



# Vendor Management Workbook

# About the Author



**Alyssa Pugh**, CISM, Security+  
GRC Content Manager  
Tandem, LLC  
[LinkedIn.com/in/AlyssaPugh](https://www.linkedin.com/in/AlyssaPugh)

Meet Alyssa, a content creator with a passion for helping people navigate the challenges of governance, risk management, and compliance (GRC). With more than ten years of professional technical and graphic design experience, she's on a mission to inspire others to level up their cybersecurity and third-party risk management practices, one vendor at a time.

## Contributors

**Leticia Saiid**, Security+  
Chief of Staff, Chief Learning Officer  
CoNetrix, LLC

**Savannah Richardson**, ITRF  
Software Specialist  
Tandem, LLC

**Missy Oliver**, CRVPM II  
Information Security & Compliance Consultant  
CoNetrix Security, LLC

**Brian Whipple**  
Marketing Director  
CoNetrix, LLC

## Why We Wrote This Book

Over the years, we have received feedback from customers that vendor management is one of their top pain points. This workbook was written from a desire to help guide vendor managers through the process in a way that is equally effective and efficient. Many of the concepts in this book are implemented in our vendor management software. While the concepts in the book are great, they are made much better when used in Tandem.

If you do not currently subscribe to Tandem Vendor Management, we encourage you to check it out at [Tandem.App](#) or watch a demo at [Tandem.App/Vendor-Management-Overview](#).

### Disclaimer

This resource is for information purposes only. Businesses may use this resource to assist with their third-party risk management practices, but are encouraged to evaluate the risks and coordinate with appropriate legal counsel before acting on ideas from this document.

# Contents

## 4 Introduction

- 5 Why Vendor Management?
- 5 Regulations & Guidance
- 6 Vendors vs. Third Parties
- 7 Governance & Structure

## 8 Planning

- 9 Risk Assessment

## 10 Due Diligence

- 12 Business Profile
- 14 Certificate of Insurance
- 16 Business Continuity Plan
- 18 SOC Report
- 20 Security Testing Reports
- 22 Financial Statement
- 26 Subcontractors
- 28 Frequently Asked Questions (FAQs)

## 30 Contract Management

- 32 Contract Review
- 34 Nondisclosure Agreement (NDA)
- 35 Service Level Agreement (SLA)
- 36 Frequently Asked Questions (FAQs)

## 38 Monitoring

## 40 Termination

## 42 Report to the Board

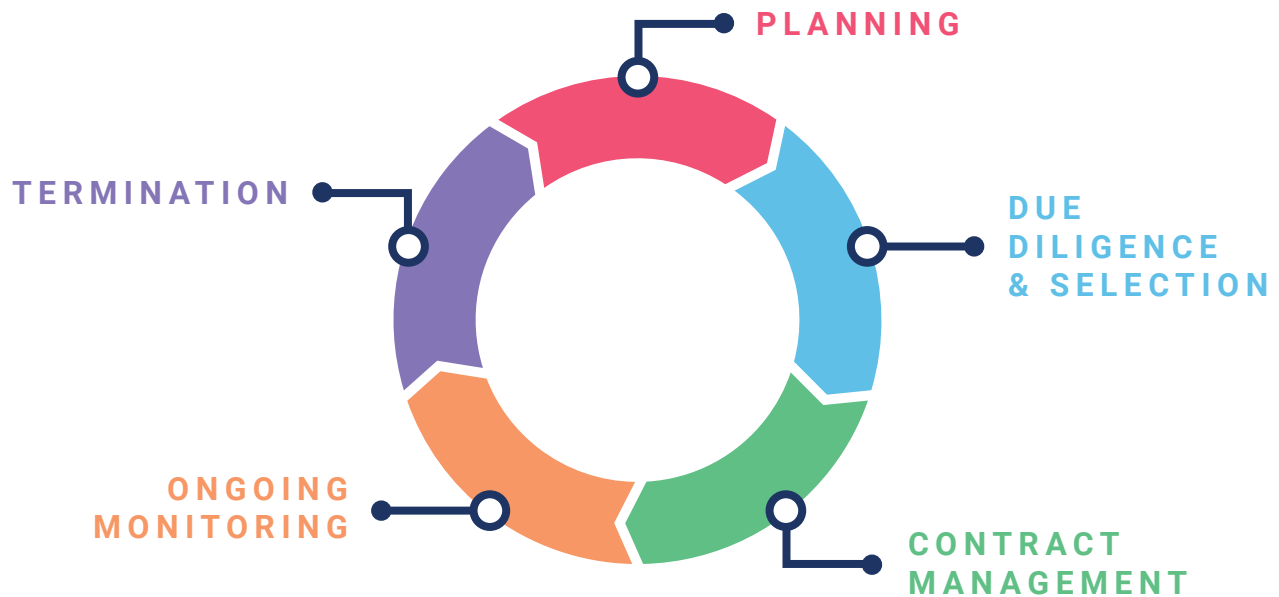
## 44 Conclusion

- 45 Further Reading
- 47 About Tandem



# Introduction

Vendor management is about managing the risks associated with third-party service provider relationships. The vendor management lifecycle is comprised of five phases, including Planning, Due Diligence & Selection, Contract Management, Ongoing Monitoring, and Termination.



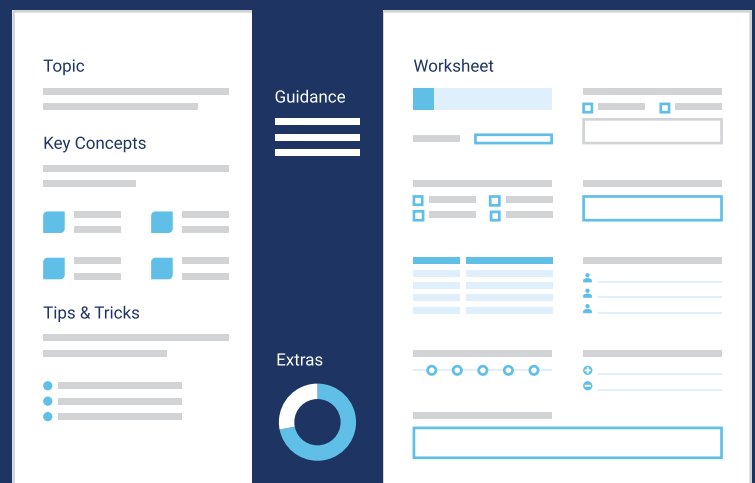
## Workbook Instructions

Use this workbook to discover and apply the fundamentals of vendor management.

Each topic will feature educational content, alongside an interactive worksheet. Use the checkboxes and text fields to answer a series of questions. Then, use the information you learn to help you make informed decisions about the vendor.

As you apply the things you learn in this workbook to your vendor management practices, keep in mind: The goal is not knowing everything about a vendor. **The goal is managing risk.**

Download a digital version of the workbook now at [Tandem.App/Vendor-Management-Workbook](https://Tandem.App/Vendor-Management-Workbook).



# Why Vendor Management?

While vendor management can often be seen as an expense and a compliance task, having an effective vendor management program can be a powerful asset to your business. If you are looking to justify your vendor management program, when done correctly, here are a few of the results you can expect to see.

- Risk Mitigation**  
Vendor management helps identify and mitigate potential risks that could cause harm to your business.
- Cost Efficiency**  
Vendor management helps businesses negotiate favorable terms, optimize costs, and streamline procurement.
- Strategic Alignment**  
Vendor management helps align vendor capabilities with strategic goals, driving innovation and success.
- Relationship Building**  
Vendor management helps build strong relationships by fostering trust, collaboration, and communication with third parties.
- Operational Continuity**  
Vendor management helps proactively address issues, prevent operational disruptions, and minimize downtime.
- Information Security**  
Vendor management helps protect the company and its customers/members from potential breaches or misuse.
- Scalability & Growth**  
Vendor management helps the business know when services can be scaled up or down based on business needs.
- Innovation & Expertise**  
Vendor management helps provide the business with access to external expertise, technology, and innovations.

## Regulations & Guidance

While having a vendor management program can benefit any business, for financial institutions, it is also a requirement. Here are a few of the regulatory building blocks when it comes to vendor management.

### 1962

The **Bank Service Company Act** (BSCA) was published. This act gave the FDIC, OCC, and FRB regulatory authority over vendors who provided specific types of services to banks.

### 2001

The **Interagency Guidelines Establishing Information Security Standards** (GLBA) required the oversight of vendors with access to customer/member information.

### 2004

The FFIEC's **Outsourcing Technology Services IT Examination Handbook** published guidance on what it looks like to manage technology service providers (TSPs).

### 2007

The NCUA published **Supervisory Letter (SL) 07-01** which instructed credit unions to take specific steps when evaluating third-party relationships.

### 2023

The FDIC, OCC, and FRB published **Interagency Guidance on Third-Party Relationships: Risk Management** which details the vendor management lifecycle.

For additional vendor management regulations, guidance, and resources, see the Further Reading section (Page 45).

# Vendors vs. Third Parties

There are several terms often used interchangeably to describe a business arrangement with an external entity. For this document, we'll be using the terms as follows.

## Third Party

Any business arrangement between a business and another entity, by contract or otherwise.

## Vendor

A subset of a third party, including entities with whom the business has a contract or conducts commerce.

## Third-Party Service Provider

A subset of vendors who provide outsourced services to the business.

While it is a best practice to have an inventory of all third-party relationships, the term "vendors" most accurately describes the relationships which need heightened attention due to the nature of the activities they perform.

For example, here are some third-party relationships you should track, but would likely **not** need to manage as vendors.



Regulators



Utility Providers



Emergency Services



Government Agencies



Law Enforcement



Local Media

That said, here are some examples of vendors you **should** include in your vendor management program.



Outsourced Services



Payment Processors



Consultants



Joint Ventures



Referral Arrangements



FinTechs



## DID YOU KNOW?

Have you ever wondered why the term "third party" is sometimes hyphenated? There's a reason for that!

"Third party" should only have a hyphen when the term is being used as a modifier for another word.

For example, if you are talking about "a third party" or "the third party," the words would not be hyphenated.

However, if you are talking about something like a "third-party relationship," "third-party service provider," or "third-party user," then you would want to add a hyphen.

Behold, the magic of grammar!



# Governance & Structure

A vendor management program is ultimately governed by your business' Board of Directors and senior management.



## Board Responsibilities

It is the Board's responsibility to:

1. Communicate if vendor relationships are aligned with the business' strategic goals and risk appetite.
2. Designate resources for the appropriate oversight of vendors.
3. Hold management accountable for the status of the vendor management program.



## Management Responsibilities

It is management's responsibility to:

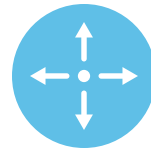
1. Implement a vendor management program that covers each of the elements defined in this book.
2. Report program status periodically and escalate issues to the Board.
3. Make sure the risk associated with vendor relationships is adequately identified and controlled.

