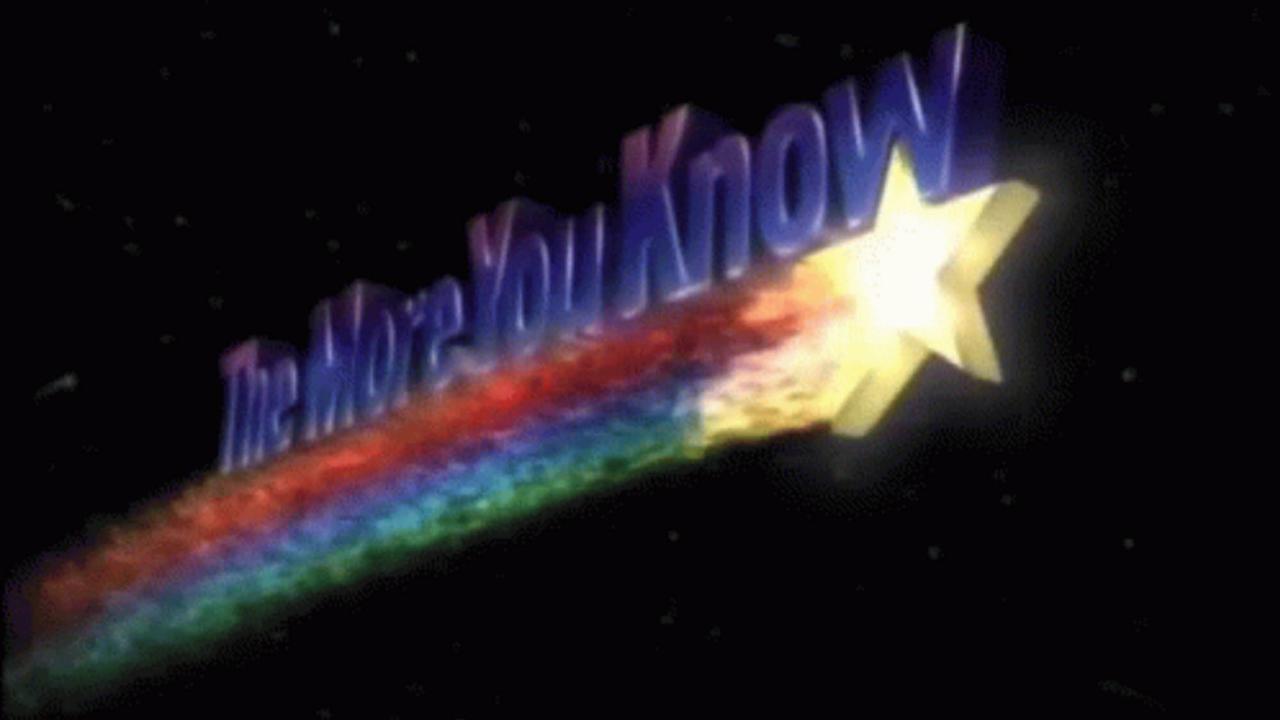


Discuss Your Options



Due Diligence Matters





### KEY TAKEAWAY

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



## Identifying Subcontractors





### IDENTIFYING & TRACKING SUBCONTRACTORS





### 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



Inefficient



**Poor Precedent** 



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.

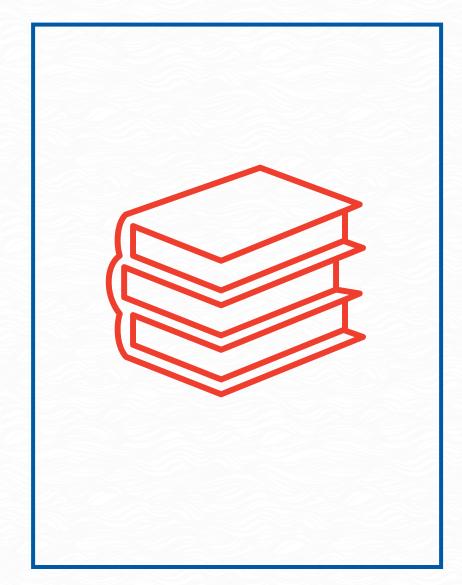
But banks do NOT have to see oversee their vendors' subcontractors.

