

WELCOME TO

Regulation S-P: How to Comply with the New Amendments

Alyssa Pugh, CISM, CRISC, Security+
GRC Content Manager
Tandem, LLC

apugh@tandem.app
[LinkedIn.com/in/AlyssaPugh](https://www.linkedin.com/in/AlyssaPugh)

DISCLAIMER

- **This presentation is for information only.**
Evaluate risks before acting on ideas from this session.
- **This presentation contains opinions of the presenters.**
Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
Unauthorized release of this information is prohibited.
Original material is copyright © 2025 Tandem.

SESSION INFO



AUDIO / VIDEO

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



SURVEY

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









RESOURCES

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



QUESTIONS

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

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



Tandem[®]

A CoNetrix company

Which of the following best describes your organization?

How many employees work for
your organization?

- Overview of the Rule
- Regulatory Requirements
 - Security Policies and Procedures
 - Incident Response
 - Customer Notice
 - Service Providers
 - Records Retention and Destruction
- Wrap Up and Bonus Content

**SUBMIT YOUR
QUESTIONS!**

Overview of the Rule

How familiar are you with the
Regulation S-P updates?

AGENCY

Securities & Exchange Commission (SEC)

TITLE

Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

TIMELINE

- **04/06/2023:** Proposed Rule
- **06/03/2024:** Final Rule Approved
- **08/02/2024:** Final Rule Effective Date
- **12/03/2025:** Mandatory Compliance Date #1
- **06/03/2026:** Mandatory Compliance Date #2

FEDERAL REGISTER

<https://www.federalregister.gov/d/2024-11116>

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 240, 248, 270, and 275

[Release Nos. 34-100155; IA-6604; IC-35193; File No. S7-05-23]

RIN 3235-AN26

Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission (“Commission” or “SEC”) is adopting rule amendments that will require brokers and dealers (or “broker-dealers”), investment companies, investment advisers registered with the Commission (“registered investment advisers”), funding portals, and transfer agents registered with the Commission or another appropriate regulatory agency (“ARA”) as defined in the Securities Exchange Act of 1934 (“transfer agents”) to adopt written policies and procedures for incident response programs to address unauthorized access to or use of customer information, including procedures for providing timely notification to individuals affected by an incident involving sensitive customer information with details about the incident and information designed to help affected individuals respond appropriately. In addition, the amendments extend the application of requirements to safeguard customer records and information to transfer agents; broaden the scope of information covered by the requirements for safeguarding customer records and information and for properly disposing of consumer report information; impose requirements to maintain written records documenting compliance with the amended rules; and conform annual privacy notice delivery provisions to the terms of an exception provided by a statutory amendment to the Gramm-Leach-Bliley Act (“GLBA”).

DATES:

Effective date: This rule is effective August 2, 2024.

Compliance date: The applicable compliance dates are discussed in section ILF of this rule.

FOR FURTHER INFORMATION CONTACT:

Emily Hellman, James Wintering, Special Counsels; Edward Schellhorn, Branch Chief; Devin Ryan, Assistant Director; John Fahey, Deputy Chief Counsel; Emily Westenberg Russell, Chief Counsel; Office of Chief Counsel,

Division of Trading and Markets, (202) 551-5550; Kevin Schopp, Senior Special Counsel; Moshe Rothman, Assistant Director; Office of Clearance and Settlement, Division of Trading and Markets, (202) 551-5550, Susan Ali and Andrew Deglin, Counsels; Michael Khalil and Y. Rachel Kuo, Senior Counsels; Blair Burnett and Bradley Gude, Branch Chiefs; or Brian McLaughlin Johnson, Assistant Director, Investment Company Regulation Office, Division of Investment Management, (202) 551-6792, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION: The Commission is adopting amendments to 17 CFR 248.1 through 248.100 (“Regulation S-P”) under Title V of the GLBA [15 U.S.C. 6801 through 6827], the Fair Credit Reporting Act (“FCRA”) [15 U.S.C. 1681 through 1681x], the Securities Exchange Act of 1934 (“Exchange Act”) [15 U.S.C. 78a *et seq.*], the Investment Company Act of 1940 (“Investment Company Act”) [15 U.S.C. 80a-1 *et seq.*], and the Investment Advisers Act of 1940 (“Investment Advisers Act”) [15 U.S.C. 80b-1 *et seq.*].

Table of Contents

I. Introduction and Background
II. Discussion
A. Incident Response Program Including Customer Notification
1. Assessment
2. Containment and Control
3. Notice to Affected Individuals
4. Service Providers
B. Scope of Safeguards Rule and Disposal Rule
1. Scope of Information Protected
2. Extending the Scope of the Safeguards Rule and the Disposal Rule To Cover All Transfer Agents
3. Maintaining the Current Regulatory Framework for Notice-Registered Broker-Dealers
C. Recordkeeping
D. Exception From Requirement To Deliver Annual Privacy Notice
E. Existing Staff No-Action Letters and Other Staff Statements
F. Compliance Period
III. Other Matters
IV. Economic Analysis
A. Introduction
B. Broad Economic Considerations
C. Baseline
1. Safeguarding Customer Information: Risks and Practices
2. Regulations and Guidelines
3. Market Structure
4. Benefits and Costs of the Final Rule Amendments
5. Written Policies and Procedures
6. Extending the Scope of the Safeguards Rule and the Disposal Rule
7. Recordkeeping
8. Exception From Annual Notice Delivery Requirement

E. Effects on Efficiency, Competition, and Capital Formation
F. Reasonable Alternatives Considered
1. Reasonable Assurances From Service Providers
2. Lower Threshold for Customer Notice
3. Encryption Safe Harbor
4. Longer Customer Notification Deadlines
5. Broader National Security and Public Safety Delay in Customer Notification
V. Paperwork Reduction Act
A. Introduction
B. Amendments to the Safeguards Rule and Disposal Rule
VI. Final Regulatory Flexibility Act Analysis
A. Need for, and Objectives of, the Final Amendments
B. Significant Issues Raised by Public Comments
C. Small Entities Subject to Final Amendments
D. Projected Reporting, Recordkeeping, and Other Compliance Requirements
E. Agency Action To Minimize Effect on Small Entities
F. Statutory Authority

I. Introduction and Background

Regulation S-P is a set of privacy rules adopted pursuant to the GLBA and the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”) that govern the treatment of nonpublic personal information about consumers by certain financial institutions.¹ The Commission is adopting rule amendments that are designed to modernize and enhance the protections that Regulation S-P provides by addressing the expanded use of technology and corresponding risks that have emerged since the Commission originally adopted Regulation S-P in 2000. The amendments in particular update the requirements of the “safeguards” and “disposal” rules. The safeguards rule requires brokers, dealers, investment companies,² and registered investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information.³ The disposal rule, which applies to transfer agents

¹ See 17 CFR 248.1.