Responsibility of a vendor management program can be centralized or decentralized. The flexibility can be freeing, but it can also leave a lot of questions about who does what. Here are some pros and cons of each structure.



## Centralized

Centralized vendor management provides greater efficiency, control, and consistency over the process. However, it can result in communication challenges, as the people managing the vendors are not the direct users or beneficiaries of the relationship.



## Decentralized

Decentralized vendor management promotes accountability and empowers the people directly connected to the vendors. However, it can result in a lack of clarity, inconsistent results, duplication of efforts for shared vendors, and reporting challenges.

As a vendor manager, your job is to carry out the strategy of the Board and senior management by overseeing these outsourced relationships. Your business has freedom to determine how the program is structured. Whatever structure you choose, expectations and responsibility need to be clearly communicated.

## BY THE NUMBERS

We asked more than 300 vendor managers about how their program was structured. Here's what they said:

- Centralized: Managed by Compliance/Risk Management (37%)
- Centralized: Managed by Information Security (32%)
- Centralized: Managed by Its Own Department (16%)
- Decentralized: Managed by Business Lines (11%)
- Centralized: Managed by Procurement (4%)

### SOURCE

Tandem Survey, August 2023 (n=305)



# Planning

Choosing the right vendor takes work. Planning is the process of evaluating how to manage risks before entering into a relationship. Next time you're thinking about outsourcing a new service, ask and answer these questions.

## Worksheet

### 01. Why do you need a vendor for this activity?

### 02. Who might be impacted by this relationship?

- |  |  |
|--|--|
| <input type="checkbox"/> Employees         | <input type="checkbox"/> Other Vendors |
| <input type="checkbox"/> Customers/Members | <input type="checkbox"/> Others _____  |

### 03. How much do you estimate this will cost?

### 04. What physical (P) or technical (T) access will the vendor need?

- | P                        | T                        |                                   |
|--------------------------|--------------------------|-----------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | Proprietary business data         |
| <input type="checkbox"/> | <input type="checkbox"/> | Confidential customer/member data |
| <input type="checkbox"/> | <input type="checkbox"/> | Unclassified data                 |
| <input type="checkbox"/> | <input type="checkbox"/> | Critical business systems         |
| <input type="checkbox"/> | <input type="checkbox"/> | Non-critical business systems     |
| <input type="checkbox"/> | <input type="checkbox"/> | Facilities                        |
| <input type="checkbox"/> | <input type="checkbox"/> | Other _____                       |

### 05. Who is responsible for this vendor?

- |   |                  |
|---|------------------|
|  | Selection _____  |
|  | Approval _____   |
|  | Management _____ |

## GUIDANCE

“As part of sound risk management, effective planning allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship. Certain third parties, such as those that support a banking organization’s higher-risk activities, including critical activities, typically warrant a greater degree of planning and consideration.”

*Interagency Guidance on Third-Party Relationships: Risk Management*



# Risk Assessment

## GUIDANCE

“Credit unions should complete a risk assessment prior to engaging in a third party relationship to assess what internal changes, if any, will be required to safely and soundly participate. Risk assessments are a dynamic process, rather than a static process, and should be an on-going part of a broader risk management strategy.”

*NCUA Supervisory Letter 07-01*

“[P]eriodically 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*





A vendor risk assessment is a process to evaluate the risk you take on by being in a relationship with a vendor. You may not know certain risks exist until you begin the due diligence and contract management process. As you know more, return and update the risk assessment.

## Worksheet

### 01. What risks are associated with the vendor relationship?

*While some risks are going to exist regardless of the vendor relationship, there are some risks which will be dependent on the nature of the relationship. For example:*

- *If the vendor has big financial obligations, you’d want to assess the credit risk.*
- *If the vendor uses subcontractors, you’d want to assess the subcontractor risk.*
- *If the vendor is foreign-based, you’d want to assess the country risk.*

	 High	 Medium	 Low	 N/A
Strategic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Operational	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reputation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Compliance/Legal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 02. How do you plan to manage the risks of the relationship?

*The risk management plan is going to be specific to the relationship. For example:*

- *If the vendor is a “high” legal risk, spend more time negotiating the contract.*
- *If the vendor is a “high” financial risk, review financial statements more often.*
- *If the vendor is a “high” operational risk, implement some technical controls.*

Perform more frequent reviews

Negotiate stronger contract requirements

Implement compensating controls

Other \_\_\_\_\_

# Due Diligence

Due diligence is about making sure a vendor is a good choice. The process often involves requesting evidence from vendors to validate things like security, resilience, and financial stability.

While there isn't a one-size-fits-all formula for due diligence, here are some examples of things many businesses look at as part of the process.

- ✓ Business Profile
- ✓ Certificate of Insurance
- ✓ Business Continuity Plan (BCP)
- ✓ SOC Report
- ✓ Security Testing Report(s)
- ✓ Financial Statement
- ✓ Vendor Management Program Summary



There may be other types of due diligence you may need to perform, but those are often specific to the nature of the engagement (e.g., cloud service providers, financial technology (FinTech) companies, software developers, vendors who interact with customers/members, etc.).

## Performing Due Diligence

So, how can you perform due diligence for your vendor? Plain and simple: Start by asking! While you may need independent verification for some things, for others, you just need answers.

Here are some common methods to do that.

-  Email
-  Automated Software Tools
-  Phone Calls & Virtual Meetings
-  Web Searches & References

Vendors are people, too. Ask for what you need *clearly* and *concisely*. The simpler you make it for them to respond, the more likely you'll get the response you need.

## GUIDANCE

"Due diligence should serve as a verification and analysis tool, providing assurance that the service provider meets the institution's needs."




*FFIEC Outsourcing Technology Services Booklet*

## BY THE NUMBERS

Using vendor management program as a decision making tool is becoming a more common practice. Due diligence is a big part of that.

How the vendor management program is used:



-  It is a decision driver (65%)
-  It is a guideline (22%)
-  It is for compliance (13%)

## SOURCE

Tandem Survey, October 2023 (n=288)

## GUIDANCE

“Conducting due diligence on third parties before selecting and entering into third-party relationships is an important part of sound risk management. It provides management with the information needed about potential third parties to determine if a relationship would help achieve a banking organization’s strategic and financial goals. The due diligence process also provides the banking organization with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship. Due diligence includes assessing the third party’s ability to: perform the activity as expected, adhere to a banking organization’s policies related to the activity, comply with all applicable laws and regulations, and conduct the activity in a safe and sound manner.”

*Interagency Guidance on Third-Party Relationships: Risk Management*

## The If/Then Method

So, how do you know what due diligence analysis is required for a vendor? We recommend using the “if/then method.” It works like this:

IF	the vendor does a specific function,
THEN	you should do certain types of due diligence.

On the next several pages, there will be specific examples of the if/then method for each of the due diligence types listed on the previous page.

“Conducting due diligence on third parties before selecting and entering into third-party relationships is an important part of sound risk management.”

## The Question Behind the Question

It can be tempting to think due diligence is all about *gathering* documents. While that is certainly part of the job, making it just about documents misses the bigger picture.

Good due diligence is about the question behind the question.

- You don’t ask for a SOC report to get a SOC report.  
You ask for a SOC report to know if the vendor is secure.
- You don’t ask for a financial statement to get a financial statement.  
You ask for a financial statement to know if the vendor is stable.
- You don’t ask for a BCP to get a BCP.  
You ask for a BCP to know if the vendor is resilient.
- You don’t ask for a document to get a document.  
You ask for a document to know if the vendor is capable.

Treating the due diligence process as an administrative function is a compliance mindset. Analyzing, learning from, and reporting on due diligence documents is a risk management mindset.

**Bottom Line:** A compliance mindset checks the boxes, but it is hollow. If you manage vendors with a focus on understanding and managing risk, you’ll benefit your business and probably be in compliance, too.



# Business Profile

## DUE DILIGENCE

**IF** the vendor is going to provide services to you,

**THEN** ensure they are qualified.

A business profile is a listing of basic information about the vendor. It typically includes things like:



Location &  
Contact  
Information



Business  
Experience



Staffing  
Qualifications



Compliance  
Requirements

**Bottom Line:** You should know who you're getting into business with and if they have the skills to pay the bills.

Here are some tips and tricks for completing a business profile.

### Use All Available Resources

Web searches, social media, review sites, and the vendor's own website can be very helpful sources of information.

### Check the OFAC Sanctions List

This list shows people and businesses prohibited from doing business in the U.S. <https://sanctionssearch.ofac.treas.gov>

### Request a Form W-9 from All Vendors

A W-9 shows the Taxpayer Identification Number (TIN) and can be used as proof of the vendor's existence. Two-for-one!

### The Key is Validating Legitimacy

Remember that vendors want to impress you. Looking at external sources provides an independent voice.

### But... When in Doubt, Ask the Vendor

It never hurts to ask questions. This is especially true while the vendor is still trying to win your business.

## GUIDANCE

"Due diligence should confirm and assess the following information regarding the service provider:

Existence and corporate history;

Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate; [...]

Strategy and reputation;

Service delivery capability, status, and effectiveness; [...]

Legal and regulatory compliance including any complaints, litigation, or regulatory actions."

*FFIEC Outsourcing Technology Services Booklet*

## PRO TIP

Some vendors are expected to comply with certain laws, regulations, guidance, and frameworks, just like you.

For example, if GLBA requires you to protect proprietary customer/member data, then vendors who handle your proprietary customer/member data must also comply with GLBA requirements.

When completing a business profile, document the vendor's compliance categories to keep tabs on compliance expectations.

# Business Profile Worksheet

## DUE DILIGENCE



### DOCUMENT REQUEST

Form W-9

01. List the vendor's names, including any DBA.

02. List the vendor's website(s).

03. List the vendor's physical address.

04. Does the vendor have any foreign locations?

- Yes       N/A  
 No       Unknown

05. How long has the vendor been in business?

06. What is the vendor's organization type?

- Corporation  
 Limited Liability Company (LLC)  
 Limited Liability Partnership (LLP)  
 Sole Proprietor  
 Other \_\_\_\_\_

07. What is the vendor's ownership structure?

- Public       Foreign  
 Private       Domestic

08. How many employees does the vendor have?

09. Does the vendor perform background checks?

- Yes       N/A  
 No       Unknown

10. Describe the vendor's qualifications.

11. Is a succession plan in place for key personnel?

- Yes       N/A  
 No       Unknown

12. What are the vendor's compliance categories?

- BSCA       ISO/IEC  
 FISMA       NIST  
 GDPR       PCI-DSS  
 GLBA       SOX  
 HIPAA       Other \_\_\_\_\_

13. Is the vendor on the OFAC sanctions list?

- Yes       N/A  
 No       Unknown

14. Does the vendor have any other legal issues?

15. Rate the vendor's reputation. ☆☆☆☆☆

# Certificate of Insurance

## DUE DILIGENCE

**IF** the vendor is going to provide services to you,

**THEN** ensure they have insurance to withstand common losses.

A certificate of insurance (COI) outlines the types and amounts of insurance coverage carried by the vendor. Here's a rundown of the most common types of insurance and when you might need to request them.