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

### SUBCONTRACTOR DUE DILIGENCE







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

**Prohibited Subcontractors** 

Right to Audit & Remediation

Prohibit Subcontracting without Consent

Prohibit Use & Disclosure of Information

Subcontractor Performance Standards

**Indemnification & Liability** 

Responsibility for Management Costs

Third-Party Liability for Subcontractors

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 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

FFIEC Joint Statement on Security in a Cloud Computing Environment Board of Governors of the Federal Reserve System

Federal Reserve System

Federal Proposition

Office of the Compressive of the Currency

Conducting Due Diligence on Financial Technology Companies

A Guide for Community Banks

Conducting Due Diligence
On Financial Technology
Companies



### Supply Chain Risk Management (SCRM)



**FFIEC Information Technology Examination Handbook** 

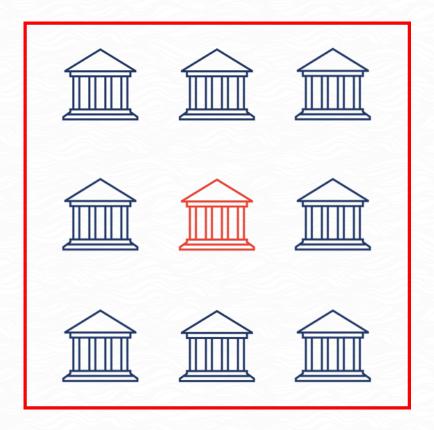
Development, Acquisition, and Maintenance

