WELCOME TO

A Banker's Guide to Understanding the New Incident Notification Rule

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

Tandem

1

Disclaimer

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **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.

Tandem

2

Presentation Information

Audio
If you do not hear audio,
turn up the volume on your device.

Questions
Submit via GoToWebinar

Resources
A link to the recording
and slides will be sent via email.

Tandem

3

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

Tandem™
A CoNetrix company

Tandem

4

PRESENTER

Alyssa Pugh, CISM, Security+

GRC Content Manager

Tandem

Tandem

5

Agenda

1. About the Rule
2. Bank to Regulator Notice
3. Service Provider to Bank Notice
4. Tandem Features & Updates

- Requirements
- Definitions
- Estimated Impact
- Preparing to Comply

Tandem

6

66424 Federal Register / Vol. 86, No. 223 / Tuesday, November 23, 2021 / Rules and Regulations

Signed in Washington, DC, on November 18, 2021.

Treena V. Garrett,

Federal Register Liaison Officer, U.S. Department of Energy.

[FR Doc. 2021–25537 Filed 11–22–21; 8:45 am]

BILLING CODE 6450–01–P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 53

[Docket ID OCC–2020–0038]

RIN 1557–AF02

FEDERAL RESERVE SYSTEM

12 CFR Part 225

[Docket No. R–1736]

RIN 7100–AG06

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 304

RIN 3064–AF59

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

AGENCY: The Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC).

ACTION: Final rule.

SUMMARY: The OCC, Board, and FDIC are issuing a final rule that requires a banking organization to notify its primary Federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

DATES: Effective date: April 1, 2022; Compliance date: May 1, 2022.

FOR FURTHER INFORMATION CONTACT:

OCC: Patrick Kelly, Director, Critical Infrastructure Policy, (202) 649–5519, Carl Kaminski, Assistant Director, (202) 649–5490, or Priscilla Benner, Senior Attorney, Chief Counsel's Office, (202) 649–5490, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219.

Board: Thomas Sullivan, Senior Associate Director, (202) 475–7656; Julia Philipp, Lead Financial Institution Cybersecurity Policy Analyst, (202) 452–3940, Don Peterson, Supervisory Cybersecurity Analyst, (202) 973–5058, Systems and Operational Resiliency Policy, of the Supervision and Regulation Division; Jay Schwarz, Assistant General Counsel, (202) 452–2970, Claudia Von Pervieux, Senior Counsel (202) 452–2552, Christopher Danello, Senior Attorney, (202) 736–1960, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551, or *https://www.federalreserve.gov/apps/ContactUs/feedback.aspx*, and click on *Staff Group, Regulations.*

FDIC: Rob Drozdowski, Special Assistant to the Deputy Director (202) 898–3971, *rdrozdowski@fdic.gov*, Division of Risk Management Supervision; or John Dorsey, Counsel (202) 898–3807, *jdorsey@fdic.gov*, Graham Rehrig, Senior Attorney, (202) 898–3829, *grehrig@fdic.gov*, Legal Division.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

The OCC, Board, and FDIC (together, the agencies) are issuing a final rule to require that a banking organization [1] promptly notify its primary Federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as those terms are defined in the final rule. As described in more detail below, these incidents may have many causes. Examples include a large-scale distributed denial of service attack that disrupts customer account access for an extended period of time and a computer hacking incident that disables banking operations for an extended period of time.

Under the final rule, a banking organization's primary Federal regulator must receive this notification as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. This requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system. This early awareness will help the agencies react to these threats before they become systemic. The final rule separately requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines it has experienced a computer-security incident that has caused, or is reasonably likely to cause,

[1] For the OCC, "banking organizations" includes national banks, Federal savings associations, and Federal branches and agencies of foreign banks. For the Board, "banking organizations" includes all U.S. bank holding companies and savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; and Edge and agreement corporations. For the FDIC, "banking organizations" includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations. Each agency's definition excludes financial market utilities (FMUs) designated under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (designated FMUs).

FINAL RULE

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank

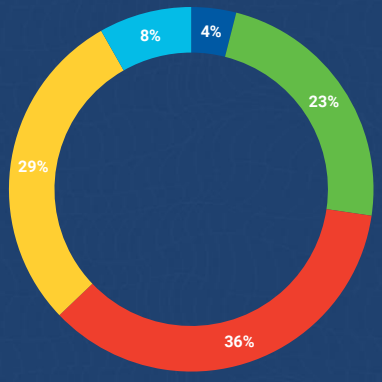
- **FDIC:** 12 CFR Part 304 Subpart C
- **FRB:** 12 CFR Part 225 Subpart N
- **OCC:** 12 CFR Part 53

Tandem

7

Poll

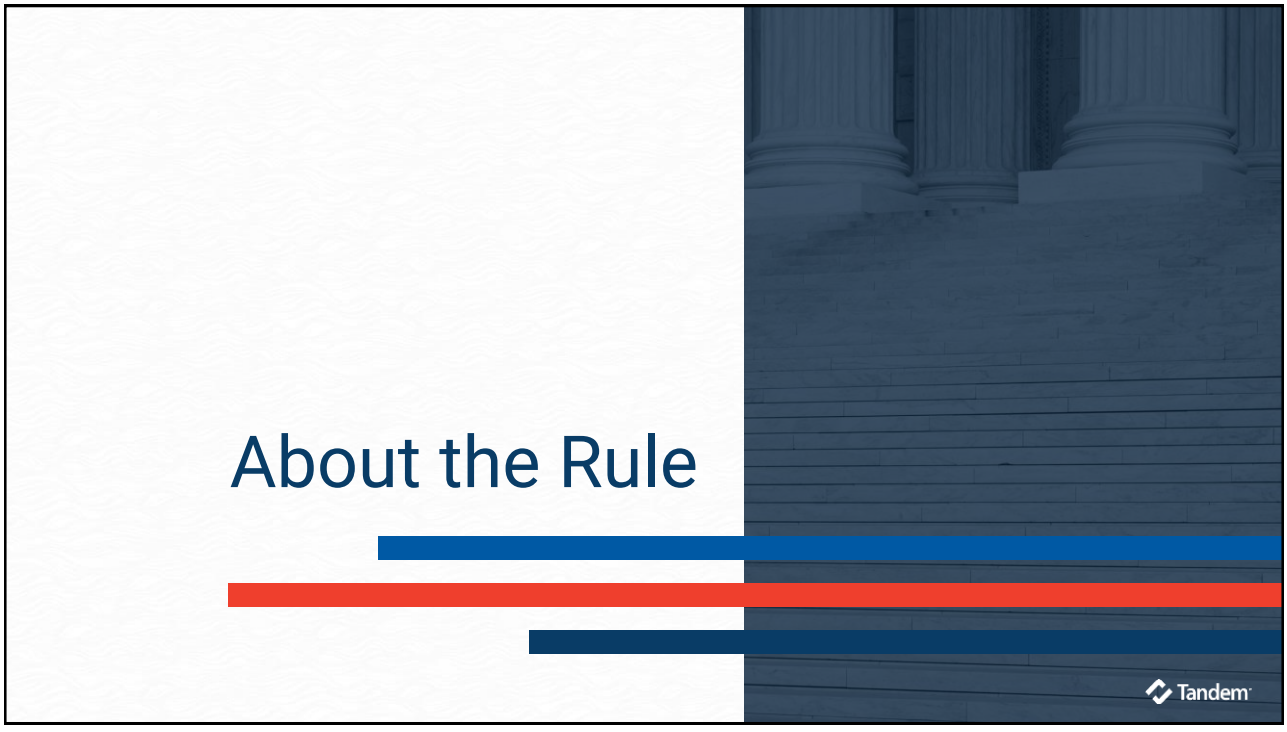
How familiar are you with the new Incident Notification Rule?