**1 General Liability**  
Every vendor should have general liability insurance. This protects the vendor from losses related to bad things that happen in the course of business (e.g., bodily injury, property damage, etc.).

**2 Workers' Compensation**  
Every vendor should have workers' compensation insurance. This protects the vendor from losses related to expenses which must be paid to an employee who gets injured on the job.

**3 Errors & Omissions (E&O)**  
Vendors who provide consulting services should have E&O insurance. This protects the vendor from losses related to claims of inadequate work, mistakes, negligence, or malpractice.

**4 Cyber Liability**  
Vendors who provide technology services should have cyber insurance. This protects the vendor from losses related to cyber incidents (e.g., data breaches, malicious attacks, etc.).

**5 Umbrella Liability**  
Vendors who pose a significant risk to your business should have umbrella liability insurance. This protects the vendor when issues occur that are beyond or outside of other insurance coverages.

### How Much is Enough?

There is no specific dollar amount that is objectively "satisfactory." We suggest working with financial and legal professionals to determine if the vendor has enough to be stable in the event of adverse circumstances.

### A Good Place to Start

For common insurance types, the following limits are considered "standard" for a small to medium business, although risk factors may cause a vendor to need different coverage levels (e.g., size, location, type of operations, client needs, industry changes, etc.).

Occurrence Limit	Aggregate Limit
\$1 million	\$1 million to \$3 million

## GUIDANCE

"An evaluation of whether the third party has existing insurance coverage helps a banking organization determine the extent to which potential losses are mitigated, including losses posed by the third party to the banking organization or that might prevent the third party from fulfilling its obligations to the banking organization."

*Interagency Guidance on Third-Party Relationships: Risk Management*

## FUN FACT

In addition to the common insurance types, here are a few others you might see in the wild.

- Automobile Liability
- Commercial Property
- Directors & Officers (D&O)
- Employment Practices Liability (EPL)
- Fiduciary Liability
- Financial Institution Bonds
- Fidelity Bonds
- Intellectual Property (IP)

## DID YOU KNOW?

The **Occurrence Limit** is the amount the insurance company will pay for a single claim.

The **Aggregate Limit** is the maximum amount the insurance company will pay on all claims during the policy period.

# Insurance Worksheet

## DUE DILIGENCE



### DOCUMENT REQUEST

Certificate of Insurance (COI)

#### 01. Certificate of Insurance Date

The date at the top of the COI helps you know if the insurance is current.

#### 02. What is the name of the insurance company?

This is important to know in case you needed to contact the company for claims purposes.

#### 03. Is your business "Additional Insured?"

Being "additional insured" means your business is insured through the vendor's policy and may file claims on it.

- Yes       N/A  
 No       Unknown

#### 04. Did your business waive rights of subrogation?

Waiving rights of subrogation means your business relinquished its legal right to compensation from the vendor's insurer. This may or may not be listed on the certificate of insurance and may be addressed in the vendor contract.

- Yes       N/A  
 No       Unknown

#### 05. Is your business a "Certificate Holder?"

Being "certificate holder" means you got the COI from the insurance company directly. While certificate holders cannot file claims on insurance, it can keep you informed of coverage changes.

- Yes       N/A  
 No       Unknown

#### 06. What coverages are listed on the COI?

- General Liability  
 Workers' Compensation  
 Errors & Omissions (E&O)  
 Cyber Liability  
 Umbrella Liability  
 Other \_\_\_\_\_  
 Other \_\_\_\_\_  
 Other \_\_\_\_\_  
 Other \_\_\_\_\_

#### 07. Are the coverage dates current?

Look for each policy's effective and expiration dates. Make sure the dates are currently effective.

- Yes       N/A  
 No       Unknown

#### 08. Are the coverage levels satisfactory?

While there is no specific dollar amount that would be objectively "satisfactory," the goal is to make sure that the vendor has enough insurance to remain financially stable in the event of adverse circumstances.

- Yes       N/A  
 No       Unknown

#### 09. Were there any changes from the prior COI?

Insurance should be stable and continuous. However, a vendor may change coverage in response to changing risks. Do not presume previous coverages were automatically renewed.

- Yes       N/A  
 No       Unknown

# Business Continuity

## DUE DILIGENCE

**IF** a vendor service outage could impact your business,

**THEN** ensure they have plans that promote resilience.

A business continuity plan (BCP) is a comprehensive plan to maintain or resume business in the event of a disruption. This includes things like:



### Written Plan

A documented plan for detecting and responding to adverse events (e.g., natural disasters, cyber attacks, pandemics, etc.).



### Review & Approval

A process to ensure the program is updated and approved at least annually. This shows top-level support and involvement.



### Exercises & Tests

A method for verification through the performance of exercises and tests. Plans work best when they are practiced.



### Service Level Agreements (SLA)

A clearly defined response time and recourse for unmet requirements. SLAs protect your business.

**Bottom Line:** When you have a vendor, your wagon is hitched to theirs. Make sure they can handle the bad stuff, so you aren't left hanging.

Not sure where to start? Here are three tips.

**1**

#### Tip #1: Get a summary instead of the full document.

BCPs can be big. You likely don't need the full plan and even if you got it, you probably don't have the time or brain power to know it inside-and-out anyway. Summaries are friends.

**2**

#### Tip #2: Compare the SLAs with your own plan.

Recovery objectives (RTOs and RPOs) need to meet your needs. For example, if a vendor's SLA is 48 hours, but you need the service in 12 hours, some negotiations are in order.

**3**

#### Tip #3: Look for the key controls.

There can be a lot of fluff in a BCP. You need to look for the key controls, like good backup hygiene, redundant communications infrastructure, an incident response plan (IRP), and the like.

If you aren't certain about something, ask the vendor. When it comes to resilience planning, ignorance is not bliss.

## GUIDANCE

"Many entities depend on third-party service providers to perform or support critical operations. A disruption in the delivery of those services can have a direct impact on entities' resilience. A critical failure at a widely used third-party service provider could have large-scale consequences. Management should assess critical third-party service providers' susceptibility to multiple event scenarios and verify such third parties' resilience capabilities. [...] Resilience planning should be closely coordinated with third-party service providers."

*FFIEC Business Continuity Management Booklet*

## DID YOU KNOW?

SLAs are both a due diligence factor and a part of contract management. For more information about SLAs, see the Contracts section (Page 35).



# Business Continuity Worksheet

## DUE DILIGENCE



### DOCUMENT REQUEST

Business Continuity Plan Summary

01. BCP Approval Date

02. Does the vendor have a formal BCP?

- Yes       N/A  
 No       Unknown

03. What are the vendor's SLAs?

04. Do the SLAs align with your expectations?

- Yes       N/A  
 No       Unknown

05. What resilience controls are in place?

- Data Backup
- Data Integrity Controls
- Redundant Communication Providers
- Layered Anti-Malware Controls
- Disaster Recovery Plan (DRP)
- Incident Response Plan (IRP)
- Prearranged Forensic Services
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_
- Other \_\_\_\_\_

06. Describe the vendor's alternate location(s).

*Vendors should have alternate operating location(s) (e.g., hot sites, warm sites, cold sites, etc.) where service could continue in the event the primary location becomes unavailable. They should be an appropriate distance from the primary location, so each location would not be affected by the same disaster.*

07. Most Recent Exercise/Test Date

08. How often does the vendor do exercises/tests?



09. Do you perform exercises with the vendor?

- Yes       N/A  
 No       Unknown

10. What scenarios are included in the exercises?

- Disruption for the vendor
- Disruption for your business
- Simultaneous attack on vendor and business
- Cyber events
- Stress testing (i.e., working at peak volumes)

11. Could any recent exercise results impact you?

- Yes       N/A  
 No       Unknown

# SOC Report

## DUE DILIGENCE

<b>IF</b>	the vendor stores information for you,
<b>THEN</b>	ensure their security is verified.

A SOC Report provides an independent attestation of a business' control environment. There are multiple flavors of SOC Reports. Here's an introduction to the terminology you might hear.

GUIDELINE		
<b>SSAE 18</b> The guideline that defines how SOC audits are performed.		
REPORT		
<b>SOC 1</b> Internal Controls Over Financial Reporting (ICFR)	<b>SOC 2</b> Trust Services Criteria	<b>SOC 3</b> Trust Services Criteria with no testing details
TYPE		
<b>TYPE 1</b> At a single point in time	<b>TYPE 2</b> Over a period of time	

In general, here are some guidelines for when you should request each kind of SOC Report.

- 1 A SOC 1 is pretty standard and is adequate if the vendor is not storing customer confidential data.
- 2 A SOC 2 is more comprehensive and should be requested if the vendor is storing customer confidential data.
- 3 A SOC 3 is primarily used for marketing purposes. Another SOC would be better for decision-making.

Generally speaking, a Type 2 is always better than a Type 1. Anything can look good for a day. If it looks good every day, that's how you know it's a winner.

## GUIDANCE

"Determine whether management documented and implemented, as appropriate, the following resilience measures for third-party service providers: [...] Reviewed third-party service provider's resilience capabilities, including available test and SOC reports."

*FFIEC Business Continuity Management Booklet*

"When relevant and available, a banking organization may consider reviewing System and Organization Control (SOC) reports and any conformity assessment or certification by independent third parties related to relevant domestic or international standards. In such cases, the banking organization may also consider whether the scope and the results of the SOC reports, certifications, or assessments are relevant to the activity to be performed or suggest that additional scrutiny of the third party or any of its contractors may be appropriate."

*Interagency Guidance on Third-Party Relationships: Risk Management*

## DID YOU KNOW?

The term "SOC Report" is an abbreviated title for "Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting."

# SOC Report Worksheet

## DUE DILIGENCE

**DOCUMENT REQUEST**  
SOC Report

### 01. SOC Report Date

See the "Auditor's Report" section beneath the auditor's signature.

### 02. What is the SOC Report number and type?

See the report's cover page. If it is not shown on the cover page:

- It is a SOC 2 report if the term "Trust Service" is used.
- It is a Type 2 report if a section for "Test Results" is included.

- |                                |                                 |
|--------------------------------|---------------------------------|
| <input type="checkbox"/> SOC 1 | <input type="checkbox"/> Type 1 |
| <input type="checkbox"/> SOC 2 | <input type="checkbox"/> Type 2 |
| <input type="checkbox"/> SOC 3 |                                 |

### 03. What was the testing period?

See the "Auditor's Report" section, "Scope" subsection.