² Regulation S-P applies to investment companies as the term is defined in section 3 of the Investment Company Act (15 U.S.C. 80b-3), whether or not the investment company is registered with the Commission. See 17 CFR 248.3(b). Thus, a business development company, which is an investment company but is not required to register as such with the Commission, is subject to Regulation S-P. Similarly, employees’ securities companies—including those that are not required to register under the Investment Company Act—are investment companies and are, therefore, subject to Regulation S-P. By contrast, issuers that are excluded from the definition of investment company—such as private funds that are able to rely on section 3(c)(1) or 3(c)(7) of the Investment Company Act—are not subject to Regulation S-P.

³ 17 CFR 248.30(a). References in this release to “rule 248.30” are to 17 CFR 248.30.

“Covered Institutions”



Investment
Companies



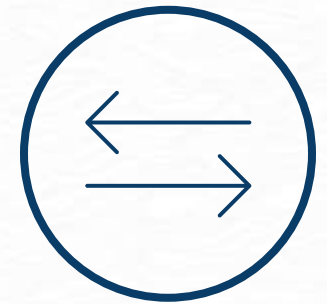
Registered
Investment
Advisers



Broker-Dealers



Funding
Portals



Transfer Agents

WHEN IS COMPLIANCE REQUIRED?



Large Institutions



Small Institutions



No Exemptions

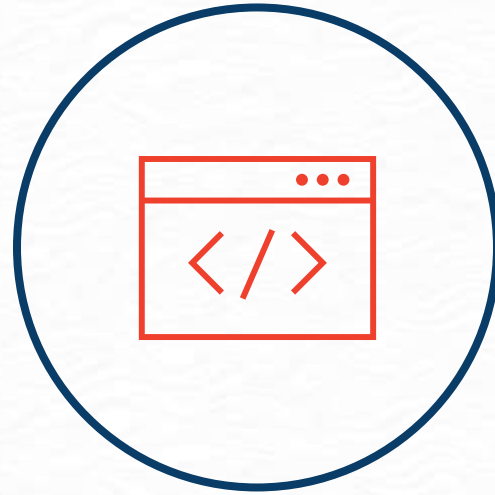
“An exemption for small entities would not be appropriate. Small entities are as vulnerable as large ones to the types of data security breach incidents we are trying to address. In this regard, the specific elements the final amendments must be considered and incorporated into the policies and procedures of all covered institutions, regardless of their size, to mitigate the potential for fraud or other substantial harm or inconvenience to investors. Exempting small entities from coverage of the amendments or any part of the amendments could compromise the effectiveness of the amendments and harm investors by lowering standards for safeguarding investor information maintained by small covered institutions. Excluding small entities from requirements that would be applicable to larger covered institutions also could create competitive disparities between large and small entities, for example by undermining investor confidence in the security of information maintained by small covered institutions.”

TYPE	LARGE (1 2 / 0 3 / 2 5)	SMALL (0 6 / 0 3 / 2 6)
Investment Company	≥ \$1 Billion Net Assets at End of Most Recent Fiscal Year	< \$1 Billion Net Assets at End of Most Recent Fiscal Year
Registered Investment Adviser	≥ \$1.5 Billion Assets Under Management	< \$1.5 Billion Assets Under Management
Broker-Dealer	All Broker-Dealers Not Classified as “Small”	<ul style="list-style-type: none"> • < \$500,000 Total Capital • Not Affiliated with Larger Firm
Transfer Agent	All Transfer Agents Not Classified as “Small”	<ul style="list-style-type: none"> • < 500 Transfers in 6 Months • < 1,000 Shareholder Accounts • Only Serve Small Issuers • Not Affiliated with Larger Firm

WHY AN UPDATED RULE?



More Data



More Threats



More Vendors

“Since Regulation S-P was first adopted in 2000, evolving digital communications and information storage tools and other technologies have made it easier for firms to obtain, share, and maintain individuals’ personal information. This increases the risk of customers’ information being accessed or used without authorization, for example in a cyberattack or if customer information is improperly disposed of or stolen. In particular, as a frequently-targeted industry, the financial sector has observed increased exposure to cyberattacks that threaten not only the financial firms themselves, but also their customers, especially considering that customer records and other information that covered institutions possess can be particularly sensitive. The final amendments will modernize and enhance the protections that Regulation S-P already provides to address this changed landscape.”

KEY TAKEAWAY

The purpose of this updated rule is to better protect customer data and ensure customers are promptly informed of breaches.

**SUBMIT YOUR
QUESTIONS!**

Regulatory Requirements

1

Security Policies and Procedures

2

Incident Response

3

Customer Notice

4

Service Providers

5

Records Retention and Destruction



REGULATORY REQUIREMENTS

Security Policies and Procedures

“Develop, implement, and maintain **written policies and procedures** that address administrative, technical, and physical safeguards for the protection of customer information.”

“Every covered institution must develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information. These written policies and procedures must be reasonably designed to:

- (i) Ensure the security and confidentiality of customer information;
- (ii) Protect against any anticipated threats or hazards to the security or integrity of customer information; and
- (iii) Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.”

SECURITY POLICY & PROCEDURE EXAMPLES

- ✓ Acceptable Use
- ✓ Access Control
- ✓ Artificial Intelligence
- ✓ Authentication
- ✓ Change Management
- ✓ Data Management
- ✓ Encryption
- ✓ Incident Management
- ✓ IT Asset Management
- ✓ Mobile Device Management
- ✓ Network Monitoring & Log Management
- ✓ Security Awareness Training
- ✓ Vendor Management
- ✓ Vulnerability & Patch Management

Does your organization have security policies and procedures?