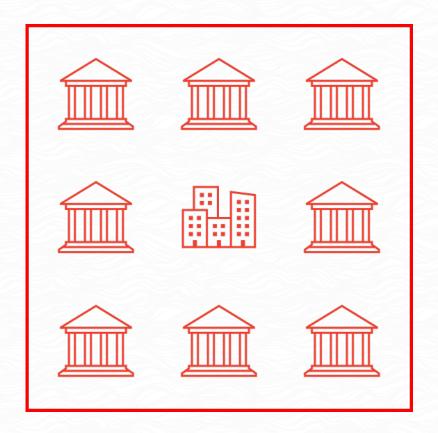
AUGUST 2024



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



**SUBCONTRACTORS** 

**THIRD PARTIES** 

**CUSTOMERS** 



Who They Depend On





Who You Depend On



You Are



Here

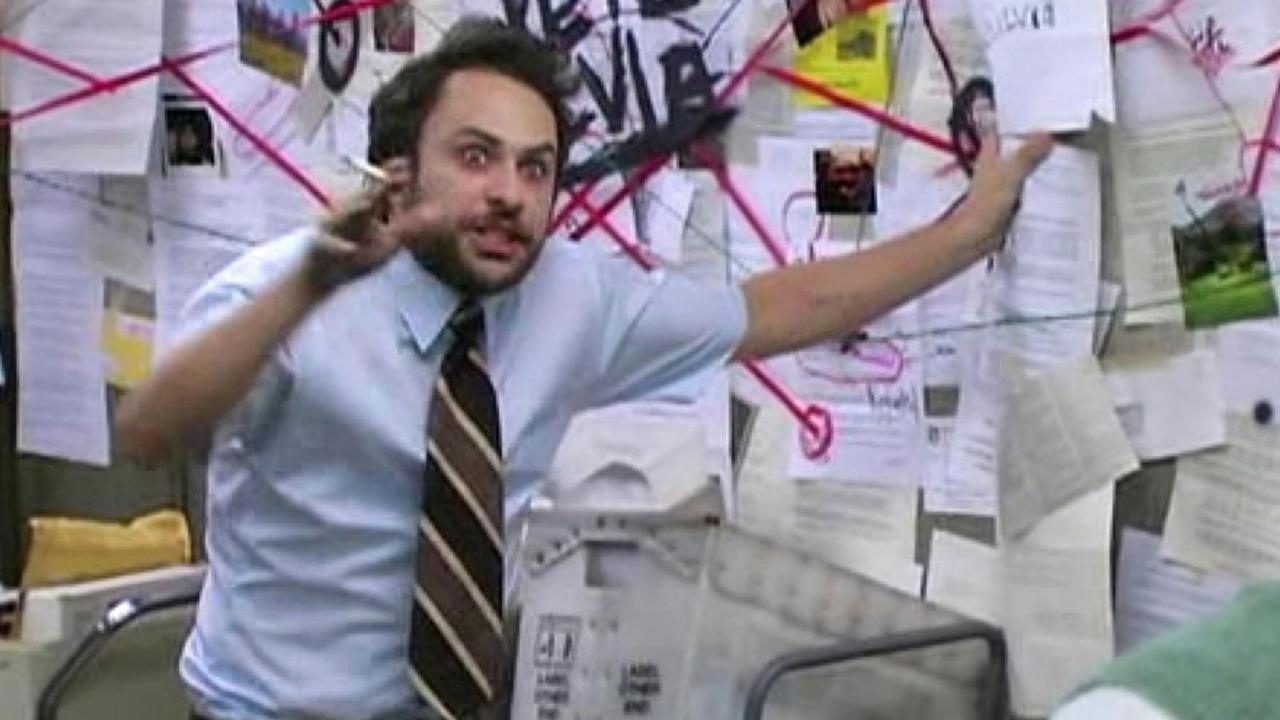




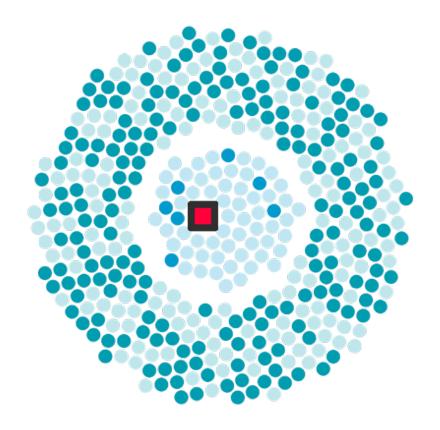


Who Depends On You





### SUPPLY CHAIN RISKS



"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."

### SUPPLY CHAIN RISK MANAGEMENT



 Verification of suppliers' claims of conformance to contractual security and compliance Validation of system or component integrity.
 Use of validation tools and techniques (e.g., scanning) for detecting malware or counterfeit goods (e.g., unauthorized systems or components sold as authentic goods). Additionally, management may use manual inspection techniques for identifying Verification of ongoing training to ensure that appropriate personnel are aware of emerging supply chain risks. Supply chain operational security is important because of the interconnectedness of numerous relationships with supply chain partners and the difficulty in coordinating multiple operational security efforts, which creates the opportunity for a potential breach. Effective nagement communicates with its supply chain partners to promote awareness of threa intelligence and relevant vulnerabilities in the entity's supply chain to inform operational security processes. In some situations, entity management may choose to withhole information from supply chain partners to prevent parties with malicious intent from using the information to compromise the native. To restart assists compromise Management should consi entity operations and asse Management should consi FFIEC IT Examination Handbook Development, Acquisition, and Maintenance may be accessible in down developed or acquired. If management considers a honeypots) beyond standar used by multiple business lines, functions, systems, and components. For example, effective nagement considers the following practices:

Determine whether there is potential foreign ownership or influence and whether the supply chain partner may have relationships with OFAC-sanctioned individuals, concealment), it should dis board, as appropriate, before additional risk to the entity organizations, or countries. Evaluate supply chain partner oversight of its subcontractors (i.e., fourth parties) or · Agreements 164 between the ent addressing common supply chair Agreements should address risks • Personnel<sup>142</sup> security contri determine how the supply chain partner demonstrates its compliance with applicable open-source licensing agreements.

Conduct research on COTS systems and components (e.g., via publicly available resources) or request proof to determine whether the supply chain partner (e.g., original the entity's supply chain. equipment manufacturer (OEMI) has performed testing as part of their quality or chain partner for systems and components not directly acquired from an OEM entity Acquire directly from vetted OEMs or their authorized distributors and resellers when obtaining alternative sources for continued support. Decisions about using alternative sources (i.e., other than OEMs or authorized resellers and servicers) should consider input from all stakeholders (e.e., business lines, IT, CISO, and compliance). <sup>100</sup> Agreements may include contracts, costs agreements. Track chain of custody of a products. Use of mechanic FFIEC IT Examination Handbook signatures, bar code scane techniques in the acquisitie throughout the entity to fac chains potentially affecting the entity. Management should plan for certain scenarios, ensuring that 179 Unplanned system or component failure and subsequent replacement Code (including mob
 Vetted system and co
 oode before installing
 Verification processe
 verify the source and Planned replacement related to feature improvements, maintenance, upgrades, and Product or service disruption (e.g., loss or degradation of data or operations). Potential supply chain disruptions affect the entity's operations (e.g., transportation issues, system and component availability problems, or financial difficulties of entiries in the supply chain). Management should consider provisions for excess capacity, bandwidth, and Audit and assurance (internal) chain, including activities to asse redundancy in agreements with supply chain partners and take appropriate mitigation steps, as necessary. For more information, refer to the FFIEC IT Handbook is "Business Continuity assurance activities may include Review of system or com as necessary. For more informat Management" booklet.