- I'm pretty much an expert.
- I read through it once.
- I skimmed it, but didn't dive in.
- I read the title. Does that count?
- What rule?

Tandem

8



9

Timeline

KEYS CONFERENCE
Tandem.App/KEYS

01/12/2021
Proposed Rule Published Date

11/23/2021
Final Rule Published Date

04/01/2022
Final Rule Effective Date

12/18/2020
Agencies Announce Proposed Rule

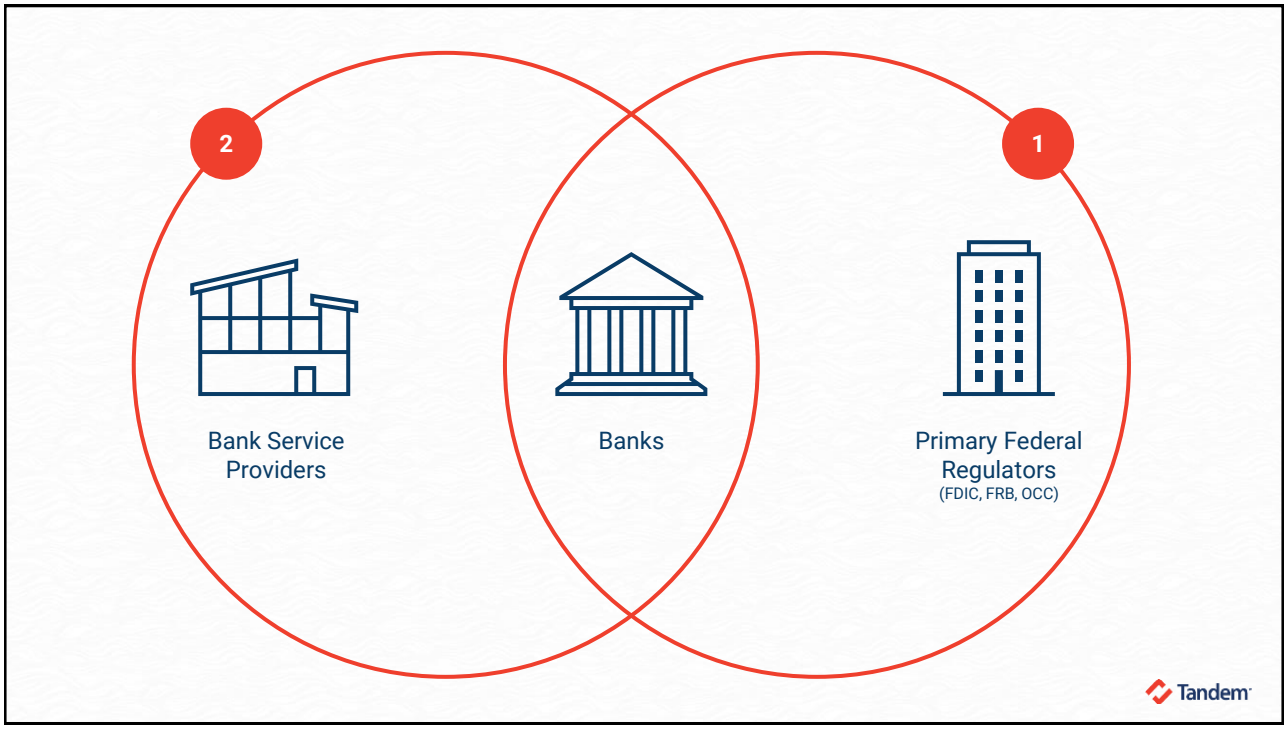
04/12/2021
Comments Closed Date

02/01/2022
You Are Here

05/01/2022
Mandatory Compliance Date

Tandem

10



11

FFIEC INFORMATION TECHNOLOGY EXAMINATION HANDBOOK

MGT

Develop a policy for escalating and reporting security incidents to the board, government agencies, law enforcement, and the institution's **primary federal and state regulator** based on thresholds defined by the financial institution and applicable legal requirements.

https://ithandbook.ffiec.gov/it-booklets/management/iii-it-risk-management/iiic-risk-mitigation/iiic3-information-security.aspx

IS

Primary considerations for incident response include the following: […] How, when, and what to communicate outside of the institution, whether to law enforcement, **regulatory agencies**, information-sharing organizations, customers, third-party service providers, potential victims, or others.

https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiid-incident-response.aspx

BCM

Incident response priorities include preservation of life, preservation of property, incident stabilization, and communicating with stakeholders (e.g., impacted personnel, third-party service providers, customers, **regulators**, law enforcement). […] The incident response team should coordinate communication with the noted stakeholders.

https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/v-business-continuity-plan/vf-other-components/vf1-incident-response.aspx

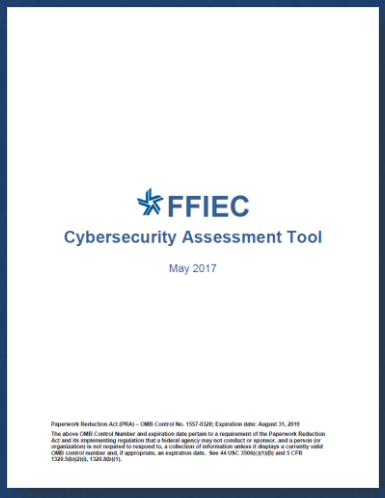
AIO

Management should implement processes to plan for and manage events, incidents, and problems. These processes should include the following: […] Maintaining contact information for individuals and groups (e.g., **regulators**, law enforcement, internal public relations, and affected lines of business) who should be notified and the circumstances under which they should be notified.

https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/vi-operations/vic-service-and-support-processes/vic4-event,-incident,-and-problem-management.aspx

Tandem

12



https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf

BASELINE

1. Contact information for law enforcement and the **regulator(s)** is maintained and updated regularly.
2. Information about threats is shared with law enforcement and **regulators** when required or prompted.
3. Procedures exist to notify customers, **regulators**, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information.