WEBINAR

How to Write an AI Policy

Thursday, July 17
2:00 PM CDT



Savannah Richards

How to Write an AI Policy

Jul 17, 2025

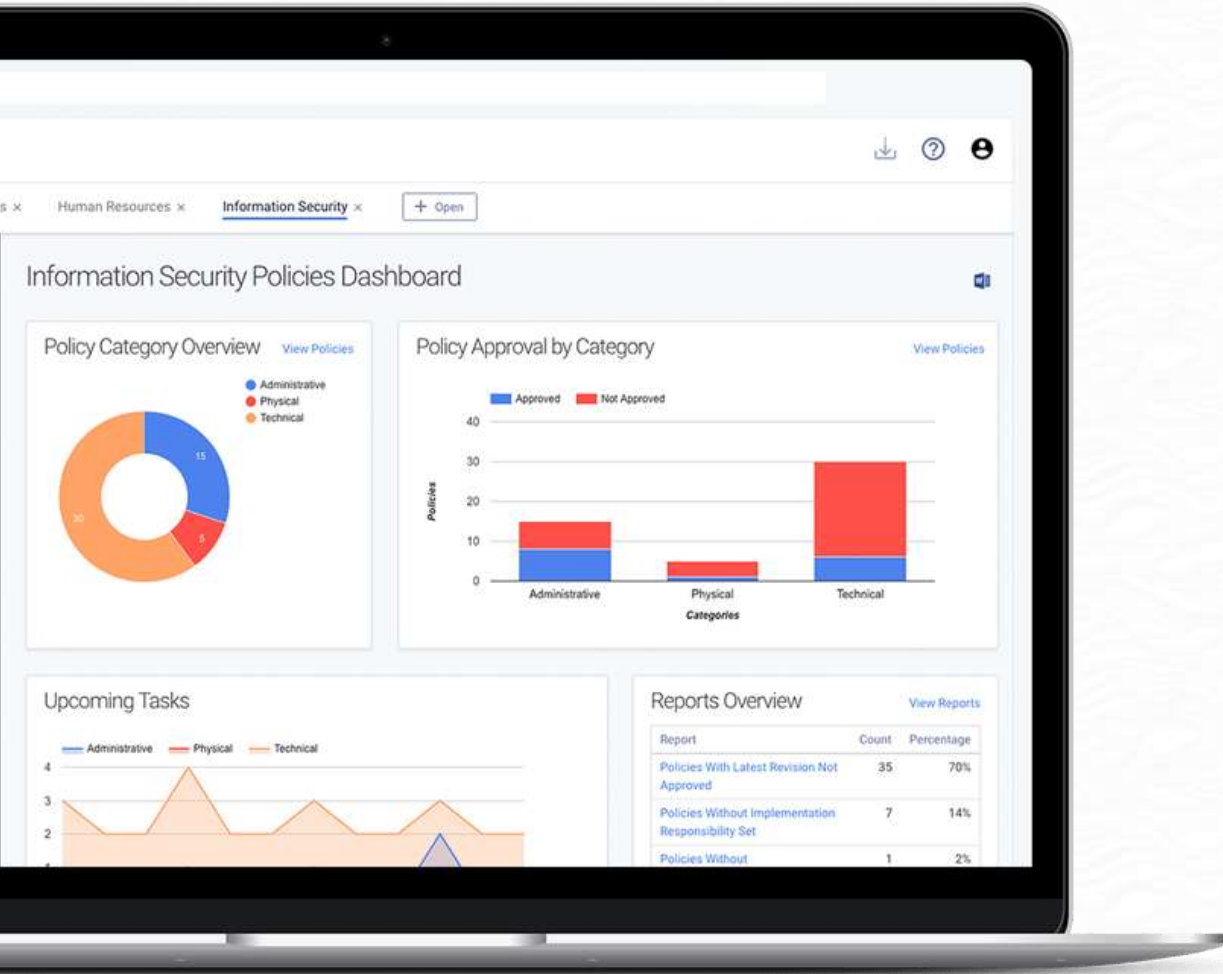
VIEW

FREE RESOURCE

AI Policy Webinar: Watch the Recording

Tandem.App/Webinars





LEARN MORE

Tandem Policies Software

Tandem.App/Policies-Management-Software



KEY TAKEAWAY

Clear security policies and procedures protect customer data, reducing risk of harm.

**SUBMIT YOUR
QUESTIONS!**

REGULATORY REQUIREMENTS

Incident Response



“Written policies and procedures in paragraph (a)(1) of this section must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:

- (i) Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;
- (ii) Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- (iii) Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with paragraph (a)(4) of this section unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.”

Does your organization have an incident response plan?



People



Logs



Alerts



News

What happened?

Perform initial investigation and construct a chain of events.

How did it happen?

Determine the entry point and perform a root cause analysis.

What was affected?

Perform an impact assessment.

How do you know?

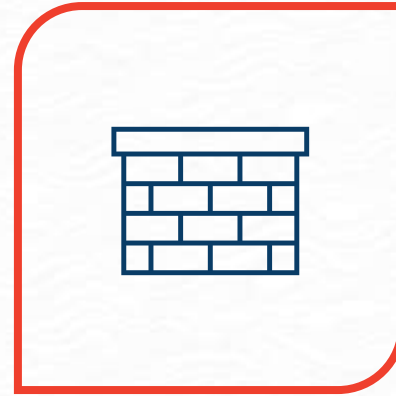
Look for indicators of compromise (IOCs) and document evidence.



Isolate
Affected
Areas



Disable
Compromised
Accounts



Block
Malicious
Traffic



Heighten
Security
Awareness



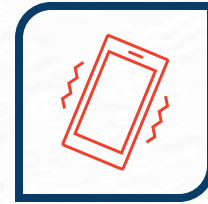
Restore Clean Backups



Remediate Vulnerabilities



Repair Affected Files



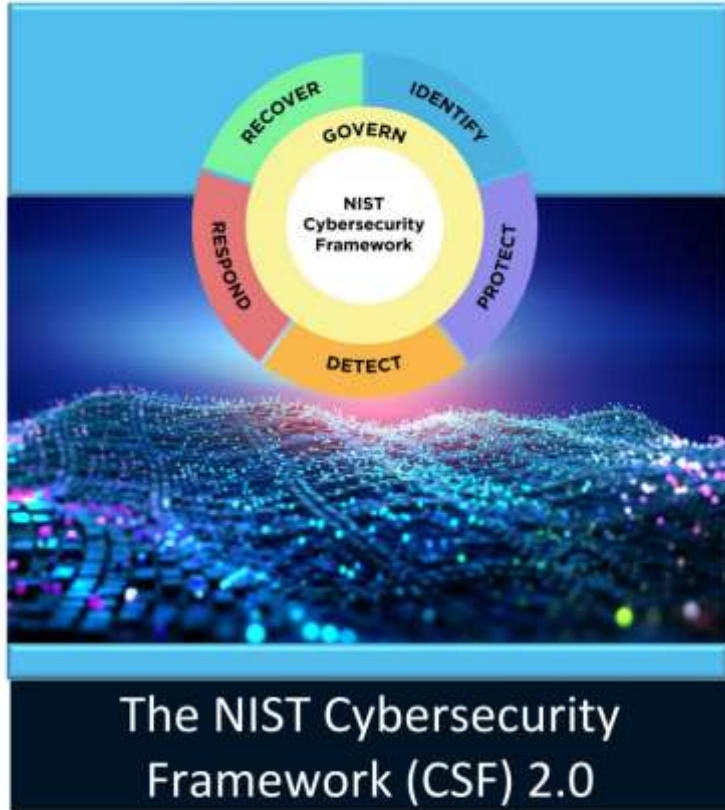
Reset Authentication Tokens



Rebuild Compromised Systems



Replace Ineffective Controls



National Institute of Standards and Technology
This publication is available free of charge from: <https://doi.org/10.6028/NIST.CSWP.29>
February 26, 2024