Type 1 will have a single date and Type 2 will have a time period.

### 04. Are significant events noted?

See the "Auditor's Report" section, "Scope" subsection.

A "significant event" is anything that happened during or after the audit that could have affected testing or reporting, such as incidents and/or material changes to the controls.

- Yes (Explain in Comments)  No

### 05. Are complementary user entity controls noted?

See the "Auditor's Report" section, "Scope" subsection.

A CUEC is a control the vendor expects you to implement. See the "Description of Controls" (or similar) section for details. Make a list of the controls and note how you have implemented each.

- Yes (Explain in Comments)  No

### 06. Are subservice organizations noted?

See the "Auditor's Report" section, "Scope" subsection.

A "subservice organization" is a vendor used by the vendor to provide the service to you. See the "Management's Assertion" (or similar) section for details.

- Yes (Explain in Comments)  No

### 07. Were any limitations noted?

See the "Auditor's Report" section, "Limitations" subsection.

A "limitation" is anything that could limit the ability for the auditor to document or test a control, such as an area that could not be assessed at the time. See the "Limitations" section for details.

- Yes (Explain in Comments)  No

### 08. What was the auditor's opinion?

See the "Auditor's Report" section, "Opinion" subsection.

The auditor's opinion should assert that the service organization's controls are (1) described fairly, (2) designed effectively, and (for Type 2 reports) (3) operating effectively over a specified period of time. This wording is standardized in all SOC Reports.

If significant exceptions are identified in the "Opinion" subsection, document them. See the "Management's Assertion" (or similar) section for details.

- Unqualified (i.e., no concerns)
- Qualified (i.e., significant concerns)
- No opinion due to limitations

### 09. Type 2: Were any control weaknesses noted?

See the "Test Results" (or similar) section. The final table column, "Results," will most commonly display "No exceptions found." If other results exist, the exception is considered a weakness for the control.

- Yes (Explain in Comments)  No

# Security Testing Reports

## DUE DILIGENCE

<b>IF</b>	the vendor transmits or processes proprietary data,
<b>THEN</b>	ensure their security is tested.

Testing is performed to validate a vendor's controls operate securely and effectively. There are four common types of security testing a vendor may have performed for their organization.



**Audits** involve a detailed review of processes and/or systems to confirm accuracy and compliance.



**Penetration tests** subject systems to real-world attacks to identify flaws in processes and controls.



**Vulnerability assessments** identify things like weak credentials, unpatched systems, or misconfigurations.



**Self-assessments** benchmark control maturity and help the vendor develop a growth plan.

**Bottom Line:** Reviewing a vendor's testing results can provide the validation you need that the vendor's controls are in tip-top shape.

### About Findings

A "finding" is a written description of a weakness or failure discovered during security testing and often indicates security deficiencies in the vendor's environment. Each finding should be:

- 1 Accounted For**  
Keeping track of findings that appear again and again can give you an idea of how the vendor views and manages security.
- 2 Assessed**  
A finding that negatively impacts the vendor could harm your business, too. Evaluate the risk of each finding.
- 3 Addressed**  
Not only should the vendor respond to each finding, you should create a plan, as well. What can you do to protect your business from these unresolved, potentially impactful issues?

## GUIDANCE

"Financial institutions are required to effectively manage their relationships with key [Technology Service Providers]. Institution management meets this requirement related to audit controls by:

Directly auditing the TSP's operations and controls;

Employing the services of external auditors to evaluate the TSP's operations and controls;

Receiving from, and reviewing sufficiently detailed independent audit reports on the TSP."

*FFIEC Audit Booklet*

## DID YOU KNOW?

A SOC Report is a form of security testing. We recommend looking at SOC Reports separately from other security testing reports, due to the SOC Report's standardized nature and widespread use.

# Security Testing Report Worksheet

## DUE DILIGENCE

**DOCUMENT REQUEST**  
Security Testing Report

### 01. Testing Date

Look to see if the testing was performed in the last 12 months. Knowing the testing date can give you an idea of if the data is accurate or if it may be outdated.

### 02. What type of security testing was performed?

- Audit
- Penetration Test
- Vulnerability Assessment
- Self-Assessment

### 03. How often does the vendor do this testing?



### 04. Was testing done by an independent party?

Independence is not always required or feasible, but it can provide credibility to the testing results.

- Yes
- No
- N/A
- Unknown

### 05. Was the scope adequate?

The purpose of this question is to determine whether testing was performed for the areas which matter most to your interests, as a client. Areas to consider could include assets, systems, processes, and/or data used to provide services to you.

- Yes
- No
- N/A
- Unknown

### 06. Were any findings identified in the testing?

- Yes (Explain in Comments)
- No

### 07. Were any findings “repeat findings?”

If a finding appears in more than one security testing report, it is important to understand the vendor’s reasoning for not addressing the finding and/or the vendor’s plans to fix it.

- Yes (Explain in Comments)
- No

### 08. Has the vendor responded to each finding?

The vendor should have either a justification or a plan to remediate each finding.

- Yes (Explain in Comments)
- No

### 09. What do you need to do about the findings?

- Nothing (e.g., there were no findings, the vendor addressed the issues, etc.)
- Limit the risk (e.g., revoke vendor access, perform heightened monitoring, etc.)
- Remediate the issue (e.g., install an update, implement a new system, etc.)

### 10. What risk do the unresolved findings present?

- High
- Medium
- Low
- N/A

# Financial Statement

## DUE DILIGENCE

**IF** the vendor going out of business could impact you,

**THEN** ensure the vendor is financially stable.

A financial statement is a record of the financial activities and status of a vendor. Broadly speaking, there are three types of financial statements.

**1**

### Audited Financial Statements

Publicly-traded companies are required to submit audited financial statements to the SEC. These reports are called “Form 10-K (Annual report)” and can be accessed online at <https://sec.gov/edgar/search>.

**2**

### Unaudited Financial Statements

These statements often look virtually identical to audited financial statements. The difference is that these statements were not independently verified by an external auditor. These statements are often provided by privately-owned vendors.

**3**

### Financial Stability Reports

Privately-owned vendors are not required to disclose financial statements and may elect to provide other information to demonstrate long-term growth and stability.

**Bottom Line:** The purpose of reviewing financial statements is to ensure the vendor will be financially stable for the foreseeable future. Any one of these documents can help you know if that’s what you can expect.

There are four parts of a financial statement.



### Balance Sheet

This shows what the vendor has (assets), what the vendor owes (liabilities) and investments (equity).



### Income Statement

This shows how the vendor makes money (revenue) and how the vendor spends money (expenses).



### Cash Flows Statement

This shows the vendor’s cash inflows and outflows, which helps showcase financial flexibility and overall health.



### Notes to the Financial Statements

The notes clarify and explain anything else going on that might impact the vendor’s financial stability.

## GUIDANCE

“Due diligence should confirm and assess the following information regarding the service provider: [...] Financial status, including reviews of audited financial statements.”

“Institutions should have on-going monitoring of the financial condition of their provider(s). To fulfill its fiduciary responsibility, an institution involved in an outsourcing arrangement should determine the financial viability of its provider(s) on an annual basis. However, if the financial condition of the provider is declining or unstable, more frequent financial reviews are warranted.”

*FFIEC Outsourcing Technology Services Booklet*

## PRO TIP

It’s dangerous to go alone! Take this: Ask someone with financial knowledge to help review your vendors’ financial statements, like a CFO or an accountant. They know what to look for and can probably do it in record time, too.

# Financial Statement: Key Terminology

## DUE DILIGENCE

### Balance Sheet

#### Liquid Assets

Liquid assets are a subset of current assets. Liquid assets typically include cash, accounts receivable, and short-term investments. Liquid assets does not include inventory (as it can be difficult to sell) or prepaid expenses (as they cannot be recovered in cash).

#### Current Assets

Current assets include all liquid assets, plus items like inventory and prepaid expenses.

#### Total Assets

Total assets include all of the vendor's assets, both current and long-term (e.g., land, equipment, properties, long-term investments, trademarks, etc.).

#### Current Liabilities

Current liabilities include debts or obligations due within one year (e.g., short-term debt, accounts payable, accrued liabilities, bills, interest payments, etc.).

#### Total Liabilities

Total liabilities include all of the vendor's liabilities, both current and long-term.

#### Total Equity

Total equity, also known as "Net Assets" or "Total Shareholders Equity," represents the overall value of the company that would remain for shareholders after all of the company's assets were sold and its debts were repaid.

### Balance Sheet Ratios

#### Working Ratio

The Working Ratio (a.k.a., Current Ratio) is used to determine if a vendor's current assets are enough to support the vendor's current liabilities.

#### Quick Ratio

The Quick Ratio (a.k.a., Acid Ratio, Liquid Ratio, or Liquidity Ratio) is used to determine if a vendor can pay their debts in the near future with only their liquid assets.

#### Debt to Equity Ratio

The Debt to Equity ratio is used to determine if the vendor has the resources to take care of its obligations.

### Income Statement

#### Income Statement

The Income Statement (a.k.a., "Profit and Loss Statement," "Statement of Revenue and Expense," or "Statement of Earnings") shows how the vendor makes money (revenues) and spends money (expenses).

#### Revenue

Revenue (a.k.a., "Net Sales") is the cash a vendor receives through selling products or providing services. Revenue can indicate whether the business has the ability to sell its products or services. However, revenue does not necessarily mean the business is profitable, as expenses may outweigh the revenue or revenue sources may be inconsistent.

#### Expenses

Expenses (a.k.a., "Cost of Revenue" or "Cost of Sales") represent the amount it costs to produce a product or perform a service.

#### Interest Expense

Interest expense is the cost a vendor pays for the debt they have acquired. Interest expense can influence a vendor's financial stability. As the economy changes, so could interest on outstanding debt.

#### Gross Income

Gross income (a.k.a., "Net Income") is the amount of money that remains from revenue after accounting for all expenses.

**Note:** Gross Income is NOT the same as Gross Profit. Gross Income looks at the full picture (i.e., the sum of all revenues and expenses), whereas Gross Profit only looks at the product and service revenue minus the cost of sales.



# Financial Statement Worksheet

## DUE DILIGENCE



### DOCUMENT REQUEST

Financial Statements

#### Before You Start

Financial Statements include a lot of data that may or may not be relevant to your job as a vendor manager. This worksheet is designed to help you know what data could be *most* valuable in decision making about a vendor's financial stability.

Also, this worksheet is for reviewing *official* financial statements. If you are provided with other financial stability documentation, these questions may not apply.