Provenance involves the chro-changes to a system or system personnel and processes used to component, or associated data. Review of processes for tr
 Use of service provider sy

minimum standards and in

150 Refer to NEST SP 800-161/1, Coherance

August 2024

components, and data, and me

risk to the entity throughout th bills of material (SBOM)<sup>138</sup> fo

purchased, open-source, and i gned using a verifiable and to formation on SBOMs, refer

Supply chain partner assess and supply chain risk manage include the supply chain infra

delivery systems) and the infe

should align with enterprise re assessment, the entity should

criticality to the business. It is criticality to the business. It is pertinent to the security, integr list), or authenticity of their su consistently evaluate supply of for which the assessment is be based on supply chain risk. Th accuracy) relied on for an asse

should document the reference

If an entity has a PMO, it can

project management processe

<sup>10</sup> NIST Glossary defines "SBOM" as a various components used in building suff assembling existing open-source and con-given] product."

10 Refer to NIST Glossey.

August 2024

FFIEC IT Examination Handbook

Development, Acquisition, and Maintenance

. Inventory is a foundational building block for supply chain management. The entity may Investory is a foundational building block for supply chain management. The entity may try to mile uplies to support in starting and operational finitions. Management should develop, document, and maintain an account an extensity of third parties that reflects the startly is key supply, document, and maintain an account an extensity of their party is created with a supply of the startly and their parties of their party is transitional level of dependency on the supplier for business function. The investory should be detailed level of dependency on the supplier for business function. The investory should be periodically closely for identifying critically and supply chain risk for tracking and exporting. The investory should be periodically reviewed and updated, including or Description of the supplied produces and services (e.g., model or software version).

Programs, projects, systems, and components that use the supplier's products and

Development, Acquisition, and Maintenance

Assigned criticality level that aligns to the criticality of the program, project, system

components or strong aflows management to tend changes made froughout the Control of the Contro is important to consider configuration management minimum security requirements from in important to consider configuration management minimum security requirements for the supply chain. Management should apply appropriate configuration management controls to its own systems and encourage or require the use of comparable controls by all parties in the entity's supply chain through contracts. For more information, refer to the FFIEC II.

entity's supply chain through controls. For more information, refer to the FFELE IT Handbook's "Budden Security" book meeting the SED Lord antiasticated throughout Resilience should be considered from the beginning the SED Lord antiasticated throughout the useful file of the system or composet. This aids in cost reduction and efficiency of implementation and included planning for alternative third-party service provides and vendors of systems, components, and evirce-marked resilience considers in alternative vendors of systems, components, and evirce-marked resilience considers in alternative delivery routes if the primary one is unavailable, especially when it applies to a critical provider. Management can improve resilience by using platform-agnostic systems and omponents that allow for portability that will improve resilience throughout the supply components that allow for pertability that will improve resultance throughout the supply classis. Having multiple that due pays source, its chartesprace; 19° in supply of systems and components one result in alternatives for availability and reduce the potential impact of a component one result in alternatives for availability and reduce the potential impact of a component one resultance of the component of the system in the component of the system in the component of any order in the component of the system in the system is the state, but the state is under a state of the system in the system in the system is the system of the system in the system in the system is the system of the component of the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the system is the system of the system in the system in the (e.g., alternative storage and processing sites and telecommunication pathways) may have their own supply chains with additional risks. Entity management should understand and mitigate all relevant risks associated with interdependencies throughout the various supply

<sup>30</sup> Heterogeneity techniques include the use of distributed storage and processing, different Ous, virtualization cellulques, and multiple sources of supply.