EVOLVING

4. **Regulators**, law enforcement, and service providers, as appropriate, are notified when the institution is aware of any unauthorized access to systems or a cyber incident occurs that could result in degradation of services.

INTERMEDIATE

5. Information is shared proactively with the industry, law enforcement, **regulators**, and information-sharing forums.

Tandem

13

PRESCRIPTIVE
Prescribes what should be done.
(Guidance)

OR

DESCRIPTIVE
Details what you have to do.
(Rules)

Tandem

14

FRAUD

FINAL RULE (1996)

Suspicious Activity Reports

- **FDIC:** 12 CFR Part 353
- **FRB:** 12 CFR Part 208 Subpart F
- **OCC:** 12 CFR Part 21 Subpart B

DATA BREACH

FINAL RULE (2005)

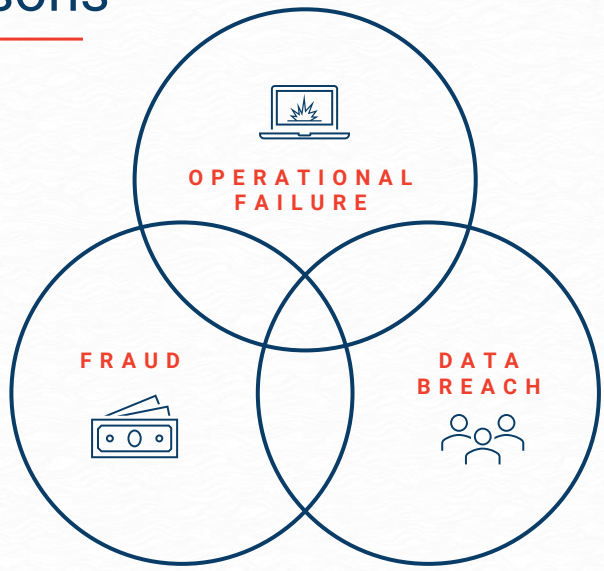
Interagency Guidance on Response Programs for Unauthorized Access […]

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

Tandem

15

Comparisons



Tandem

16

Why a New Rule?

https://www.federalregister.gov/d/2021-25510/p-52

Tandem

17

TAKEAWAY

A significant operational failure may have extensive impact, not just on your bank, but on the greater banking industry.

Tandem

18

Bank to Regulator Notice

Tandem

19

BANK TO REGULATOR | REQUIREMENTS

WHO?
Regulator-Designated Point of Contact

HOW?
Email, Telephone, or Similar Methods

WHEN?
ASAP and within 36 Hours

OF?
Determining a "Notification Incident" Occurred

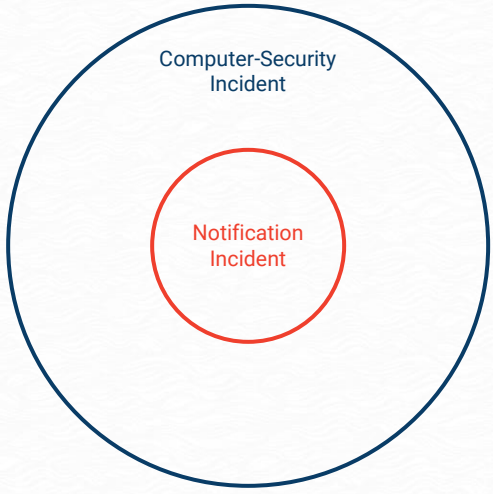
FINAL RULE

"A banking organization must notify the appropriate [FDIC/OCC supervisory office, or] Regulator-designated point of contact, about a notification incident through email, telephone, or similar methods that the Regulator may prescribe. The Regulator must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred."

Tandem

20

BANK TO REGULATOR | DEFINITIONS



Tandem

21

BANK TO REGULATOR | DEFINITIONS

FINAL RULE

~~NIST~~ **DEFINITION**

"A *computer-security incident* is an occurrence that results in actual ~~or potential~~ harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; ~~or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."~~

https://www.federalregister.gov/d/2021-25510/p-113

Tandem

22

BANK TO REGULATOR | DEFINITIONS

COMPUTER-SECURITY INCIDENT

"Actual Harm"

"Confidentiality, Integrity, and Availability"

"Information Systems or the Information"

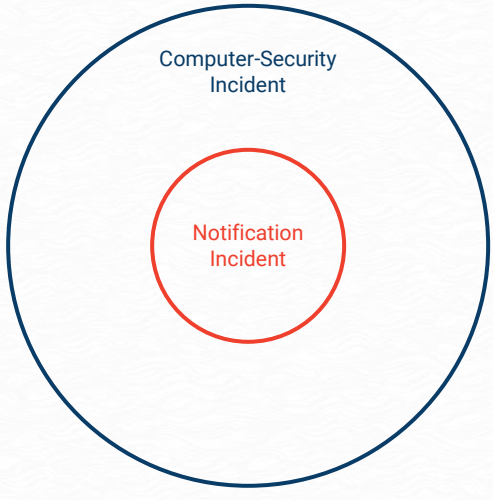
FINAL RULE

"*Computer-security incident* is an occurrence that results in actual harm to the confidentiality, integrity, and availability of an information system or the information that the system processes, stores, or transmits."

Tandem

23

BANK TO REGULATOR | DEFINITIONS



Tandem

24

BANK TO REGULATOR | DEFINITIONS

NOTIFICATION INCIDENT

"Computer-Security Incident"

+

1. Inability to operate - or - provide services to many customers.
2. Projected detrimental financial losses.
3. Possible impact to the financial stability of the U.S.

FINAL RULE

"*Notification incident* is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's – (i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."

Tandem

25

BANK TO REGULATOR | EXAMPLES OF NOTIFICATION INCIDENTS

1. **Large-scale** DDoS attack that disrupts **customer account access** for an **extended** time (e.g., 4+ hours).
2. **Core banking service provider** experiences **widespread** system outages with an **undeterminable** recovery time.
3. **Failed** system upgrade or change that results in **widespread** user outages.
4. **Unrecoverable** system failure that results in activation of a bank's BCP or DRP.
5. Computer hacking incident that **disables** banking operations for an **extended** time.
6. Malware that poses an **imminent** threat to the banks' **core business lines** or critical operations.
7. Ransomware attack that encrypts a **core banking system** or backup data.