01. Financial Statements Date

#### 02. What is the financial statement type?

- Audited Financial Statement
- Unaudited Financial Statement
- Form 10-K
- Other \_\_\_\_\_

#### 03. Auditor's Opinion: Financial Position of the Vendor

*For audited financial statements, see the "Auditor's Report" section.*

- Not concerned (e.g., Unqualified, Unmodified, etc.)
- Concerned (e.g., Qualified, Adverse, etc.)
- No opinion due to limitations (i.e., Disclaimer)
- N/A - The statements were not audited.

#### 04. Auditor's Opinion: Internal Control Over Reporting

*For audited financial statements, see the "Auditor's Report" section.*

- The vendor DID maintain effective control
- The vendor did NOT maintain effective control
- N/A - Not a Form 10-K.

#### 05. What does the vendor's balance sheet show?

Balance Sheet	This Year	Last Year
Liquid Assets	<input type="text"/>	<input type="text"/>
Current Assets	<input type="text"/>	<input type="text"/>
Total Assets	<input type="text"/>	<input type="text"/>
Current Liabilities	<input type="text"/>	<input type="text"/>
Total Liabilities	<input type="text"/>	<input type="text"/>
Total Equity	<input type="text"/>	<input type="text"/>

#### 06. What is the vendor's Working Ratio?

*Current Assets / Current Liabilities. Recommended Ratio: > 2.5.*

Year	C. Assets	C. Liabilities	Ratio
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

#### 07. What is the vendor's Quick Ratio?

*Liquid Assets / Current Liabilities. Recommended Ratio: > 1.0.*

Year	L. Assets	C. Liabilities	Ratio
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

#### 08. What is the vendor's Debt to Equity Ratio?

*Total Liabilities / Total Equity. Recommended Ratio: < 1.5.*

Year	T. Liabilities	T. Equity	Ratio
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

#### 09. Did the ratios highlight any concerns?

*A year-to-year change in the ratios could indicate the vendor is less capable of fulfilling their payment obligations than before.*

- ▼ Decrease in Working Ratio
- ▼ Decrease in Quick Ratio
- ▲ Increase in Debt to Equity Ratio
- No Concerns



**10. List the vendor's primary sources of revenue.**

The primary sources of revenue should come from the vendor's primary operation. For example, if you are conducting due diligence for a vendor to provide a new software solution, you would want to ensure the vendor's primary means of income is from the sale of their software or software-related products, not an unrelated product (e.g., arts and crafts supplies, food, clothing, etc.).

+ \_\_\_\_\_

+ \_\_\_\_\_

+ \_\_\_\_\_

**11. List the vendor's primary expenses.**

The vendor's primary expenses should be things like cost of materials, rent, payroll, etc. Review the list of expenses to see where the vendor is spending its resources.

- \_\_\_\_\_

- \_\_\_\_\_

- \_\_\_\_\_

**12. What does the income statement show?**

Income Statement	This Year	Last Year
Total Revenue		
Interest Expense		
Total Expense		
Gross Income		

**13. Did the income statement highlight any concerns?**

A year-to-year change in these areas could indicate the vendor is less profitable than before.

- ▼ Decrease in Revenue
- ▲ Increase in Interest Expense
- ▲ Increase in Total Expense
- ▼ Decrease in Gross Income
- No Concerns

**14. What does the cash flows statement show?**

Cash Balance	This Year	Last Year
Beginning of Year		
End of Year		

**15. Do the cash balances match?**

The cash balance on the Balance Sheet should exactly match the cash balance on the Cash Flows Statement. If these two values do not match, that could be a red flag and warrant further review.

Yes  No

**16. Did the cash flows highlight any concerns?**

A year-to-year change in these areas could indicate the vendor is less capable of managing their current liabilities than before.

- ▼ Decrease in cash during the year
- ▼ Decrease in cash from year to year
- No Concerns

**17. Do the notes describe significant events?**

Look for information about events that occurred in the previous year, such as legal proceedings (e.g., litigation, indemnification, etc.), new products or services, mergers and acquisitions, and changes in key positions (e.g., CEO, CFO, etc.).

Yes (Explain in Comments)  No

**18. Do the notes describe unique adjustments?**

Most financial statements follow an accepted accounting principle (e.g., GAAP, IFRS, etc.). If certain aspects of the principle were not followed, it should be highlighted in Note 1.

Yes (Explain in Comments)  No

**19. Do the notes describe future plans?**

Look for plans of the vendor which could also include things like legal proceedings, new products or services, mergers and acquisitions, and changes in key positions. A good way to find future plans is to perform a word search for the next year in the document.

Yes (Explain in Comments)  No

# Subcontractors

## DUE DILIGENCE

**IF** the vendor uses subcontractors for critical functions,

**THEN** ensure they manage their own vendors well.

Subcontractors are third parties hired by your vendor to help provide products or services to your business. What this means is that (for better or worse) your business is dependent on these subcontractors.

### Should I personally manage my vendors' subcontractors?

This is not a recommended practice and it comes with several challenges. For example:

- It is an inefficient use of your valuable and limited time.
- It sets a precedent that you are accountable for the vendor's choices.
- It is legally questionable, since you do not have a legal agreement with the subcontractor. They don't have to provide you anything.

**Bottom Line:** While you should know who works with your data, systems, and processes, your vendor should be managing their own vendors.

### How can I know if my vendors are managing the subcontractors?

Here are some topics to discuss and questions to ask when performing due diligence on your own vendors.

- 1 Volume**  
How much does the vendor subcontract? This could tell you a lot about things like the vendor's capacity and expertise.
- 2 Nature**  
What activities does the vendor subcontract? This tells you what data, systems, or processes the subcontractor is involved with.
- 3 Reliance**  
How much does the vendor rely on their subcontractors? This tells you if the vendor could function with or without the relationship.
- 4 Geography**  
Where are the subcontractors located? This tells you about any international regulatory or resilience challenges you may face.
- 5 Dependencies**  
Do several vendors depend on a single subcontractor? If so, there might be a single point of failure among your vendors.
- 6 Process**  
What does the vendor's own vendor management program look like? This tells you if they have a stable process for selecting and managing their own vendors.

## GUIDANCE

"An evaluation of the volume and types of subcontracted activities and the degree to which the third party relies on subcontractors helps inform whether such subcontracting arrangements pose additional or heightened risk to a banking organization. This typically includes an assessment of the third party's ability to identify, manage, and mitigate risks associated with subcontracting, including how the third party selects and oversees its subcontractors and ensures that its subcontractors implement effective controls. Other important considerations include whether additional risk is presented by the geographic location of a subcontractor or dependency on a single provider for multiple activities."

*Interagency Guidance on Third-Party Relationships: Risk Management*

## FUN FACT

Subcontractors have lots of names. Some people refer to them as:

- Fourth Parties
- 4th Parties
- Nth Parties
- Subservice Organizations

What do you call them?

# Subcontractors Worksheet

## DUE DILIGENCE



### DOCUMENT REQUEST

Vendor Mgmt. Program Summary

#### 01. How much does the vendor subcontract?

- A lot of activities are subcontracted.
- Some activities are subcontracted.
- Not many activities are subcontracted.

#### 02. What activities does the vendor subcontract?

#### 03. The subcontractors have access to our:

- Proprietary business data
- Confidential customer/member data
- Unclassified data
- Critical business systems
- Non-critical business systems
- Facilities
- Other \_\_\_\_\_

#### 04. Is the vendor reliant on their subcontractors?

- Yes, highly       Yes, minimally
- Yes, somewhat       No, not at all

#### 05. Are any of the subcontractors foreign-based?

*Foreign-based subcontractors can present legal and regulatory challenges, especially related to data security and privacy.*

- Yes (Explain in Comments)       No

#### 06. Are subcontractors geographically dispersed?

*For resilience purposes, critical subcontractors should not rely on the same infrastructure that you or your vendors do.*

- Yes       No (Explain in Comments)

#### 07. Is the subcontractor used by several vendors?

*A subcontractor used by several vendors could be a single point of failure if compromised or if they stop providing services.*

- Yes       N/A
- No       Unknown

#### 08. Vendor Review Frequency for Subcontractors

*In the same way that you review and perform due diligence on your vendors, your vendors should review and perform due diligence on their subcontractors.*

- Annually       Quarterly
- Semiannually       Other \_\_\_\_\_

#### 09. Does the vendor do background checks?

*Vendors should perform background checks for subcontractors who have access to critical systems or confidential information.*

- Yes       N/A
- No       Unknown

#### 10. Which of the following does the vendor review?

*In addition to the listed items, other types of due diligence to consider include: outstanding issues with regulatory entities or law enforcement agencies; consumer complaints; online activity, publicity, public reports, or social media for adverse events; etc.*

- Business Continuity Plan Summaries
- Financial Statements
- Insurance Coverage
- SOC Reports
- Security Testing Reports
- Other \_\_\_\_\_

# Frequently Asked Questions (FAQs)

## DUE DILIGENCE

### When should I start the due diligence process?

The best time to set your due diligence expectations is **before** you begin service with the vendor, when the vendor is on their best behavior and still trying to win your business. If you're already in a relationship with the vendor, the second best time is **now**.

### Can I hire someone to do due diligence for me?

Yes and no. There are vendors who specialize in due diligence gathering and review services. You can also partner with other organizations to do due diligence together. (Regulatory guidance calls this "collaborative arrangements.") However, these options come with their own set of operational, financial, and legal hurdles.

For example, unless you negotiate it in your contract, a vendor is not legally required to provide information about their company to an unaffiliated third party (i.e., the person you hire to do due diligence). Additionally, there may be legal consequences if you share a vendor's proprietary information without the vendor's approval.