FFIEC IT Examination Handbook

Development, Acquisition, and Maintenance

FFIEC IT Examination Handbook

from an SCRM nerspective.

sensitivity o

for manage

o Specify info

safekeeping
 Detail infon

SCRM plan cont

implementations

plan can be stand-along but is often part of an entity's information security program and plan can be stand-abore but is often part of an entity's information security program and third-party risk management program. The plan should address supply chain risks associated with geographic location (e.g., defining acceptable locations). The entity should define roles and responsibilities for personnel (e.g., development, acquisition, and maintenance) to address various roks associated with supply chain activities.

address various risks associated with supply shins neitwires.

\*General centrals and processes are bossed on the SCRAD plan and entity risk assessments.

\*Management analyzes the risks and designs controls to mitigate risks to an acceptable level as officionly longity senior management and the board. To protect confidentiality, integrity, integrity, integrity of the control of the senior of

Appropriate protections in the information systems, components, and networks for data in transit and at rest for the supply

testing data, blueprints, and intells
Tamper-resistance and detection of
Appropriate logging, disparate da usage pattern reports, and time of

Appropriately segregated and iso (e.g., development, testing, and pr

Controls over the use of security IT environments. o Logical and physical access contr

potential for insider threats as ent

Formal process for assigning ide systems and components (e.g., dij throughout the supply chain. o Provisions for physical and logic

controls in the entity's agreement Appropriate monitoring tools and

systems and supply chain partner

111 Refer to FTC 16 CFR 314, "Standards for Safes products or services and is unable to provide them, should be considered. Conversely, too many suppli-and integrity or quality of service may be compron-

15 Criticality analysis can help determine which on

Aurost 2024

arous an obscut proporties.

Address system and component supply chain traceability.

Specify supply chain due diligence for new vendoes, third-party service provides, and ongoing supply chain monitoring. The initial assessment should occur during the initiation phase of a project, before new products or services are provided, or new

Instruct staff on how to choose hardware, software, and third-party service providers

Management should monitor, control, and protect communications (i.e., information tra

or received) applicable to supply chain-related activities at key access points (e.g., external boundaries and key internal boundaries). Effective management uses architectural designs,

software development techniques, and systems engineering principles to promote effective

information security in the supply chain by identifying and mitigating potential SCRM-related

An attempt should be made to identify potential single points of failure among all entities in the entity's supply chain due to the numerous interconnectivities and risks from all partners. Review of documents, such as system and network topologies and process flow diagrams, may help with identification of three single points of failure.

NIST identifies SCRM high-level controls in various documents. <sup>152</sup> Management should consider the following controls in all development, acquisition, and maintenance activities.

SCRM policies, standards, and procedures that

 Align with other internal and external policies, standards, and procedures (e.g., information security and business continuity management).

FFIEC IT Examination Handbook Development, Acquisition, and Maintenance or intellectual property (e.g., customer data and logos), and malware inserted into authentic

Development, Acquisition, and Maintenance

the Trosson's Office of Foreign Assets Control (OFAC) Sanctions Lad or located in countries that are on the list. Management should ensure that the entity's supply chain partners are not the OFAC list. "If This may include evaluating the third party's ownership structure (including identifying any beneficial ownership whether public or private, foreign or domentic). <sup>149</sup> To accurately determine whether a third party is on the list or affiliated with companies on the list, it is important to consider any nested relationships through common ownership or any subsidiary or affiliate relationships. It is important to understand risks related to supply chains by tracking terdependencies between all parties involved (e.g., owners and third-party service provider including vendors) in the supply chain.

Supply chain risks increase when supply chain partners are unstable financially or during times of economic, cyber, or logistical disruption to the operations and continuity of key supply chain elements. <sup>100</sup> Theo partners include third parties and their supply chain partners (also referend to as fourth parties). Some supply chain attackers use indirect paths and trusted relationships to gain access to the entity for disruptive purposes, financial gain, or to obtain intelligence. Attackers often exploit a third-party service provider's supply chain to access multiple other victim businesses (i. e. the service provider's customers) for subsequent attacks.