<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

NIST Special Publication 800
NIST SP 800-61r3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

A CSF 2.0 Community Profile

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-61r3>



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>

ENJOYING THIS WEBINAR?

Sign Up for the Next One!

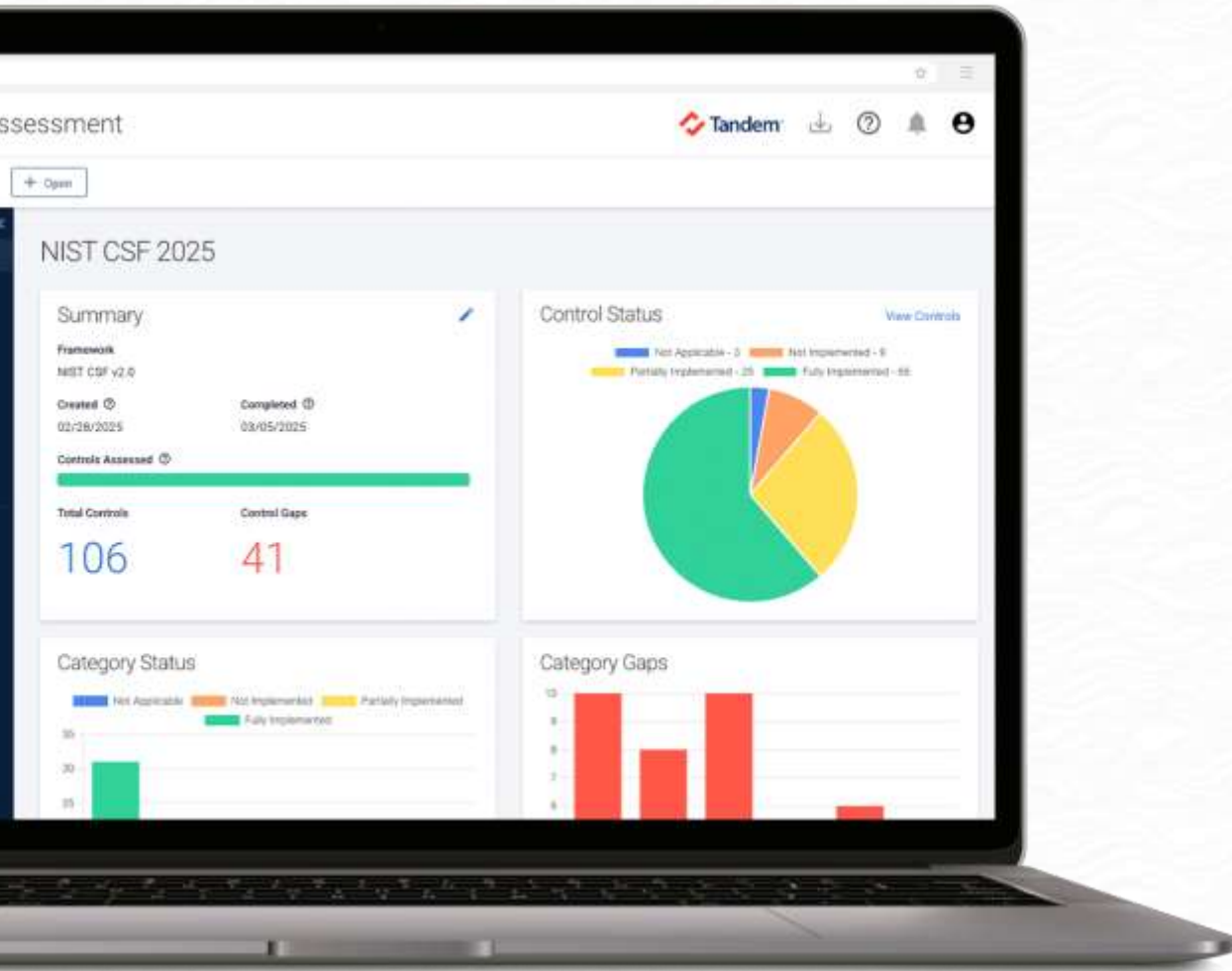
From CAT to CSF: A Strategic Conversation for Financial Institutions



Tuesday, September 30
2:00 PM (CT)

TANDEM.APP/WEBINARS





LEARN MORE

Tandem Cybersecurity Assessment Software

Tandem.App/Cybersecurity



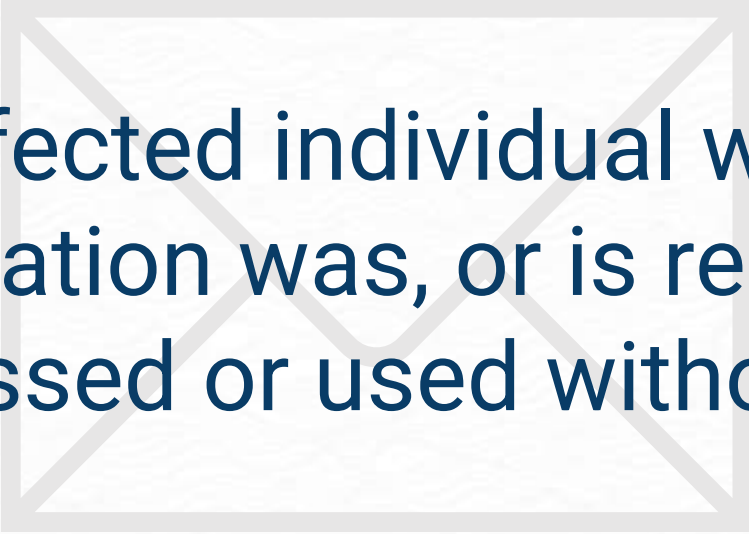
KEY TAKEAWAY

An incident response program provides a playbook for minimizing damage and safeguarding customer trust.