Also, you can't outsource accountability. Your business is still responsible for decisions or issues involving your vendors, even if someone else does the research. According to the [Interagency Guidance on Third-Party Relationships: Risk Management](#):

*"Use of any collaborative efforts does not abrogate the responsibility of banking organizations to manage third-party relationships in a safe and sound manner. [...] It is important for the banking organization to evaluate the conclusions from such collaborative efforts based on the banking organization's own specific circumstances and performance criteria for the activity."*

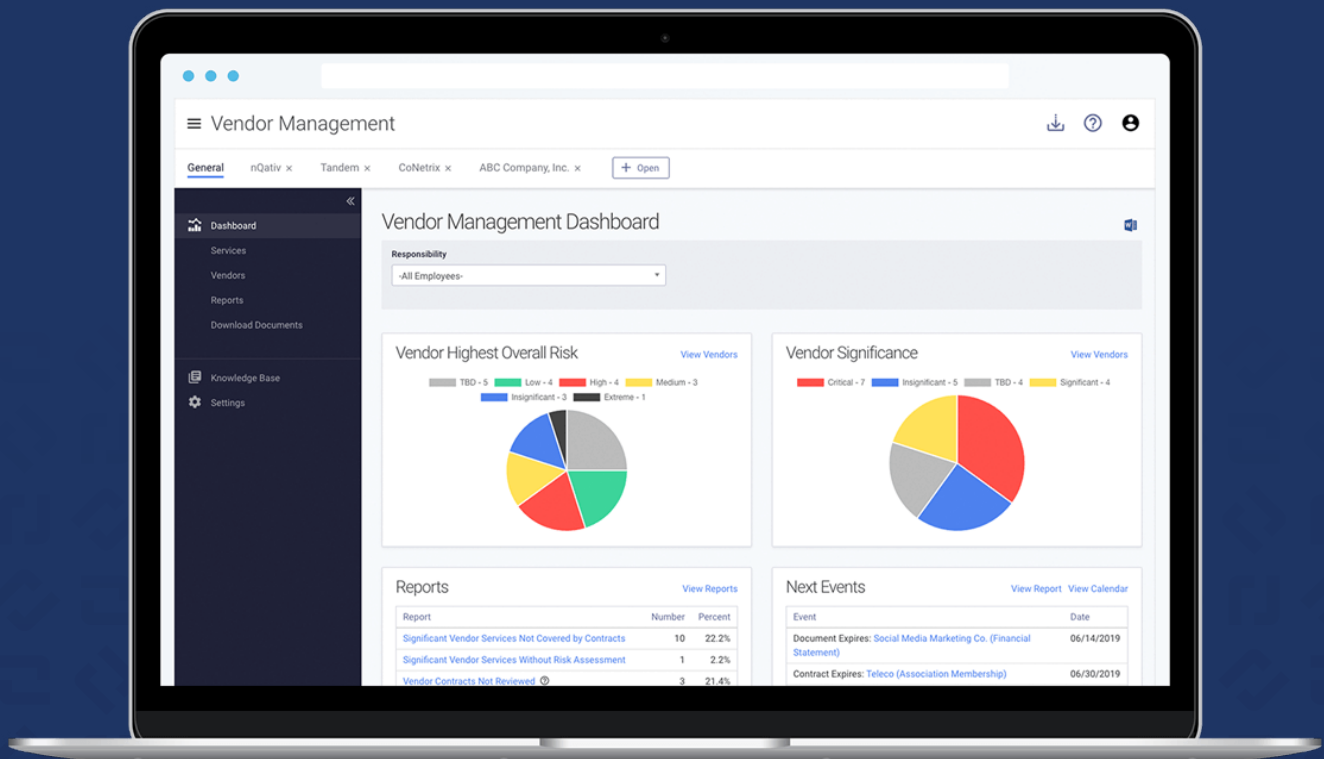
### What if the vendor won't respond?

This is a tough situation, but it is one that a lot of vendor managers face. What if the vendor doesn't have what you requested? What if they can't answer all your questions? Worst of all, what if the vendor "ghosts" you and never replies? Here's the thing: In vendor management, a lack of an answer can still be an answer. If this is where you find yourself with a vendor, here are four possible next steps to consider.

- 1 Communicate with Management**  
The people who are ultimately responsible for the vendor relationship need to be aware of the situation. The decision-makers at your business can help you navigate, advocate for you, or even start the process of finding another vendor.
- 2 Look for Complimentary Controls**  
Sometimes, a vendor may not have the exact answers you need or documents you've requested. In those circumstances, ask yourself (and maybe the vendor), "Is there another way to validate what I need to know?"
- 3 Document an Exception**  
It may be in the best interest of your business to officially accept or defer the risk. This allows you to "excuse" the vendor. This may not be a permanent solution, but an official exception can show your efforts and justify your decisions.
- 4 Reevaluate the Relationship**  
In extreme cases, a lack of evidence or willingness to work with you may be reason to question the legitimacy of the relationship. If you've tried everything and aren't okay with the results, it might be time to do something else.

# Tandem Vendor Management

Manage your third-party risk with Tandem.



Avoid complicated spreadsheets, manually updated calendars, and trying to organize files across network folders. Tandem provides a simplified and streamlined interface, designed to organize your vendor management program.

**Watch a Demo**

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

# Contract Management

A contract exists to define the expectations and obligations of a relationship between your business and a vendor. A contract should be negotiated in such a way that it protects both sides from unwanted or unexpected consequences.

## Common Types of Contracts & Agreements

A contract can come in many flavors. While some may require you to read through several pages and sign at the end, others require you to mark a checkbox and click to agree. Here are some of the most common types of contracts and agreements.

- ✓ Software/Service Agreement
- ✓ User Agreement
- ✓ Terms of Service/Terms of Use
- ✓ Nondisclosure Agreement (NDA)
- ✓ Service Level Agreement (SLA)



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

## Contract Significance & Reviewers

All contracts are legally binding. This fact makes *all* contracts important. However, some contracts carry more risk than others. For example:

- Long-term contracts (e.g., three years, five years, ten years, etc.)
- Contracts for highly expensive services
- Contracts for operationally critical or data critical services

Because of this, you want to make sure you have the right parties involved with the review process. Consider people like:

- |                          |                       |
|--------------------------|-----------------------|
| ✓ Legal Professionals    | ✓ Financial Experts   |
| ✓ Subject Matter Experts | ✓ Senior Management   |
| ✓ Risk Management Team   | ✓ Compliance Officers |

It is better to involve appropriate personnel before the contract is signed than to wait until it may be too late to change things.

## GUIDANCE

“After selecting a service provider, management should negotiate a contract that meets their requirements. [...] The contract is the legally binding document that defines all aspects of the servicing relationship. A written contract should be present in all servicing relationships. This includes instances where the service provider is affiliated with the institution. When contracting with an affiliate, the institution should ensure the costs and quality of services provided are commensurate with those of a nonaffiliated provider. The contract is the single most important control in the outsourcing process.”

*FFIEC Outsourcing Technology Services Booklet*

## DID YOU KNOW?

There's a reason certain parts of contracts use all capital letters.

(And no, it's not that the vendor is yelling or that they forgot to turn off the caps lock.)

Capital letters in a contract are typically used when the vendor has something important to say.

For example, the contract might be asking you to waive your rights to something or it might be telling you of a right that the vendor has reserved.

Whatever the reason, capital letters are used to help make clauses clear and unambiguous.

So, next time you are reading through a contract, pay special attention to the words in ALL CAPS to make sure you aren't missing something key.

## Contract Duration

Contracts can also have different durations. You need to know how long your agreements are effective, so you can know when the renegotiation or termination window opens. Common durations include:



### Fixed-Term

The contract has a specific start date and a predetermined end date.



### Fixed Term (Option to Renew)

The contract has a specific start date and a predetermined end date, but your business may choose to renew again.



### Auto-Renewing

The contract automatically renews at the end of each term unless one party decides to terminate it with notice.



### Indefinite

The contract does not set a predetermined duration or end date. It continues until one party terminates it with notice.



### Project-Based

The contract is tailored for a specific project. It has a defined start date, but the end date is based on project completion.

## Contract Negotiation

If a contract doesn't tick all the checkboxes, so to speak, don't worry. You have a few options.



### Negotiate

While you may not be able to negotiate with every vendor, there may be some who are willing to compromise with you. You have the right to ask. Of course, they have the right to say no, but it never hurts to check.



### Compensate

If you can't come to an agreement, determine if there's another way to mitigate the risk. This is often called "compensating controls." It means that when you can't go with Plan A, there's a Plan B not far behind.



### Evaluate

Sometimes you're stuck. When this happens, you have to make some tough decisions. If you can live with things as they are, you can accept the risk. If you can't, it may be time to consider other options and other vendors.

# Contract Review Worksheet

## CONTRACT MANAGEMENT

### Does the contract define each of the following?

#### 01. Nature and Scope of the Arrangement

Contracts should clearly define things like rights and responsibilities, services provided, service specifications, and resource use (e.g., information, facilities, personnel, systems, intellectual property, equipment, etc.).

Yes  Somewhat  No  N/A

#### 05. Compliance Requirements

Contracts should require the vendor to comply with all applicable laws and regulations. In addition, contracts should also reserve your right to require the vendor to fix and provide status reports on issues of noncompliance.

Yes  Somewhat  No  N/A

#### 02. Performance Measures and Benchmarks

Contracts should clearly define things like key performance indicators (KPIs), service levels, quality standards, deadlines, and other quantifiable criteria. Performance measures should align with business goals.

Yes  Somewhat  No  N/A

#### 06. Cost and Compensation Arrangements

Contracts should clearly define all of the financial aspects of the arrangement, including cost structures, conditions under which costs may be changed, upfront and termination fees, any reimbursement requirements, payment of legal fees, etc.

Yes  Somewhat  No  N/A

#### 03. Information Responsibilities

Contracts should clearly define things like ownership, location(s), and format(s) of data stored by the vendor, the business' ability to access and use its data in a timely manner, restrictions on the vendor's ability to grant access to your systems and data, notification of significant strategic or operational changes, etc.

Yes  Somewhat  No  N/A

#### 07. Ownership and License Details

Contracts should clearly define if and at what point data generated by the vendor becomes your property. In addition, contracts should also include appropriate warranties related to intellectual property (e.g., warranties for the use, licensure, or subscriptions to the vendor's IP).

Yes  Somewhat  No  N/A

#### 04. Right to Audit and Require Remediation

Contracts should require the vendor to have periodic, independent audits by a third-party auditor and/or by your business. In addition, contracts should also reserve your right to require the vendor to fix and provide status reports on issues identified during the audit.

Yes  Somewhat  No  N/A

#### 08. Security and Incident Response Requirements

Contracts should prohibit the vendor (and its subcontractors) from misuse or disclosure of your information. Contracts should also require the vendor to implement appropriate security measures, notify you of incidents, and take corrective action for incidents.

Yes  Somewhat  No  N/A



### 09. Resilience and Business Continuity Plans

Contracts should clearly define how the service will continue in the event the vendor experiences an operational disruption (e.g., business continuity plans, disaster recovery plans, etc.). The contract should also define required resilience controls.

Yes  Somewhat  No  N/A

### 10. Indemnification Clauses

Contracts should clearly define the extent to which each party may be held liable for issues. The contract should not require you to hold the vendor harmless and should allow you to hold the vendor accountable when issues arise.

Yes  Somewhat  No  N/A

### 11. Insurance Requirements

Contracts should require the vendor to maintain insurance commensurate with the risk of possible losses. In addition, consider if you should be listed as "additional insured" and if the vendor should provide notice of coverage changes.

Yes  Somewhat  No  N/A

### 12. Dispute Resolution Processes

Contracts should clearly define processes for resolving issues, including defining whether services will continue to be provided during the resolution process. In addition, contracts should not prohibit arbitration or impose restrictive forum selections.

Yes  Somewhat  No  N/A

### 13. Subcontracting Expectations

Contracts should clearly define under what circumstances a vendor may be allowed to subcontract services. In addition, contracts should address notice requirements, hold the vendor accountable for subcontractors, and define prohibited subcontractors.