"Consider, on a case-by-case basis, whether any significant computer-security incidents constitute notification incidents for purposes of notifying the appropriate agency."

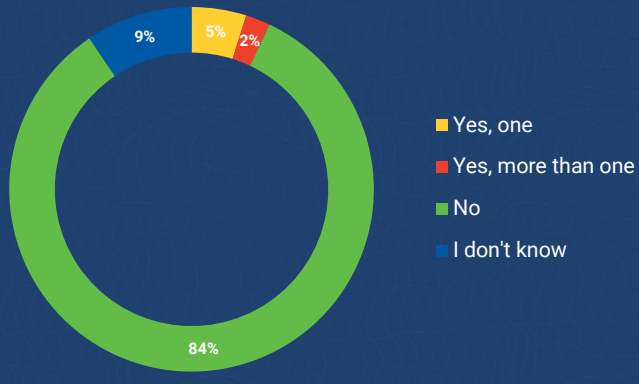
https://www.federalregister.gov/d/2021-25510/p-148

Tandem

26

Poll

Have you experienced a “notification incident” in the last year?



Tandem

27

BANK TO REGULATOR | ESTMATED IMPACT

What is the agencies’ estimated number of total annual notification incidents?

Estimated Percent of Banks which will experience a Notification Incident in 2022

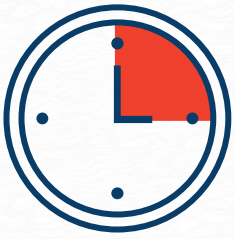
https://www.federalregister.gov/d/2021-25510/p-235

Tandem

28

BANK TO REGULATOR | ESTMATED IMPACT

3 HOURS



"Overall, the agencies expect the benefits of the final rule to outweigh its small costs."

https://www.federalregister.gov/d/2021-25510/p-241

Tandem

29

BANK TO REGULATOR | WHAT'S MISSING?

NOTICE REQUIREMENTS

"The notification is intended to serve as an early alert to a banking organization's primary federal regulator about a notification incident. The agencies anticipate that banking organizations will share general information about what is known at the time of the incident. No specific information is required in the notification other than that a notification incident has occurred. The final rule does not prescribe any form or template."

Do your best.

RESCINDING NOTICES

"A banking organization or bank service provider may update its original notification if it later determines that its initial assessments were incorrect or overcautious."

Accidents happen.

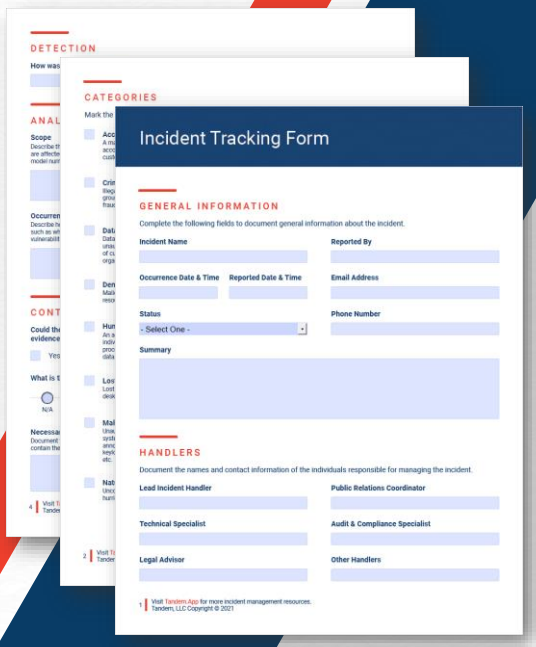
RECORDKEEPING REQUIREMENTS

"Other commenters discussed the need to obtain or retain copies of the notifications for recordkeeping purposes. The rule does not impose any recordkeeping requirements."

About that...

Tandem

30



FREE RESOURCE

Incident Tracking Form

Tandem.App/Incident-Tracking-Form

Tandem

31

POP QUIZ

True or False: A “computer-security incident” is the same thing as a “notification incident.”

A True

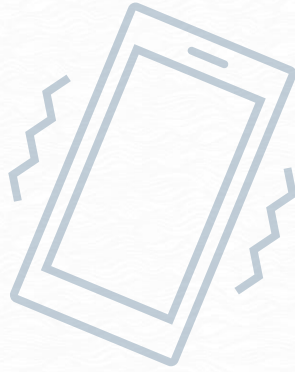
B False

Tandem

32

BANK TO REGULATOR | PREPARING TO COMPLY

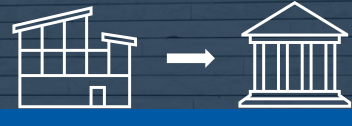
- [x] Identify your regulator contact.
- [x] Update your Incident Response Plan.
- [x] Review your Incident Management Policy.
- [x] Train your incident response team.



Tandem

33

Service Provider to Bank Notice



Tandem

34

SERVICE PROVIDER TO BANK REQUIREMENTS

WHO?
Bank Service Providers (subject to BSCA)

TO?
One Bank-Designated Point of Contact -or- CEO and CIO at Affected Banks

HOW?
Any Reasonable Means

WHEN?
ASAP

OF?
Bank Service Provider Incident

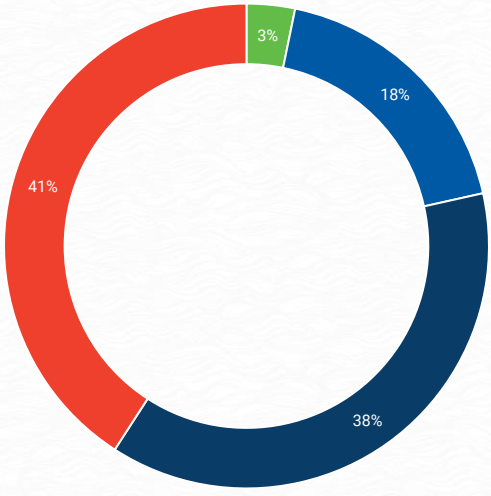
FINAL RULE

A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. (1) A bank-designated point of contact is an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer. (2) If the banking organization customer has not previously provided a bank designated point of contact, such notification shall be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

Tandem

35

SERVICE PROVIDER TO BANK DEFINITIONS



How familiar are you with the Bank Service Company Act (BSCA)?