**SUBMIT YOUR
QUESTIONS!**

REGULATORY REQUIREMENTS

Customer Notice



Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

“(iii) Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with paragraph (a)(4) of this section unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.”

“Any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.”

EXAMPLE A

Identifiers used to authenticate identity

(e.g., social security number, government ID, passport, biometric info, telecommunication identifying information)

EXAMPLE B

Account-related information

(e.g., name, account number, username, combined with authentication info like passwords, security questions, credit card details, date of birth)

Substantial Harm or Inconvenience

“The Commission proposed to define “substantial harm or inconvenience” to mean all personal injuries, as well as instances of financial loss, expenditure of effort, or loss of time when they are “more than trivial,” with the proposal also providing a non-exhaustive list of examples of included harms or inconveniences. [...] After considering comments, and as discussed further below, we have determined not to define the term “substantial harm or inconvenience” in the final amendments.”

CUSTOMER NOTICE | SUBSTANTIAL HARM OR INCONVENIENCE



Theft or Fraud



Damaged Reputation



Harassment or Intimidation



Impaired Credit Eligibility



Physical Harm



Misuse of Information to Obtain
Financial Products or Services



Impersonation



Unauthorized Access to or
Transactions on Customer Accounts

Customer notice is not required if:

EXCEPTION 1



Reasonable Investigation

shows the data has not been and is not likely to be misused in a way that causes harm or inconvenience.

EXCEPTION 2



Reasonable Determination

shows that a specific individual's data was not accessed or used without authorization.

“(iii) Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with paragraph (a)(4) of this section unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.”

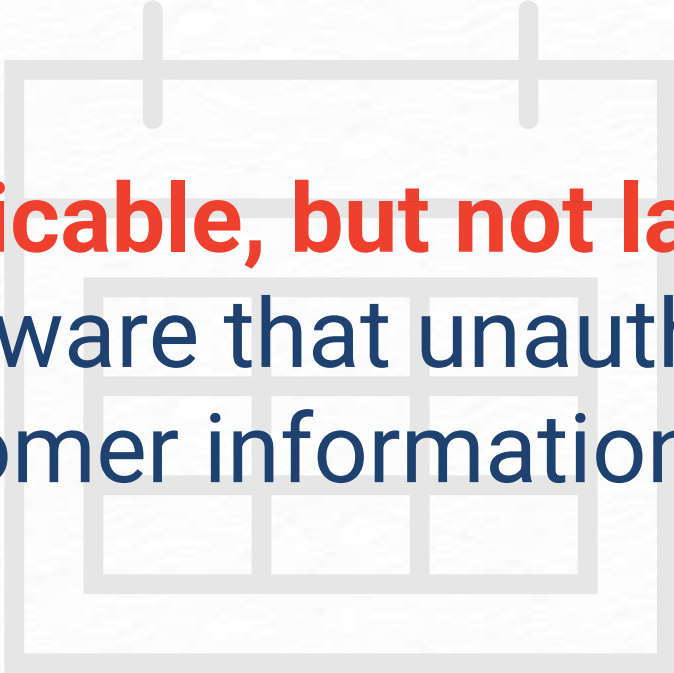
“Notwithstanding the foregoing, if the covered institution reasonably determines that a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization, the covered institution is not required to provide notice to that individual under this paragraph.”

Why did this happen?

A cybercriminal accessed our computer system without our permission.

What is ██████ doing?

We investigated and called law enforcement. We are also making our computer systems even stronger than before. We do not want this to happen again.



As soon as practicable, but not later than 30 days,
after becoming aware that unauthorized access to
or use of customer information has occurred.

“A covered institution must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred unless the United States Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, in which case the covered institution may delay providing such notice for a time period specified by the Attorney General, up to 30 days following the date when such notice was otherwise required to be provided. The notice may be delayed for an additional period of up to 30 days if the Attorney General determines that the notice continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, notice required under this section may be delayed for a final additional period of up to 60 days if the Attorney General determines that such notice continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph (a)(4)(iii), if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such delay through Commission exemptive order or other action.”

“In Writing”



Physical



Electronic *

“Notifying affected individuals of unauthorized access or use –(i) Notification obligation. Unless a covered institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information that occurred at the covered institution or one of its service providers that is not itself a covered institution, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience, the covered institution must provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.”

* “This requirement to provide notice “in writing” could be satisfied either through paper or, for customers who agree to receive information electronically, though electronic means consistent with existing Commission guidance on electronic delivery of documents.”



Incident Details



Timing



Contact Info



Guidance for Affected Individuals

HOW TO

- Review account statements
- Report suspicious activity
- Place a fraud alert
- Remove fraud from credit reports
- Obtain a free credit report
- Protect against identity theft
- Report identity theft to the FTC

"Notice contents. The notice must: (A) Describe in general terms the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization; (B) Include, if the information is reasonably possible to determine at the time the notice is provided, any of the following: the date of the incident, the estimated date of the incident, or the date range within which the incident occurred; (C) Include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including the following: a telephone number (which should be a toll-free number if available), an email address or equivalent method or means, a postal address, and the name of a specific office to contact for further information and assistance; (D) If the individual has an account with the covered institution, recommend that the customer review account statements and immediately report any suspicious activity to the covered institution; (E) Explain what a fraud alert is and how an individual may place a fraud alert in the individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft; (F) Recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted; (G) Explain how the individual may obtain a credit report free of charge; and (H) Include information about the availability of online guidance from the Federal Trade Commission and [usa.gov](https://www.usa.gov) regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the Federal Trade Commission, and include the Federal Trade Commission's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft."

[Name of Company]

NOTICE OF DATA BREACH

Dear [Insert Name],
We are contacting you because a data breach has occurred at [insert name of company].

What Happened?

[Describe how the data breach occurred, the date of the breach, and the information that has been exposed.]

What Information Was Exposed?

This incident involved the exposure of personal information, including [insert list of information exposed] due to the breach.

What We Are Doing

[Describe how you are addressing the breach, including: steps you are taking to remedy the situation, steps you are taking to protect information that has been breached, and any other steps you are offering (like credit monitoring or identity restoration services).]