Yes  Somewhat  No  N/A

### 14. Foreign-Based Vendor Requirements

Contracts should clearly define approved data storage locations (e.g., only in the United States). In addition, contracts should prohibit moving data offshore and include clauses related to choice-of-law and jurisdictional provision for dispute resolution.

Yes  Somewhat  No  N/A

### 15. Default and Termination

Contracts should clearly define your ability to change vendors, specify what constitutes default, identify remedies, and allow for opportunities to cure defaults. The contract should also ensure the prompt return or destruction of your data and resources.

Yes  Somewhat  No  N/A

### 16. Regulatory Supervision Expectations

Contracts should clearly define if and when provided services are subject to regulatory oversight by your business' regulators, including provisions for access and the ability to terminate the relationship without penalty, if required by the regulator.

Yes  Somewhat  No  N/A

## Contracts and agreements can be messy.

Just because each of these things *should* be defined in your contract doesn't mean that they *will* be. Do your best to find them. Sometimes, they can even be spread out across multiple agreements. If any of these things aren't defined in your contract, it's time to negotiate, compensate, and/or evaluate (see Page 31).

# Nondisclosure Agreement

## CONTRACT MANAGEMENT

**IF** the vendor or its subcontractors access proprietary data,

**THEN** have them sign a nondisclosure agreement (NDA).

A nondisclosure agreement (NDA) is a specific type of contract that exists to protect sensitive information from unauthorized disclosure. Sometimes, this is addressed in the primary agreement. Other times, it has its own document. Either way is good, as long as it is addressed.

## Worksheet

### 01. What data types are covered by the NDA?

*An NDA should explicitly define all the types of information which need to be protected from unauthorized disclosure or misuse.*

- Confidential current/former customer or member data
- Confidential current/former employee data
- Proprietary business data
- Unclassified data
- Other \_\_\_\_\_

### 02. Does the NDA prohibit the vendor from disclosing the data?

*The vendor (and by extension, the vendor's subcontractors) should agree to not misuse or disclose protected information, except as necessary to provide the service.*

- Yes     Somewhat     No     N/A

### 03. Does the NDA require security controls to be implemented?

*The vendor and its subcontractors must implement controls that are equal to (or better than) the controls you would implement to secure the protected information.*

- Yes     Somewhat     No     N/A

### 04. How soon after a breach must the vendor notify you?

*If the vendor or its subcontractors become aware that your protected information was compromised, they must notify you ASAP and within a certain timeframe.*

## DID YOU KNOW?

A nondisclosure agreement goes by many names. Some common aliases include "Confidentiality Agreement" and "Mutual Confidentiality Agreement."

Whatever you call it, the purpose is the same:



"Keep it secret.  
Keep it safe."

(Yes, that's Gandalf.)

## FUN FACT

"Proprietary business data" is an umbrella term that refers to any kind of data that gives a business a competitive advantage.

This often includes things like:

- Financial information
- Business plans
- Trade secrets
- Intellectual property
- Customer lists
- Vendor lists
- Software source code

# Service Level Agreement

## CONTRACT MANAGEMENT

### PRO TIP

Don't just take the SLA at face value. Get out your own BCP and compare the stated timelines to make sure it would meet your expectations.

For example:

If a SLA has a RTO of 48 hours,



but you need it in 12 hours,



that leaves a gap of 36 hours.



What would you do in that gap? Would your operations be able to continue? If not, you may need to negotiate, compensate, and/or evaluate your options (see Page 31).

**IF** the vendor provides operationally important services,

**THEN** have them sign a service level agreement (SLA).

A service level agreement (SLA) is a specific type of contract that exists to ensure resilience and continuity of operations. Sometimes, this is addressed in the primary agreement. Other times, it has its own document. Either way is good, as long as it is addressed.

## Worksheet

### 01. Are covered services clearly defined by the SLA?

*A SLA should identify which services are included. Knowing this information can help you know if the SLA is suitable for the services provided to you by the vendor.*

Yes  Somewhat  No  N/A

### 02. Which of the following metrics are specified by the SLA?

*A SLA should specify measurable performance metrics (e.g., recovery timeframes, availability percentages, etc.).*

Recovery Time Objective (RTO) \_\_\_\_\_

Recovery Point Objective (RPO) \_\_\_\_\_

Uptime \_\_\_\_\_

Response Time \_\_\_\_\_

Satisfaction Score \_\_\_\_\_

Other \_\_\_\_\_

### 03. Does the SLA define recourse if the agreement is not met?

*A SLA should define penalties or remedies for the vendor's failure to meet the service levels (e.g., financial reimbursement, service credits, etc.).*

Yes  Somewhat  No  N/A

### 04. Do the service levels align with your business needs?

*The service levels should support the successful operation of your business. Compare the metrics with your own business continuity plan (BCP) to determine adequacy.*

Yes  Somewhat  No  N/A

# Frequently Asked Questions (FAQs)

## CONTRACT MANAGEMENT

### Where are my contracts?


Believe it or not, this is a common question. If you don't have a contract management process, fully-executed contracts have a tendency to disappear. This is especially true of long-term contracts. The good news is that your vendor should have a copy. Reach out to your contact and ask for the executed version. If they don't have it, that's probably your sign it is time to renegotiate.


### How often should a contract be reviewed?

Always review a contract before you sign it. In the case of auto-renewing or indefinite contracts, the contract stays the same until you or the vendor decides to change it. That said, some contracts can get out of date, especially long-term ones. Because of this, you probably want to re-review the contract:

- 1 When You Change**  
Let's say you start a new product or service. Will the contract you negotiated "back then" still cover what you need or do you need to level up for your new project?
- 2 When the Vendor Changes**  
Let's say the vendor goes through a big change (e.g., a merger, a lawsuit, an incident, a new investor, etc.). Can they still meet the terms? Better yet, could they do better now?
- 3 Before Renewal Dates**  
If you are coming up on an expiration or renewal date, there is no better time to revisit the contract. Is there something you discovered that needs renegotiated?
- 4 If it is Old**  
Long-term contracts are notorious for getting outdated. As technology, regulations, and best practices change, so should the contract. What might need a refresher?

### Addendums vs. Amendments: What's the difference?

 **Addendum**  
An addendum is an **addition** to a contract. Think of it as though you and your vendor are saying, "Yes, and ..." For example, if the scope of work needs expanded or if you need to build in a new notification requirement, instead of renegotiating the entire contract, you can add an addendum.

 **Amendment**  
An amendment is a **change** to a contract. Think of it as though you and your vendor are saying, "Instead, let's ..." For example, if the price changes due to cost of materials or if the contract needs an extension, instead of starting from square one, you can change it via amendment.

### When can I ask for a change to my contract?

Anytime! Contrary to popular belief, an addendum can be added or an amendment can be made at any time during the relationship, as long as both parties agree to the modification. This is an especially helpful tool for handling regulatory changes. For example, if you are now required to provide notice to your regulators of an incident, you might want to add an "Incident Notification Addendum" to your contract with the vendor. This may open up negotiations or the vendor may say "no." Either way, it helps you and can be a decision factor next time you renew.

# Tandem Partner Program

---

We have partners ready to help with your vendor management needs.



The Tandem Partner Program exists to connect consultants with organizations who use Tandem. Work with our partners to gain access to specialized expertise and take your vendor management program to the next level.

[Tandem.App/Partner-Program](https://Tandem.App/Partner-Program)

# Monitoring

The purpose of monitoring is to confirm things are going well, escalate problems, and respond to any issues that have come up. While it may sound simple enough, monitoring is often the most time-consuming and misunderstood part of vendor management.

## The Secret of Monitoring

The reason monitoring is so hard is because it can often feel like fighting against a brick wall.

- You ask for documents and you don't get them.
- You ask questions and you don't get replies.
- You hire companies to do monitoring for you and you find out you still have to do most of the work anyways because your kids get along better than your vendors do.

Does any of that sound familiar to you? If so, here are two secrets you should know about monitoring:

1. You are more likely to get the information you want from a vendor when they are trying to win your business.
2. If you do a great job setting a baseline during planning, due diligence, and contract negotiation, monitoring will take a lot less effort.

**Bottom Line:** Monitoring is important, but the foundation you build *before* you get into a relationship with a vendor sets the tone for monitoring.

## What Changed?

Instead of being the bread-and-butter of a vendor management program, monitoring should be the icing on the top. It's about answering one simple question: What changed?

- 1 Did you change?** Does the vendor still meet your needs? Did you grow? Did you have a shift in priority? Is there a better option out there? You get the idea. Relationships change.
- 2 Did they change?** Have there been any changes since the last time you reviewed the vendor? Look at the same documents you looked at last year and see what's different.
- 3 Did the world change?** Is there anything foreseeable that could impact the relationship (e.g., the economy, a merger, a technology development, etc.)?

In ideal circumstances, there should be very little that changed. If there are significant changes, this should be a decision factor for you and for your business.

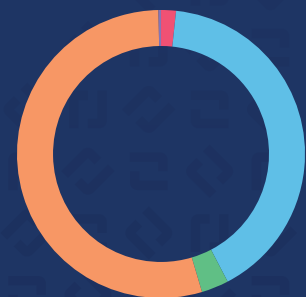
## GUIDANCE

"Financial institutions should have an oversight program to ensure service providers deliver the quantity and quality of services required by the contract. The monitoring program should target the key aspects of the contracting relationship with effective monitoring techniques. The program should monitor the service provider environment including its security controls, financial strength, and the impact of any external events."

*FFIEC Outsourcing Technology Services Booklet*

## SURVEY SAYS

We asked a group of vendor managers about where they spend the most time. **Over half** of responders said they spend the most time "Monitoring."



- Planning (2%)
- Due Diligence (41%)
- Contract Management (3%)
- Monitoring (54%)
- Termination (<1%)

## SOURCE

Tandem Survey, August 2023 (n=359)

# Monitoring Worksheet

## MONITORING



### DOCUMENT REQUEST

Previously Requested Documents

01. Last Review Date

02. Today's Date

### SINCE THE LAST REVIEW

03. Has your business significantly changed?

Yes  No

04. Are there any notable changes in the following?

*Look for anything that might be different from the last time you reviewed the same type of document. How is this year's document different from last year's, and could that mean anything to you?*

- Business Profile
- Certificate of Insurance
- Business Continuity Plan (BCP) Summary
- SOC Report
- Security Testing Report
- Financial Statement
- Vendor Management Program Summary
- Other \_\_\_\_\_

05. Are there any external forces to consider?

- Economic challenges
- Geopolitical instability
- Mergers and acquisitions
- Technological developments
- Other \_\_\_\_\_

06. Were all contractual expectations met?

*Make note of any instances in which the vendor did not fulfill contractual requirements (e.g., contracts, NDAs, SLAs, etc.).*

Yes  No

07. Summarize any notable changes or concerns.

*Not all changes are negative. Consider how positive changes may also impact your relationship with the vendor.*

08. Based on the review, what do you suggest?

- Continue as normal
- Monitor more frequently
- Escalate to senior management
- Negotiate with the vendor
- Explore termination options
- Other \_\_\_\_\_

# Termination

All good things must come to an end. Planning for the eventual termination of a relationship is a good step to take now, so your business isn't surprised when it happens.