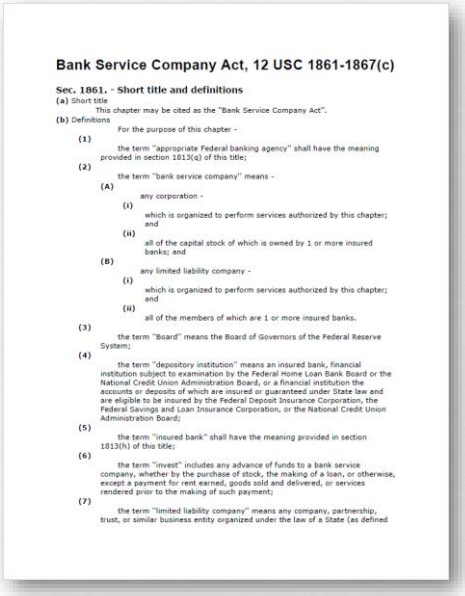
- Very
- Somewhat
- Slightly
- Not at All

Source: Third-Party Incident Handling | Tandem Webinar Poll (04/20/2021)

Tandem

36

SERVICE PROVIDER TO BANK | DEFINITIONS



Bank Service Company Act, 12 USC 1861-1867(c)

Sec. 1861. - Short title and definitions

(a) Short title

This chapter may be cited as the "Bank Service Company Act".

(b) Definitions

For the purpose of this chapter -

(1)

the term "appropriate Federal banking agency" shall have the meaning provided in section 1813(q) of this title;

(2)

the term "bank service company" means -

(A)

any corporation -

(i)

which is organized to perform services authorized by this chapter; and

(ii)

all of the capital stock of which is owned by 1 or more insured banks; and

(B)

any limited liability company -

(i)

which is organized to perform services authorized by this chapter; and

(ii)

all of the members of which are 1 or more insured banks.

(3)

the term "Board" means the Board of Governors of the Federal Reserve System;

(4)

the term "depository institution" means an insured bank, financial institution subject to examination by the Federal Home Loan Bank Board or the National Credit Union Administration Board, or a financial institution the accounts or deposits of which are insured or guaranteed under State law and are eligible to be insured by the Federal Deposit Insurance Corporation, the Federal Savings and Loan Insurance Corporation, or the National Credit Union Administration Board;

(5)

the term "insured bank" shall have the meaning provided in section 1813(h) of this title;

(6)

the term "invest" includes any advance of funds to a bank service company, whether by the purchase of stock, the making of a loan, or otherwise, except a payment for rent earned, goods sold and delivered, or services rendered prior to the making of such payment;

(7)

the term "limited liability company" means any company, partnership, trust, or similar business entity organized under the law of a State (as defined

FINAL RULE

Bank Service Company Act

https://ithandbook.ffiec.gov/media/resources/3238/con-12usc1861_1867c_bank_service_company_act.pdf

12 USC 1861-1867(c)

Tandem

37

SERVICE PROVIDER TO BANK | DEFINITIONS

BANK SERVICE PROVIDER[1]

"Bank Service Company" [2]
(i.e., any corporation or LLC owned by banks)

OR

"Person" [3]
(i.e., individual, corporation, partnership, trust, association, etc.)