DATA BREACH RESPONSE

A Guide for Business

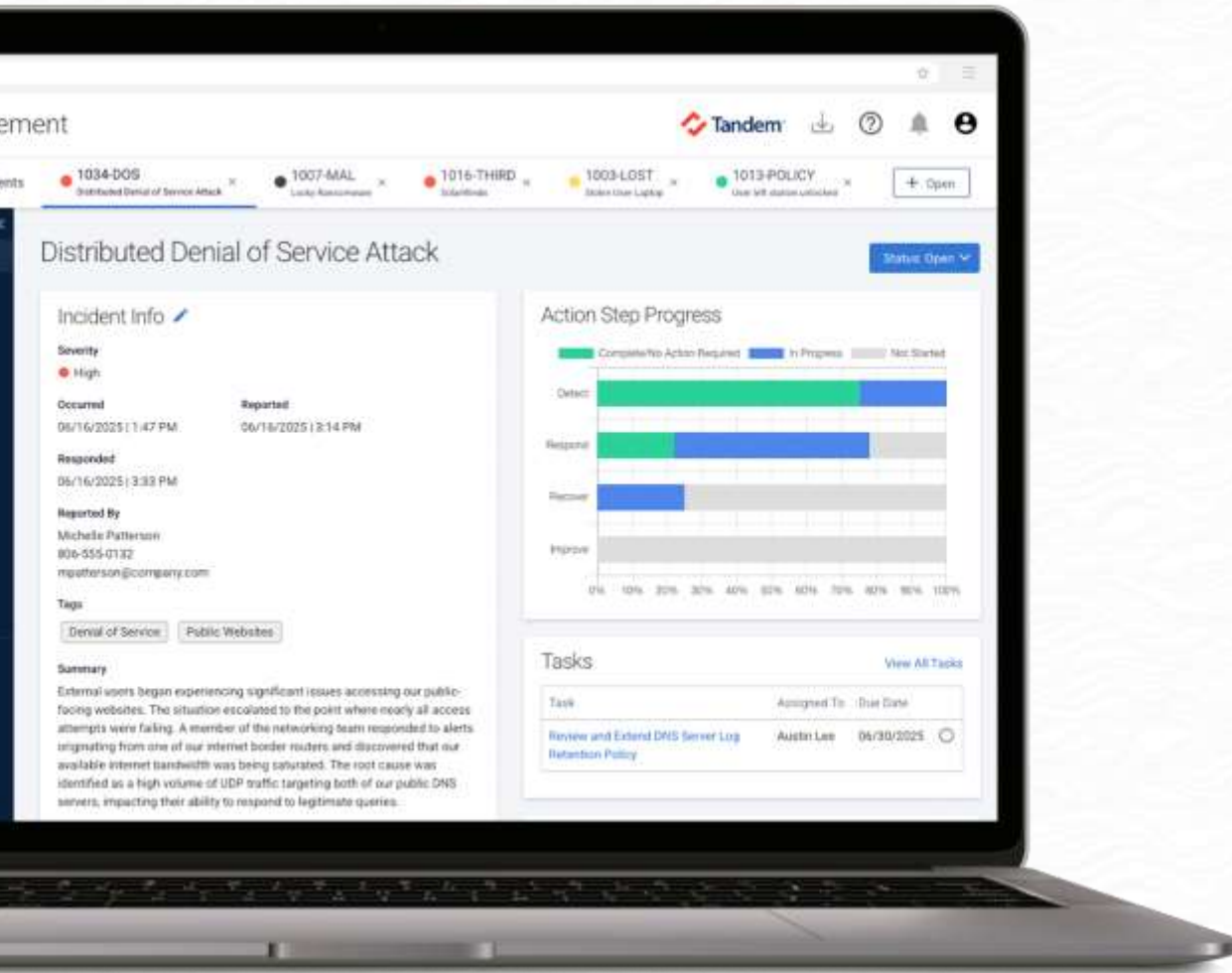


Federal Trade Commission | business.ftc.gov

FREE RESOURCE

Data Breach Response: A Guide for Business

[FTC.gov/business-guidance/resources/
data-breach-response-guide-business](https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business)



LEARN MORE

Tandem Incident Management Software

Tandem.App/Incident-Management-Software



KEY TAKEAWAY

Timely and thorough notice gives customers the information they need to respond and protect themselves after a breach.

**SUBMIT YOUR
QUESTIONS!**

REGULATORY REQUIREMENTS

Service Providers



“Written policies and procedures reasonably designed to require oversight, including through due diligence on and monitoring, of service providers.”

“(5) *Service providers.* (i) A covered institution's response program prepared in accordance with paragraph (a)(3) of this section must include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4) of this section.”

Does your organization have a vendor management program?



“**Any person or entity** that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.”



Service providers must protect against unauthorized access to or use of customer information.



Service providers must notify you ASAP, but no later than 72 hours after becoming aware of a security breach.

“The policies and procedures must be reasonably designed to ensure service providers take appropriate measures to:

(A) Protect against unauthorized access to or use of customer information; and

(B) Provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider. Upon receipt of such notification, the covered institution must initiate its incident response program adopted pursuant to paragraph (a)(3) of this section.”

Q: If a service provider experiences an incident that breaches customer data, can they just notify affected individuals?

A: Yes, but only if you agree to it in writing and maintain a record of the contract. Even then, you're still liable for ensuring the notice is provided.

1

Make a list of your “data critical” vendors.

2

Ensure your agreement has a security clause.

3

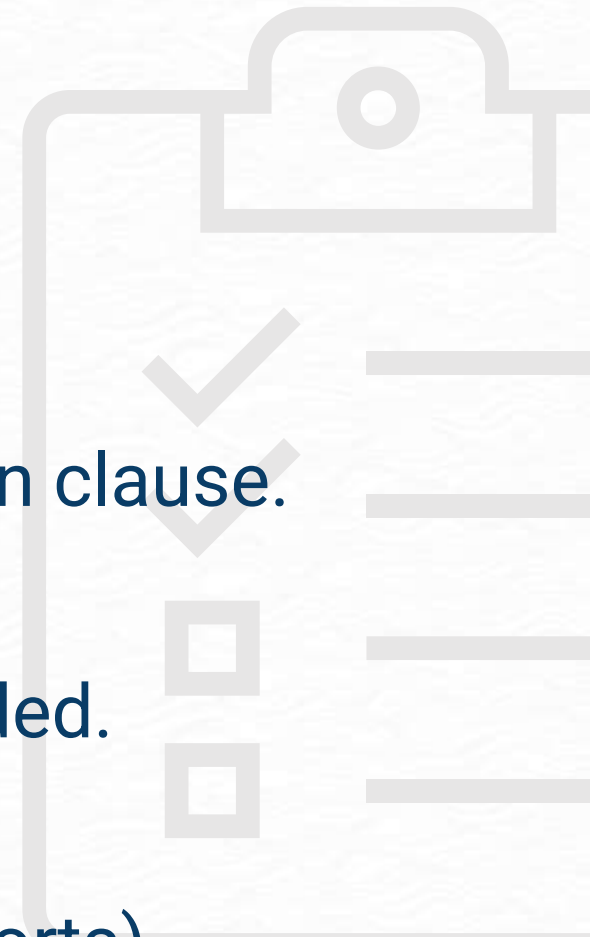
Ensure your agreement has incident notification clause.

