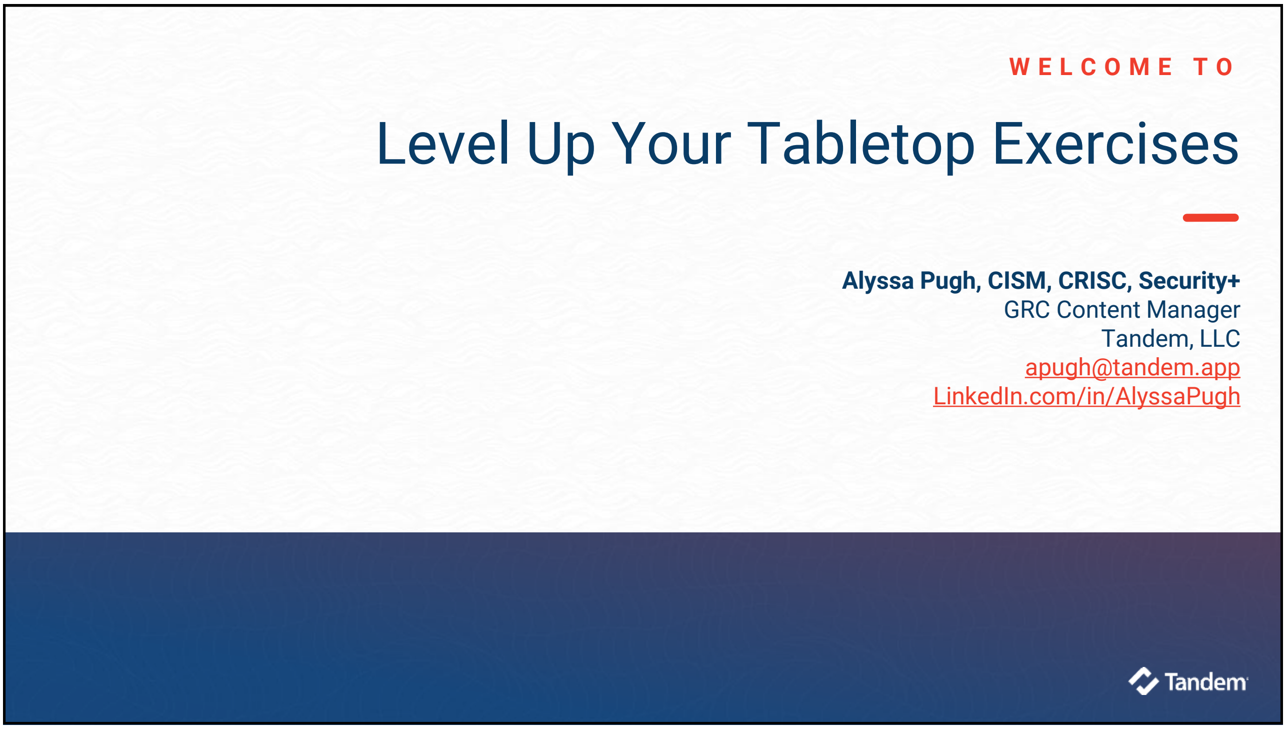


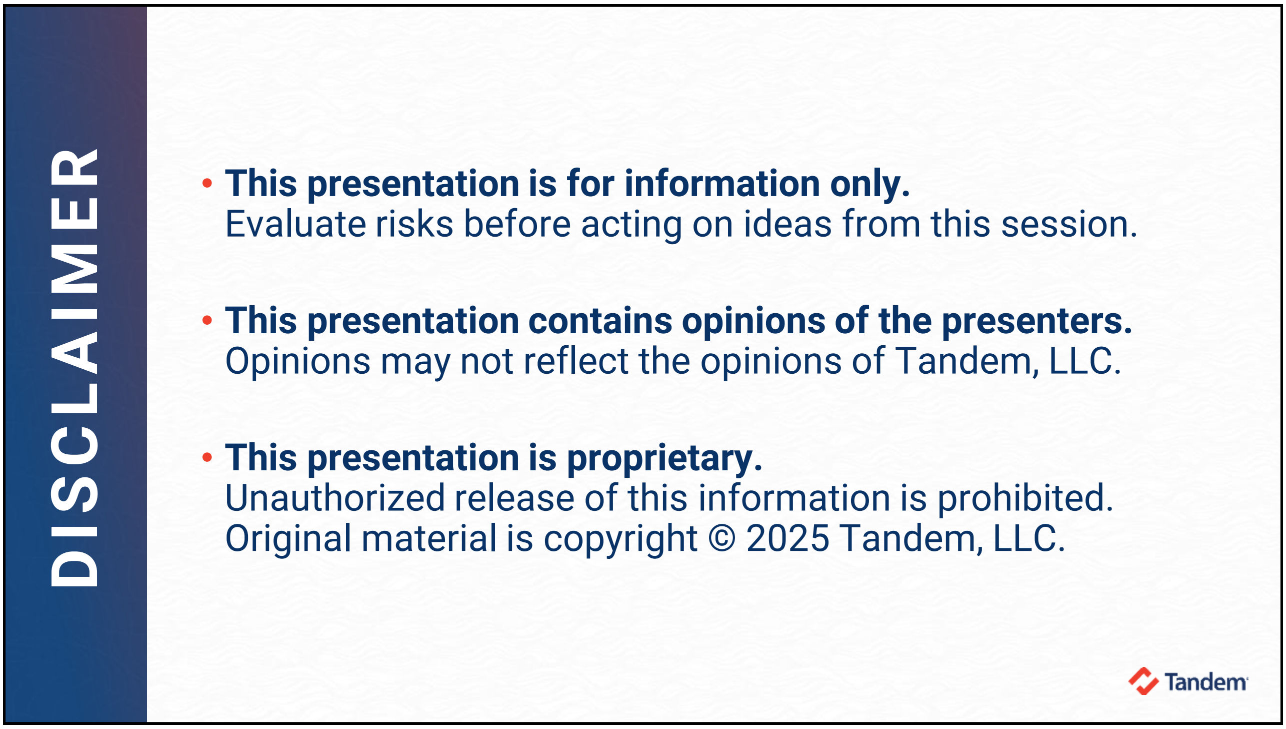
WELCOME TO

# Level Up Your Tabletop Exercises

**Alyssa Pugh, CISM, CRISC, Security+**
GRC Content Manager
Tandem, LLC
apugh@tandem.app
LinkedIn.com/in/AlyssaPugh

Tandem

1

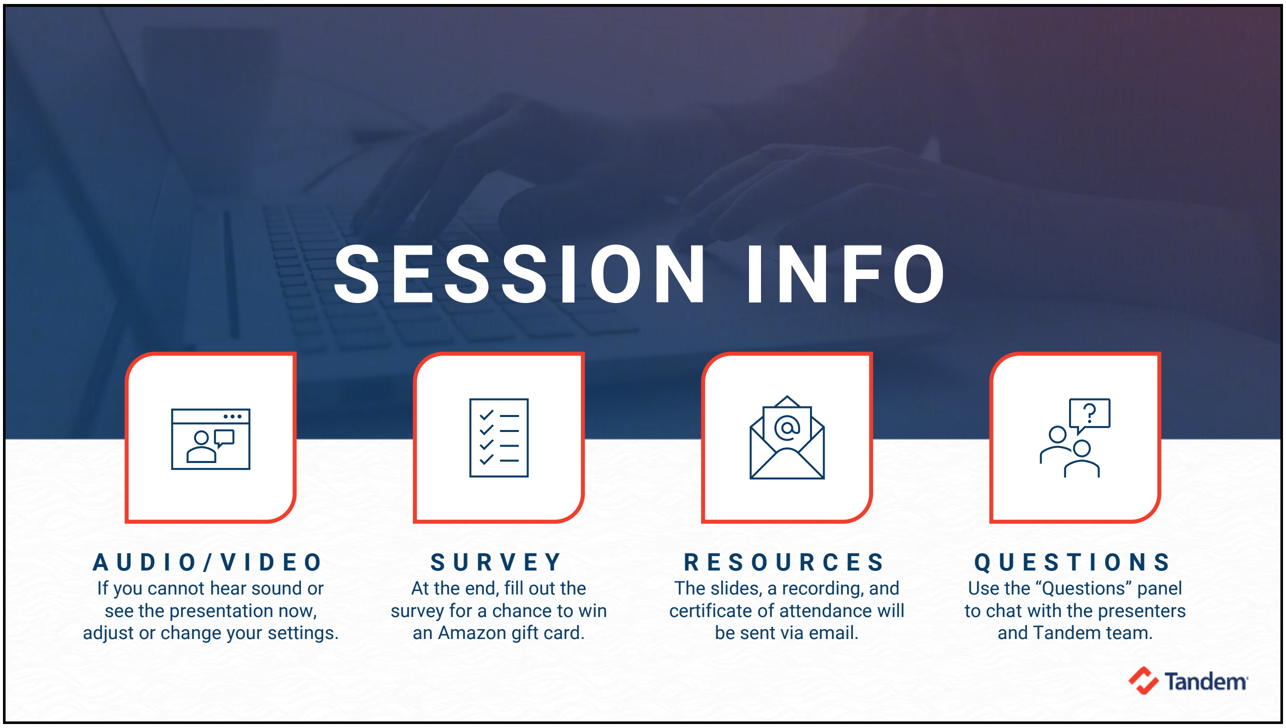