When termination happens, you really have just three options:



Switch to another vendor



Bring the service(s) in-house



Discontinue the activity

Termination impacts a lot of different areas. As you plan for termination, think about the following potential impacts.



## Financial Impact

Determine if all the termination costs and fees are accounted for in the contract.



## Resource Impact

Consider the amount of time, effort, and expertise it will take to transition away from the vendor. (Time is money, too.)



## Security Impact

Evaluate what the transition may mean for things like access control, data retention, data destruction, etc.



## People Impact

Consider how the transition may impact your employees, your customers/members, and your other vendors.

Whatever you end up doing, your purpose is to ensure as smooth of a transition as possible, so you can avoid any operational disruptions.

**Bottom Line:** Planning for termination is a necessary part of vendor management today, so that tomorrow isn't a major headache.

## GUIDANCE

"A banking organization may terminate a relationship for various reasons, such as expiration or breach of the contract, the third party's failure to comply with applicable laws or regulations, or a desire to seek an alternate third party, bring the activity in-house, or discontinue the activity. When this occurs, it is important for management to terminate relationships in an efficient manner, whether the activities are transitioned to another third party, brought in-house, or discontinued."

*Interagency Guidance on Third-Party Relationships: Risk Management*



# Termination Worksheet

## TERMINATION

### 01. What is your termination plan?

- Switch vendors
- Bring the service(s) in-house
- Discontinue the activity

### 02. What resources would a transition require?

- Time \_\_\_\_\_
- Effort \_\_\_\_\_
- Cost \_\_\_\_\_
- Other \_\_\_\_\_

### 03. Will there be any downtime during transition?

- Yes             N/A
- No               Unknown

### 04. What are the vendor's data retention procedures?

### 05. What are the vendor's data destruction procedures?

### 06. Will any residual data be left with the vendor?

- Yes             N/A
- No              Unknown

### 07. Will the vendor's access need to be changed?

*Consider if the vendor or its subcontractors have access to your business' systems or facilities. If so, consider how that access may need modified or restricted following termination.*

- Yes             N/A
- No              Unknown

### 08. Who will be impacted by the termination?

- Employees
- Customers/Members
- Other Vendors
- Others \_\_\_\_\_

### 09. Additional Termination Details

# Report to the Board

At this point, you might be wondering: What's next? What should you do with the information you learned? Bringing it full circle, this is the part of the process where you translate your data into meaningful information for the decision-makers at your organization. Here are three things they need to know:



## New Relationships

Create a list of new vendor relationships started since your last report. Share what they do for your business.



## Incidents

Identify any vendors who experienced an incident since your last report. Share what the incident was and how you were impacted.



## Status Update

Communicate the status of your vendor relationships. Share what you think your business should do with the info.

## Not Sure What to Share?

Here's a template you can follow to create your status update.

Situation	Business Impact	Action Plan
[ABC] fact about the vendor.	This exposes the business to [XYZ] risk.	I recommend [123].

## Status Update Examples

Here are some examples of what this could look like in action.

Situation	Business Impact	Recommended Action Plan
The contract does not address data destruction.	This exposes the business to legal risk, operational risk, and reputation risk.	I recommend negotiating a "data destruction" addendum.
The financial statements show negative trends.	This exposes the business to financial risk and strategic risk.	I recommend requesting quarterly financial statements.
The vendor won't respond to my questions.	This exposes the business to strategic risk and operational risk.	I recommend evaluating other vendors.

**Bottom Line:** You are the vendor management expert. Providing helpful reports to senior management and the Board of Directors is one way you can turn vendor management into a value-add for your business.

# Report to the Board Worksheet

01. Who are your new vendors and what services do they provide for your business?



---



---



---



---



---

02. Have any vendors had recent incidents? If "yes," please describe.

Yes

No

N/A

Unknown

03. What status update(s) do you need to share?

Vendor	Situation	Business Impact	Recommended Action Plan

# Conclusion

The key takeaway is this: Vendor management isn't just about regulatory compliance. When done correctly, vendor management can be a practical tool, designed to give you the roadmap you need to successfully navigate your vendor relationships, manage risks, and support your business.

While the idea of a lifecycle is nice, we know the vendor management process doesn't always end up looking like a perfect circle, and that's okay. The goal isn't perfection. Vendor management isn't a "once-and-done" kind of thing. It's a moving target. You will find many twists and turns during your adventures.

Our hope is that you can use the tools in this workbook to help you:

- Identify the areas of your vendor management program where things could be leveled up;
- Spot vendor data and trends which could be key decision factors for your business;
- Grow and nurture healthy partnerships with your vendors;
- And ultimately, help your business thrive.

If you found this book helpful, we would love for you to check out [Tandem Vendor Management](#). It takes the forms in this book to the next level. With helpful reminders, customizable reporting, an easy-to-use interface, a knowledge base full of tutorials, and a team of vendor management experts to boot, Tandem makes managing vendors easy.

Best wishes for a successful vendor management journey!



# Further Reading

## FFIEC GUIDANCE

IT Examination Handbook

- Architecture, Infrastructure, and Operations Booklet
- Business Continuity Management Booklet
- Information Security Booklet
- Outsourcing Technology Services Booklet
- Supervision of Technology Service Providers

Cybersecurity Assessment Tool:  
External Dependency Management Domain

Joint Statement: Security in a Cloud Computing Environment

## FDIC GUIDANCE

- FIL-52-2023 InTREx Procedures
- FIL-29-2023 Third-Party Relationships: Risk Management
- FIL-74-2021 Computer-Security Incident Notification Rule
- FIL-59-2021 Conducting Due Diligence on FinTechs
- FIL-19-2019 Technology Service Provider Contracts
- FIL-13-2014 Technology Outsourcing Tools
- FIL-44-2008 Guidance for Managing Third-Party Risk\*
- FIL-49-99 Bank Service Company Act

## FRB GUIDANCE

- SR 23-4 Third-Party Relationships: Risk Management
- SR 22-4 Computer-Security Incident Notification Rule
- SR 21-16 Access to Innovation through Partnerships
- SR 21-15 Conducting Due Diligence on FinTechs
- SR 13-19 Guidance on Managing Outsourcing Risk\*
- SR 12-14 Supervision of Technology Service Providers

## OCC GUIDANCE

- 2023-17 Third-Party Relationships: Risk Management
- 2021-55 Computer-Security Incident Notification Rule
- 2021-40 Conducting Due Diligence on FinTechs
- 2020-10 Third-Party Relationships FAQ\*
- 2017-7 Supplemental Examination Procedures
- 2013-29 Third-Party Relationships: Risk Management\*
- 2012-34 Supervision of Technology Service Providers
- 2002-16 Foreign-Based Service Providers

## NCUA GUIDANCE

- 23-CU-07 Cyber Incident Notification Requirements
- 23-CU-02 Expansion of CUSO Activities
- 21-CU-16 Third-Parties that Provide Digital Assets
- 14-CU-07 Contractual Agreements with CUSOs
- 2011-01 Corporate Credit Union CUSO Activities
- 10-CU-26 Payment System Service Providers
- 08-CU-19 Mortgage Brokers & Correspondents
- 08-CU-09 Third-Party Relationships Questionnaire
- SL 07-01 Evaluating Third Party Relationships
- 2000-04 Third-Party Risk
- 01-CU-20 Due Diligence Over Service Providers

NCUA Information Security Examination (ISE)

- Technology Service Providers Components
- Third-Party Risk Management Components

## TANDEM BLOG

- What is Vendor Management?
- Bank Service Company Act (BSCA)
- Difference Between Vendors and Third Parties
- Due Diligence Collection Methods
- FinTech Risk Management
- Office of Foreign Assets Control (OFAC)
- SOC Report Reviews
- Subcontractor Risk Management
- Third-Party Incident Response
- Top Vendor Management Software Features to Consider Before You Buy
- Vendor Risk Assessment

\* These guidance documents are considered "inactive," but may still provide helpful vendor management context or insights.



# The State of Cybersecurity Report

Each year, a panel of Tandem security and compliance experts analyze survey data from hundreds of security professionals to understand how financial institutions are managing cybersecurity.



Download the State of Cybersecurity Report by Tandem to see more insights like the ones in this document, and learn more about how your organization's vendor management and cybersecurity practices compare with your peers.

[Tandem.App/State-of-Cybersecurity-Report](https://Tandem.App/State-of-Cybersecurity-Report)

# About Tandem

## WHO WE ARE

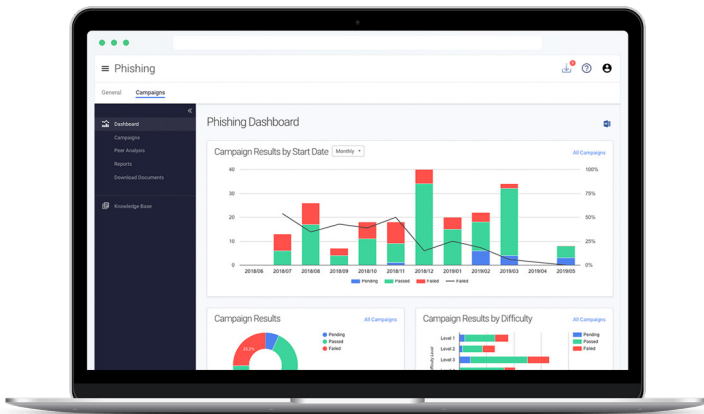
A problem financial institutions experience is the burden of information security compliance. Tandem grew out of the confidence that we can solve this problem.

First, we supported our clients by helping them maintain their documents, but it didn't take long to decide that a software solution could help more people, faster. In 2007, we began developing the do-it-yourself compliance application for information security, now known as Tandem.

We named our product Tandem because it works in partnership - in tandem - with you. You bring your knowledge of your organization and your needs. We bring software built by information security experts to help you create, organize, and manage your information security program.

We believe you have what it takes to manage information security and regulatory compliance. With the right tool, you can do it fast.

Learn more about how Tandem can help you at [Tandem.App](https://Tandem.App) or watch a demo at [Tandem.App/Vendor-Management-Overview](https://Tandem.App/Vendor-Management-Overview).



## OUR PRODUCTS



Audit Management



Business Continuity Plan



Compliance Management



Cybersecurity



Identity Theft Prevention



Incident Management



Internet Banking Security



Phishing



Policies



Risk Assessment



Vendor Management



Copyright © Tandem, LLC. 2024.06.v1  
info@tandem.app  
844-698-9800