4

Negotiate an amendment or addendum, if needed.

5

Ask for proof of security testing (e.g., SOC Reports).



Risk Assessment

GUIDANCE

"Each of us should complete a risk assessment prior to engaging in a third party relationship to assess and understand the risks. If any will be required to safety and soundly participate, risk assessments are a key step in the process, and should be a key part of a broader risk management strategy."

ACMA Supervisory Letter 07/01

"The actual conducting risk assessments for each third party relationship is up to the discretion of what the risks have changed over time and to update the management practices accordingly."

Prudential Guidance on Third-Party Relationships and Management

Governance & Structure

A vendor management



Best practice

1. Identify
2. Assess
3. Monitor
4. Review

Vendors vs. Third Parties

There are several terms often used in business agreements with an external party using the terms as follows:

Third Party
Any business arrangement between a business entity by contract or otherwise.

Vendor
A subset of a third party including entities with whom the business has a contract or other relationship.

Third Party Service Provider
A subset of vendors who provide services to the business.

While it is a best practice to have an internal policy (relationship), the term "third party" relationship which need to be managed by the business.

For example, here are some third parties that would likely not need to be managed by the business:

- Regulation
- Emergency Services
- Law Enforcement

That said, here are some examples of vendor management programs:

- Contracted Services
- Consultants
- Relational arrangements



Responsibility of a vendor

Can be shared with the business

As a vendor manages, outsourced relationships should be managed by the business.

BY THE NUMBERS

We asked you what you would do if you were a vendor. Here's what you said:

- Centralized - Most
- Centralized - Many
- Decentralized - Many
- Decentralized - Most
- Centralized - Many

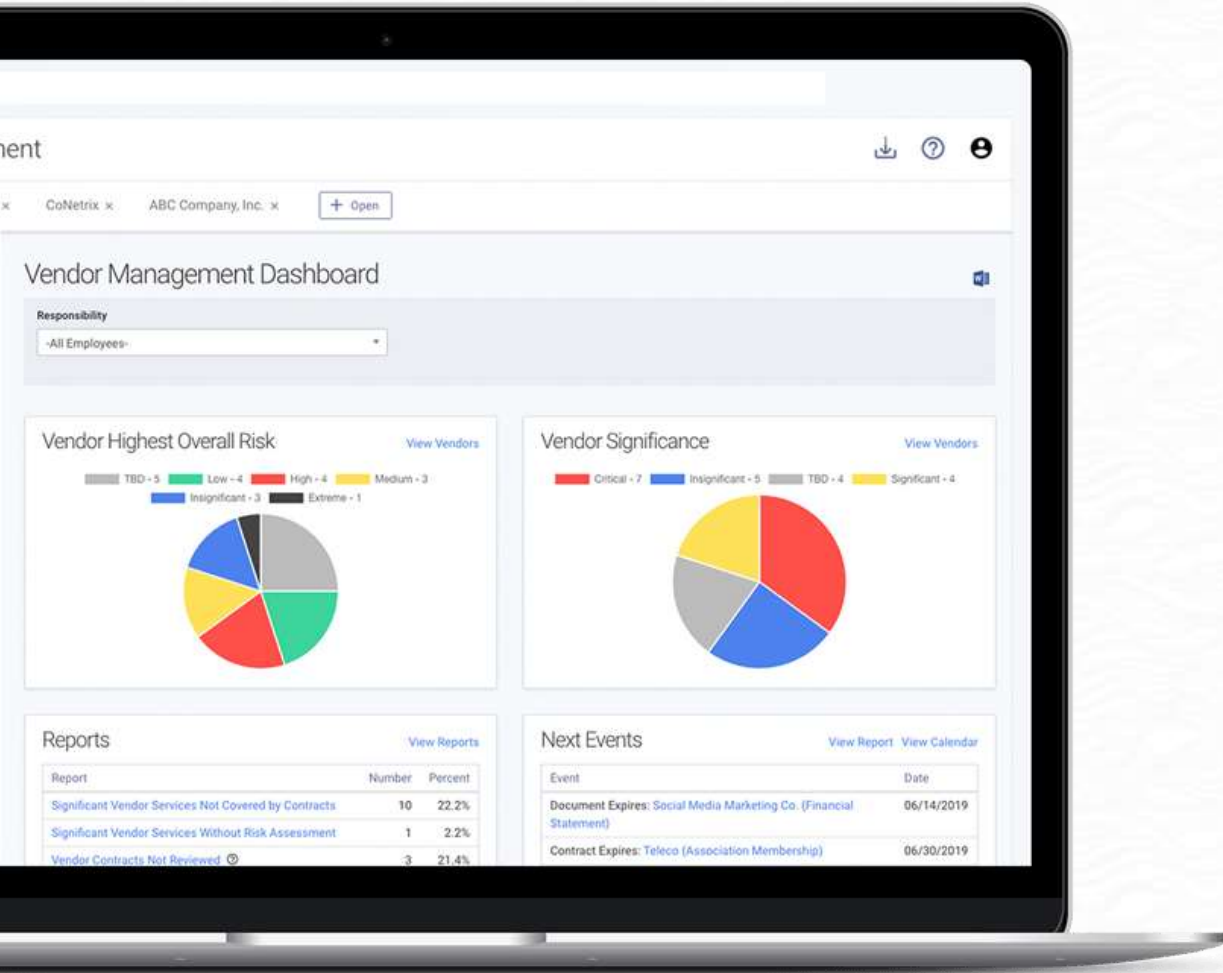
SOURCE: Tandem by the Numbers 2018



FREE RESOURCE

Vendor Management Workbook

Tandem.App/Vendor-Management-Workbook



LEARN MORE

Tandem Vendor Management Software

Tandem.App/Vendor-Management-Software



KEY TAKEAWAY

Outsourcing shifts control,
but not accountability.
Third-party oversight is key
to protecting customer data.