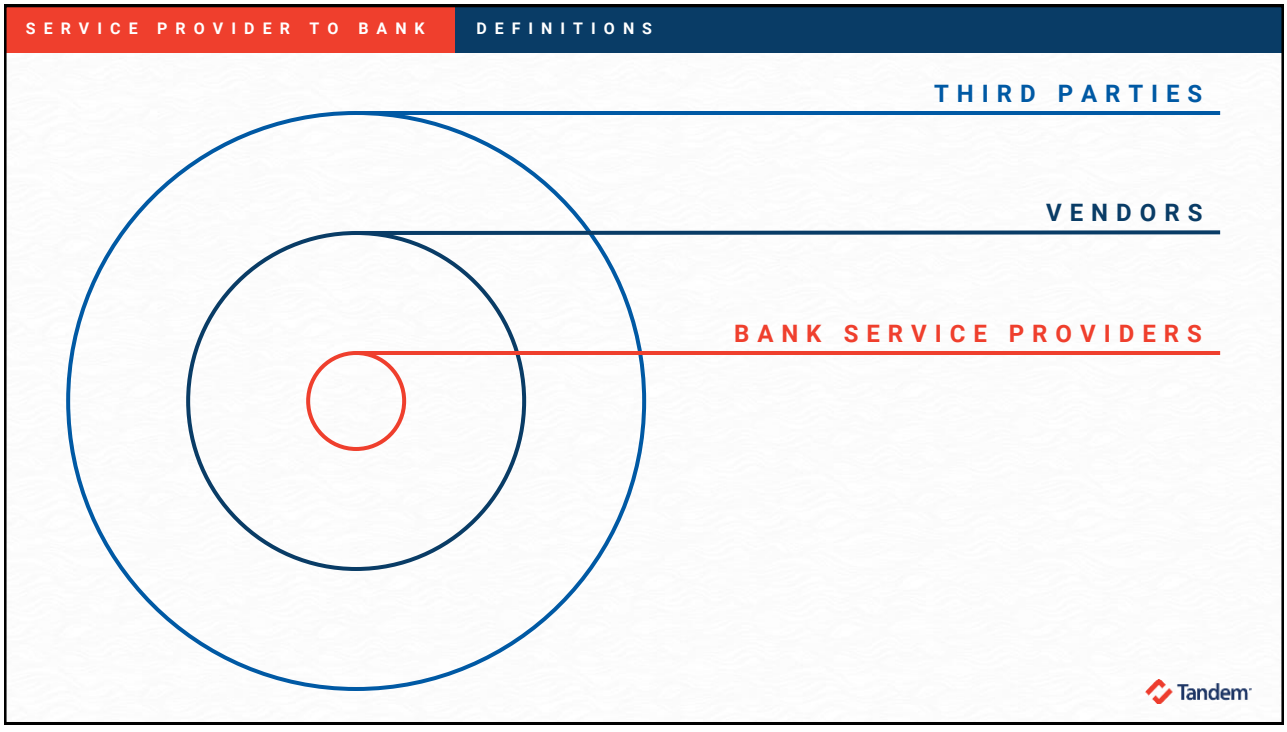
+

4

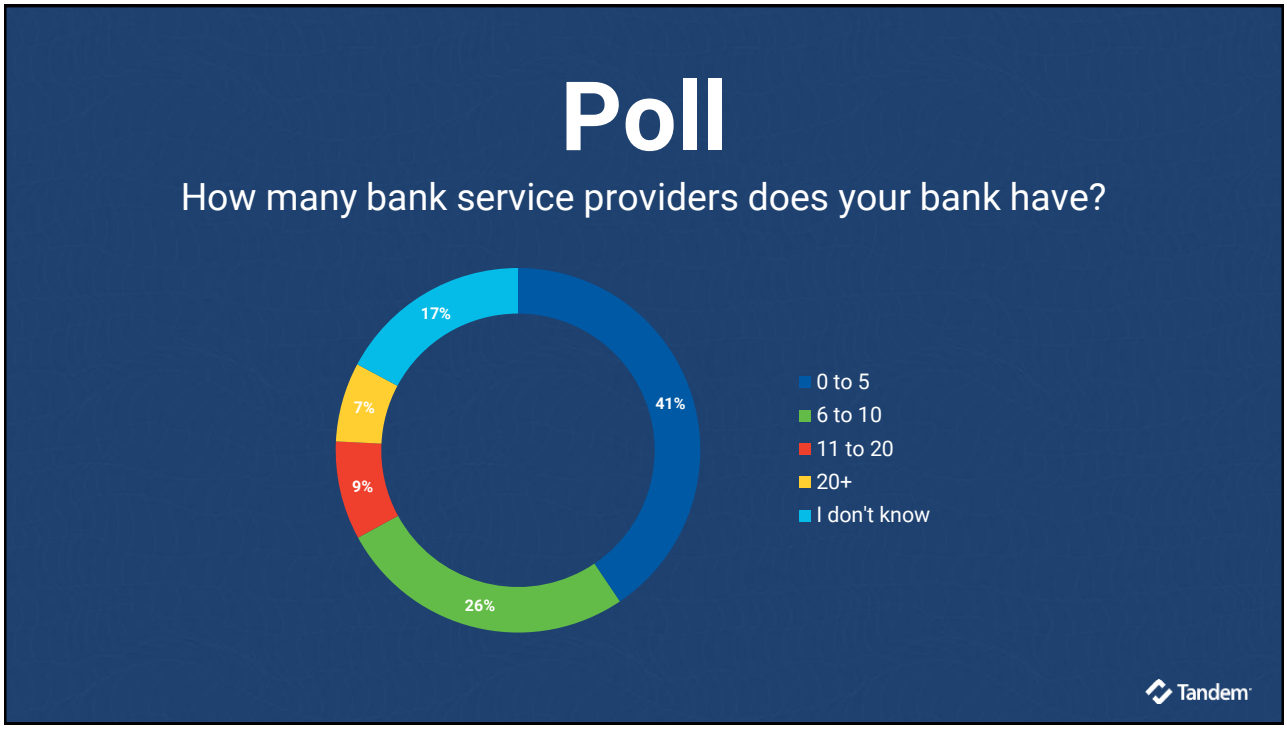
1. https://www.federalregister.gov/d/2021-25510/p-349
2. https://ithandbook.ffiec.gov/media/resources/3238/con-12usc1861_1867c_bank_service_company_act.pdf
3. https://uscode.house.gov/view.xhtml?req=(title:12%20section:1817%20edition:prelim)
4. https://www.fdic.gov/news/financial-institution-letters/2019/fil19019.html

Tandem

38


SERVICE PROVIDER TO BANK
DEFINITIONS
THIRD PARTIES
VENDORS
BANK SERVICE PROVIDERS
Tandem

39

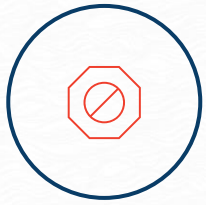

Poll
How many bank service providers does your bank have?
17%
41%
7%
9%
26%
0 to 5
6 to 10
11 to 20
20+
I don't know
Tandem

40

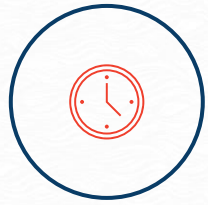
SERVICE PROVIDER TO BANK | DEFINITIONS

BANK SERVICE PROVIDER INCIDENT

"Computer-Security Incident"



"Disrupt or Degrade"



"Four or More Hours"

FINAL RULE

"A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours."

Tandem

41

WHY?

"Core banking service provider experiences widespread system outages with an undeterminable recovery time."

Tandem

42

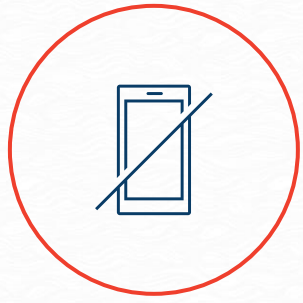
SERVICE PROVIDER TO BANK | DEFINITIONS

DO I HAVE TO UPDATE MY CONTRACTS?

PROBABLY NOT*

Contracts may already address the requirements.

Bank service providers must comply "regardless of current contract language."



Banks are generally not responsible for bank service provider failure to notify.

*BUT IT IS A GOOD IDEA.

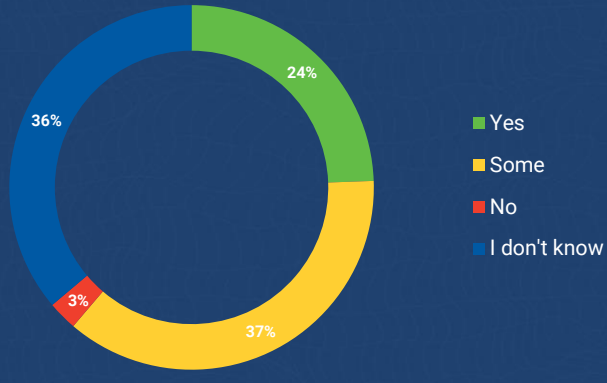
https://www.federalregister.gov/d/2021-25510/p-183

Tandem

43

Poll

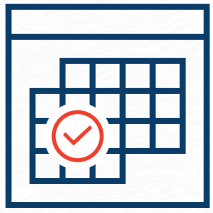
Do your contracts with bank service providers already address these provisions?



Tandem

44

SERVICE PROVIDER TO BANK | EXCEPTIONS



Scheduled Maintenance, Testing, or Software Updates

*Unless it exceeds communicated parameters and becomes an incident.

https://www.federalregister.gov/d/2021-25510/p-185

FINAL RULE

"The notification requirement in paragraph (a) of this section does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer."