#### IV.Q.1 Supply Chain Risk Management

SCRM is the systematic process for managing supply chain risk by identifying susceptibilities, Sexion is not systematic process or managing upply cann risk by socially mig susceptivations, vulnerabilities, and factor throughout the supply chin and developing militarion strategies to combat flower flowers whether presented by the supplier, the supplier's product and its subcomponents, or the supply chine (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). <sup>112</sup> SCRM builds on traditional acquisition and procurements practice by adding processes to identify, nearure, monitor, and control risks procurement practices or yauding personance to security, measure, monitoring, and control reass. throughout the supply chain. SCMM processes provide entity management with information to help supplement third-party risk management activities (e.g., due diligence and contract supplement of systems or components by presenting all elements in the supply

<sup>400</sup> Par the U.S. Department of the Transary's Office of Toroga Assuts Canton's UOFAC's "Basic Information (MAC on Section", "U.S. persons must comply with GFA cognitions, including all U.S. citizes and GFAC on Section (Including all U.S. citizes and the United State Office and entities within the United State Office and entities within the United State Constitution (Including Consti 140 Refer to Interagency Guidance on Third-Party Relationships: Risk Management.

18 Refer to NIST IR 8419, Blockchain and Related Technologies to Support Manufacturing Supply Chain

10 Refer to NIST Glossary.



# "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.

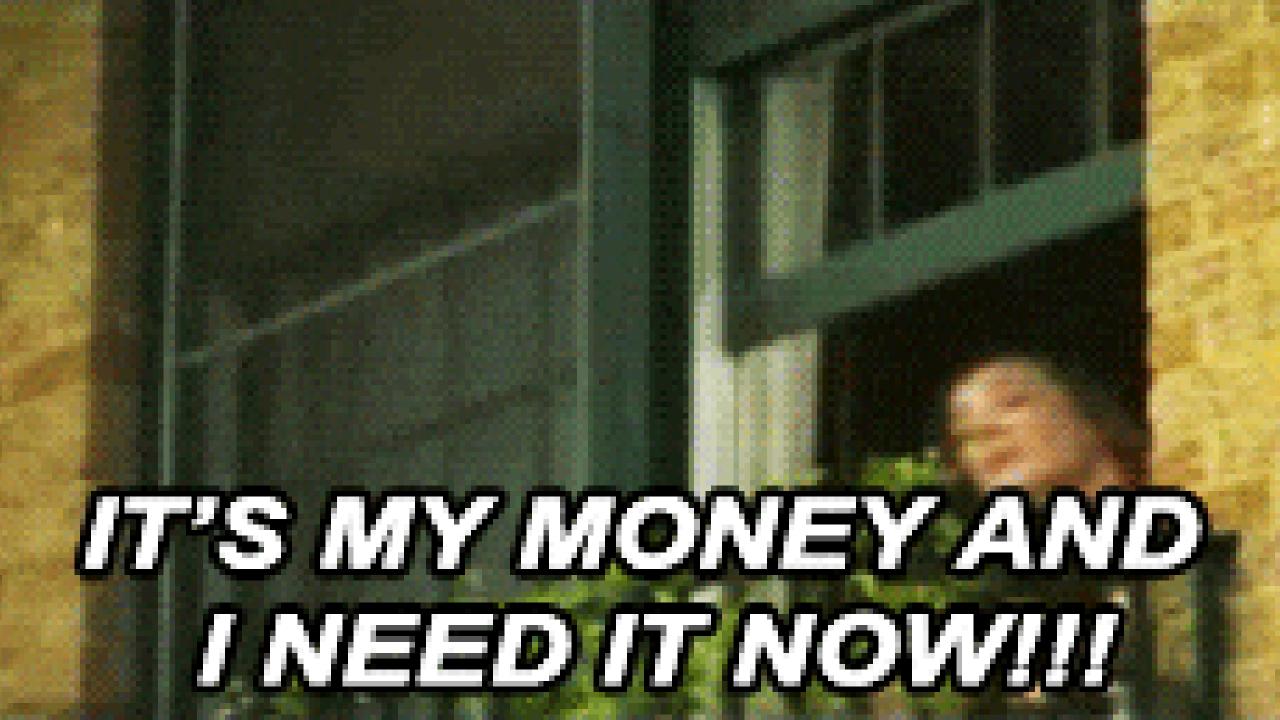
It's YOUR organization.

It's YOUR money.

YOU get to call the shots.









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.