**SUBMIT YOUR
QUESTIONS!**

REGULATORY REQUIREMENTS

Records Retention and Destruction

Does your organization have a data retention and destruction policy?

RETENTION REQUIREMENTS

Covered Institution	Records Type	Retention Period	Easily Accessible?
Investment Companies	Policies & Procedures	Six Years	Yes
	All Other Records	Six Years	Just the first two years
Registered Investment Advisers	All Records	Five Years	Just the first two years
Broker-Dealers	All Records	Three Years	Yes
Transfer Agents	All Records	Three Years	Yes



Properly dispose of customer information.

“(b) Disposal of consumer information and customer information –(1) Standard. Every covered institution, other than notice-registered broker-dealers, must properly dispose of consumer information and customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(2) Written policies, procedures, and records. Every covered institution, other than notice-registered broker-dealers, must adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information according to the standard identified in paragraph (b)(1) of this section.”

KEY TAKEAWAYS

Retention shows your work when you need it.

Secure destruction helps keep data out of the wrong hands.

**SUBMIT YOUR
QUESTIONS!**

Wrap Up & Bonus Content

REGULATORY RESOURCES

- [17 CFR Part 248 Subpart A – Regulation S-P](#)
- [Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information](#)

ADDITIONAL RESOURCES

- [How to Write an AI Policy Webinar Recording](#)
- [Data Breach Response: A Guide for Businesses](#)
- [Vendor Management Workbook](#)
- [Tandem Blog: Regulation S-P Overview](#)

TANDEM PRODUCTS

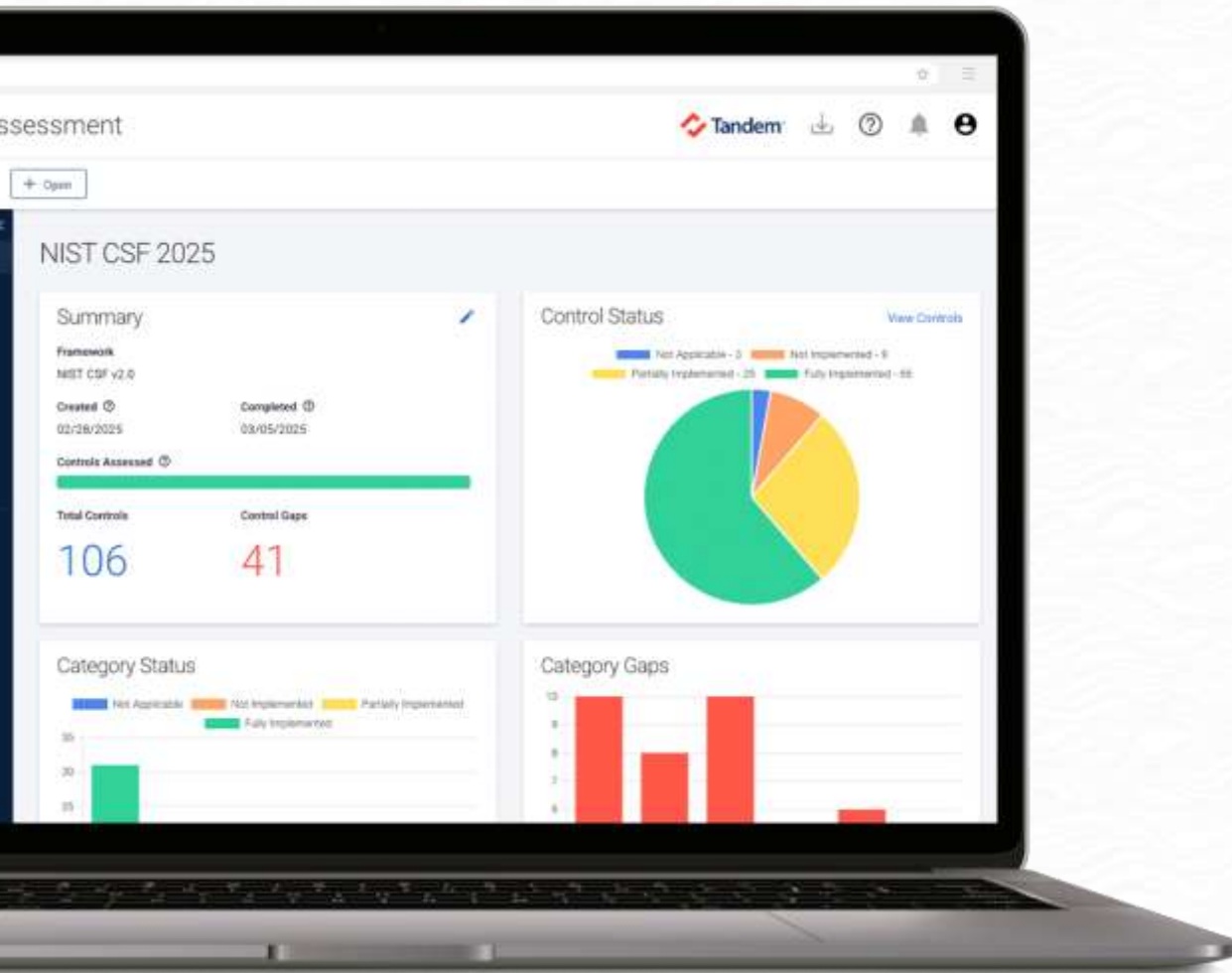
- [Tandem Cybersecurity Assessment](#)
- [Tandem Incident Management](#)
- [Tandem Policies](#)
- [Tandem Vendor Management](#)



The slides, recording, and certificate of attendance will be sent after the session.

Fill out the survey for a chance to win.



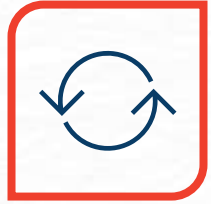


LEARN MORE

Information Security & Compliance Software

Tandem.App





Software Updates



Dedicated Support Team



Knowledge Base



Partner Program



Training Video Library



Annual Conference



Watch a Video

[Tandem.App/Demos](https://tandem.app/demos)



Fill Out the Survey

After the Session



Sign Up for Free

[Tandem.App/Cybersecurity](https://tandem.app/cybersecurity)

THANKS FOR JOINING

Regulation S-P: How to Comply with the New Amendments

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

Remember to complete the survey