Tandem

45

SERVICE PROVIDER TO BANK | ESTIMATED IMPACT

120K × **2%** = **2.4K**

NAICS Industry Code 5415 Computer System Design and Related Services

Estimated Annual Percent of Bank Service Providers with an Incident

Annual Bank Service Provider Incidents

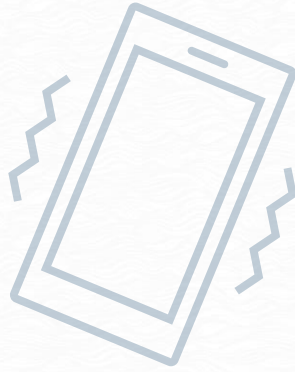
https://www.federalregister.gov/d/2021-25510/p-262

Tandem

46

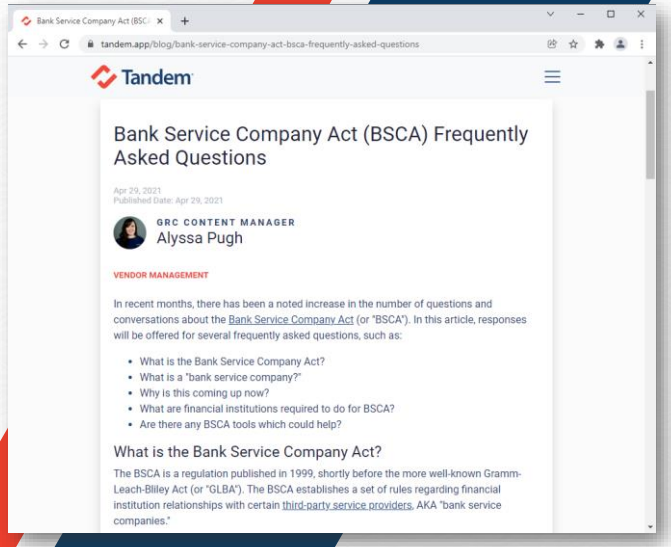
SERVICE PROVIDER TO BANK | PREPARING TO COMPLY

- Identify your bank service providers.
- Review your existing contracts.
- Review your vendor management program.
- Train your designated contacts.



Tandem

47



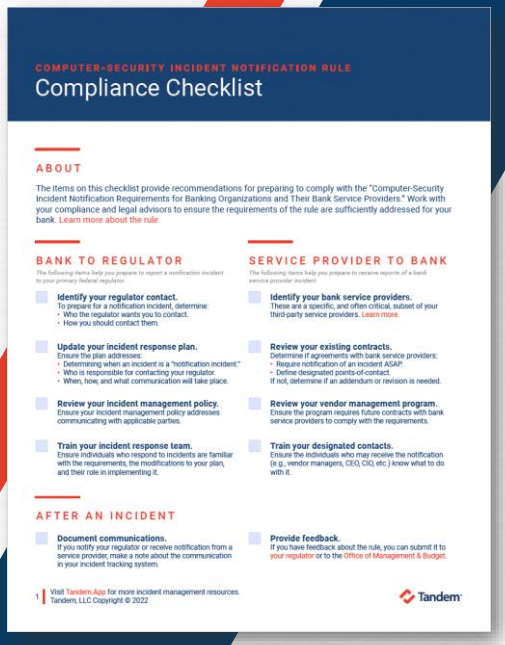
FREE RESOURCE

Bank Service Company Act (BSCA) Frequently Asked Questions

https://tandem.app/blog/bank-service-company-act-bsca-frequently-asked-questions

Tandem

48



FREE RESOURCE

Compliance Checklist

Tandem.App/Incident-Notification-Rule-Checklist

Tandem

49

SUBMIT FEEDBACK | PREPARING TO COMPLY

	FDIC	FRB	OCC
MAIL	James P. Sheesley, Asst. Executive Secretary Attention: Comments Federal Deposit Insurance Corporation 550 17th Street NW Washington, DC 20429	Ann E. Misback, Secretary Board of Governors of the Federal Reserve System 20th Street and Constitution Avenue NW Washington, DC 20551	Chief Counsel's Office Attention: Comment Processing Office of the Comptroller of the Currency 400 7th Street SW, Suite 3E-218 Washington, DC 20219
EMAIL	comments@fdic.gov	regs.comments@federalreserve.gov	N/A
FAX	N/A	202-452-3819 -or- 202-452-3102	N/A
DETAILS	Include "RIN 3064-AF59" in the subject line of your message.	Include "Docket No. R-1736 RIN 7100-AG06" in the subject line of your message.	Include "OCC" and "Docket ID OCC-2020-0038" in your comment.

Note: All comments will become a matter of public record.

Tandem

50

Tandem Features & Updates

Tandem

51

TANDEM FEATURES & UPDATES

Policies

Vendor Management

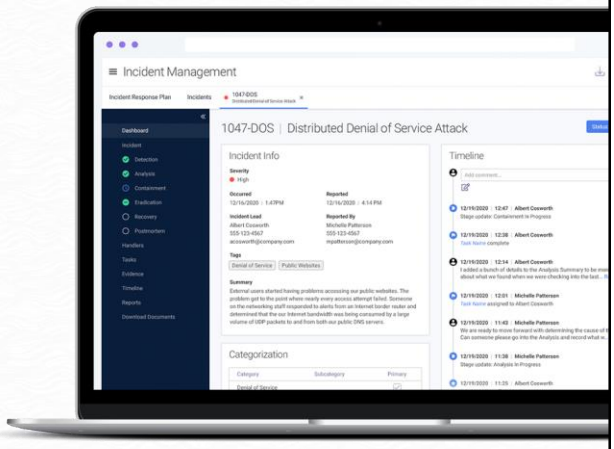
Incident Management

Tandem

52

RECENT TANDEM UPDATES

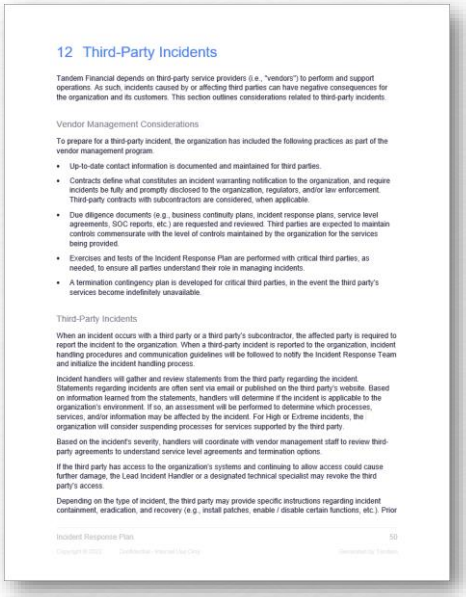
- Updated Incident Management Policy
- Updated Vendor Management Policy
- Updated Contract Review Template
- New BSCA Compliance Category
- Added New Terms to Glossary
- Updated Incident Handling Process: Analysis
- Updated Additional Documentation: Third-Party Communication



Tandem

53

EXISTING TANDEM FEATURES



12 Third-Party Incidents

Tandem Financial depends on third-party service providers (i.e., "vendors") to perform and support operations. As such, incidents caused by or affecting third parties can have negative consequences for the organization and its customers. This section outlines considerations related to third-party incidents.