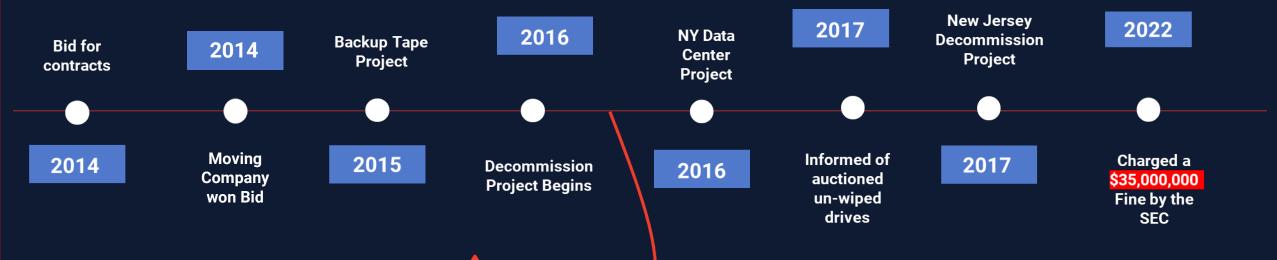
Bank will receive an asset report and disposition report (inventory and whether they were returned to the bank, resold, or destroyed).



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







Moving Company switches subcontractors

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



## **TRUST**



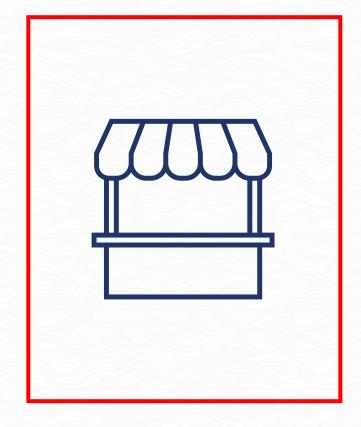








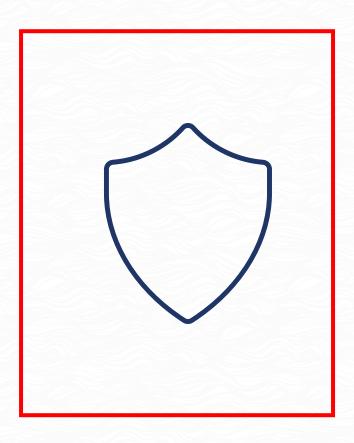
### CONTRACT ISSUES



**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?

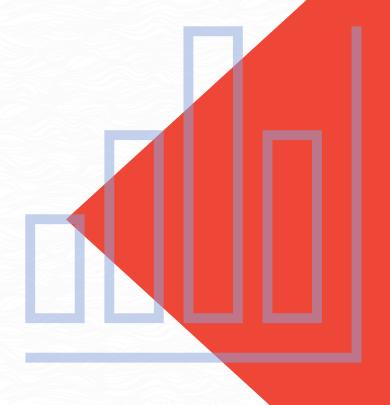


If the subcontractor is on the same infrastructure as you or your vendor, this will cause problems if that infrastructure goes down.





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





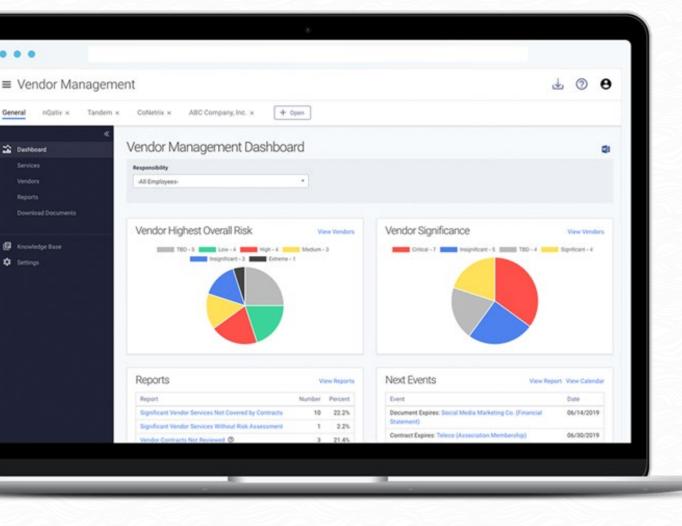
### DIGITAL VERSION

## Tandem.App/ Vendor-ManagementWorkbook









#### LEARN MORE

## Tandem Vendor Management Software

Tandem.App/Vendor-Management-Software























## Fill out the survey for a chance to win!





# SUBMIT YOUR QUESTIONS!



## Connecting the Dots: Subcontractor Relationship Management

Samantha Torrez-Hidalgo, CSXF

storrez@tandem.app

LinkedIn.com/in/samanthatorrez



Remember to complete the survey!