Vendor Management Considerations

To prepare for a third-party incident, the organization has included the following practices as part of the vendor management program.

- Up-to-date contact information is documented and maintained for third parties.
- Contracts define what constitutes an incident warranting notification to the organization, and require incidents be fully and promptly disclosed to the organization, regulators, and/or law enforcement. Third-party contracts with subcontractors are considered, when applicable.
- Due diligence documents (e.g., business continuity plans, incident response plans, service level agreements, SOC reports, etc.) are requested and reviewed. Third parties are expected to maintain controls commensurate with the level of controls maintained by the organization for the services being provided.
- Exercises and tests of the Incident Response Plan are performed with critical third parties, as needed, to ensure all parties understand their role in managing incidents.
- A termination contingency plan is developed for critical third parties, in the event the third party's services become indefinitely unavailable.

Third-Party Incidents

When an incident occurs with a third party or a third party's subcontractor, the affected party is required to report the incident to the organization. When a third-party incident is reported to the organization, incident handling procedures and communication guidelines will be followed to notify the Incident Response Team and initialize the incident handling process.

Incident handlers will gather and review statements from the third party regarding the incident. Statements regarding incidents are often sent via email or published on the third party's website. Based on information learned from the statements, handlers will determine if the incident is applicable to the organization's environment. If so, an assessment will be performed to determine which processes, services, and/or information may be affected by the incident. For High or Extreme incidents, the organization will consider suspending processes for services supported by the third party.

Based on the incident's severity, handlers will coordinate with vendor management staff to review third-party agreements to understand service level agreements and termination options.

If the third party has access to the organization's systems and continuing to allow access could cause further damage, the Lead Incident Handler or a designated technical specialist may revoke the third party's access.

Depending on the type of incident, the third party may provide specific instructions regarding incident containment, eradication, and recovery (e.g., install patches, enable / disable certain functions, etc.). Prior

Incident Response Plan 50

INCIDENT MANAGEMENT

Additional Documentation: Third-Party Incidents

Learn More

Tandem

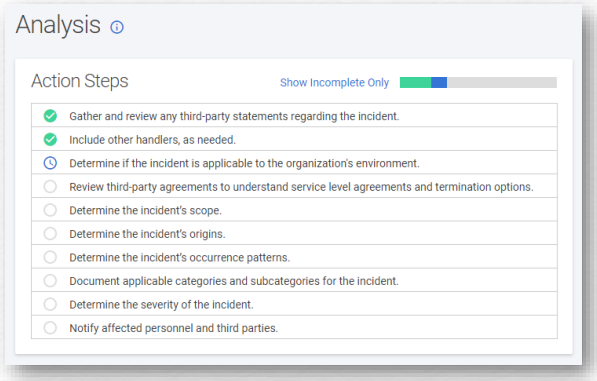
54

EXISTING TANDEM FEATURES

INCIDENT MANAGEMENT

Action Plan: Third-Party Incidents

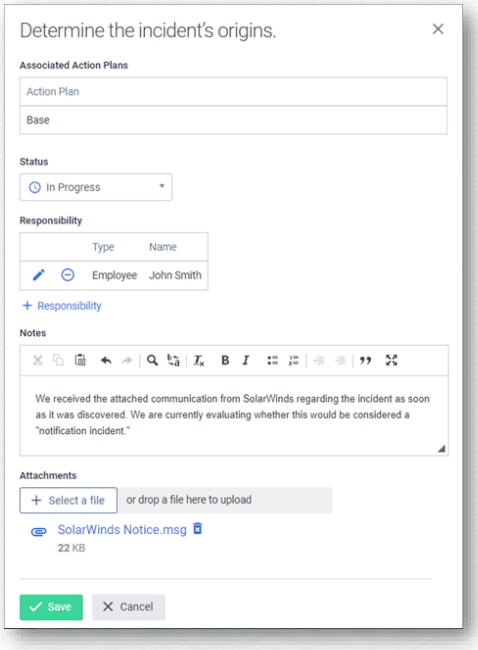
Read the Blog | Download the Checklist



Tandem

55

EXISTING TANDEM FEATURES



INCIDENT MANAGEMENT

Attach Files to Action Steps

Tandem

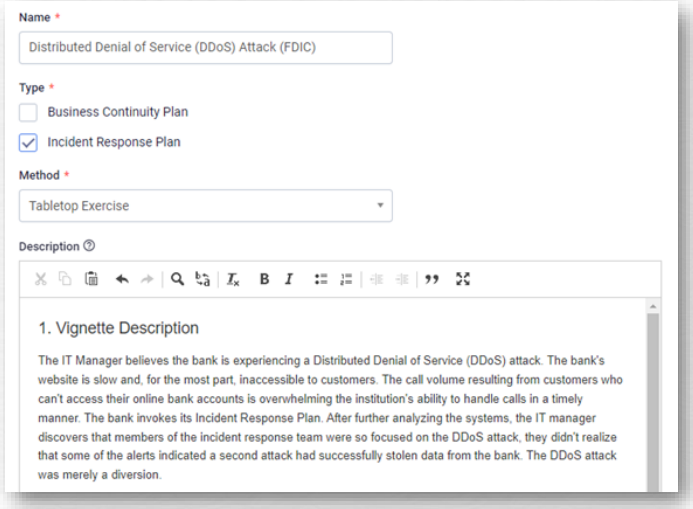
56

EXISTING TANDEM FEATURES

INCIDENT MANAGEMENT

Exercise & Test Scenarios from the FDIC and NIST

Software Update | Press Release



Tandem

57

EXISTING TANDEM FEATURES

INCIDENT MANAGEMENT

Security Incident Management Training Course

Learn More

Tandem

58

COMPLETE THE SURVEY
Answer "Yes" on Question 8

VISIT OUR WEBSITE
Tandem.App/Demos

59

KEYS CONFERENCE

March 30 – April 1, 2022
Allen, Texas

TRACKS

- Tandem
- Risk & Compliance
- Cybersecurity
- Consulting

Tandem.App/KEYS

Tandem

60

Fill out the survey for a chance to win!

Tandem

61

62

THANKS FOR JOINING

A Banker's Guide to Understanding the New Incident Notification Rule

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

https://www.linkedin.com/in/alyssapugh/
https://tandem.app/speakers/Alyssa-pugh/

Tandem

63