## DISCLAIMER

- **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, LLC.
- **This presentation is proprietary.** Unauthorized release of this information is prohibited. Original material is copyright © 2025 Tandem, LLC.

Tandem

2



# SESSION INFO

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

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

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

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

Tandem

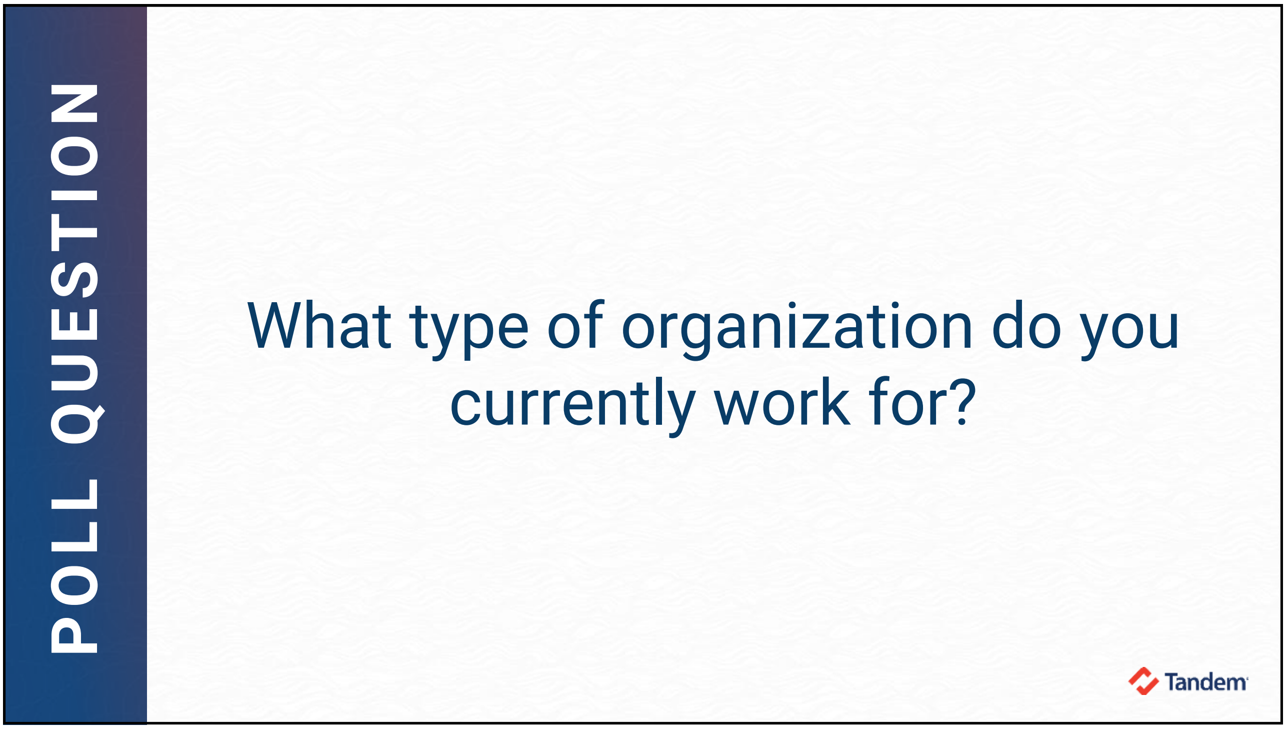
3

- 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

Tandem

4

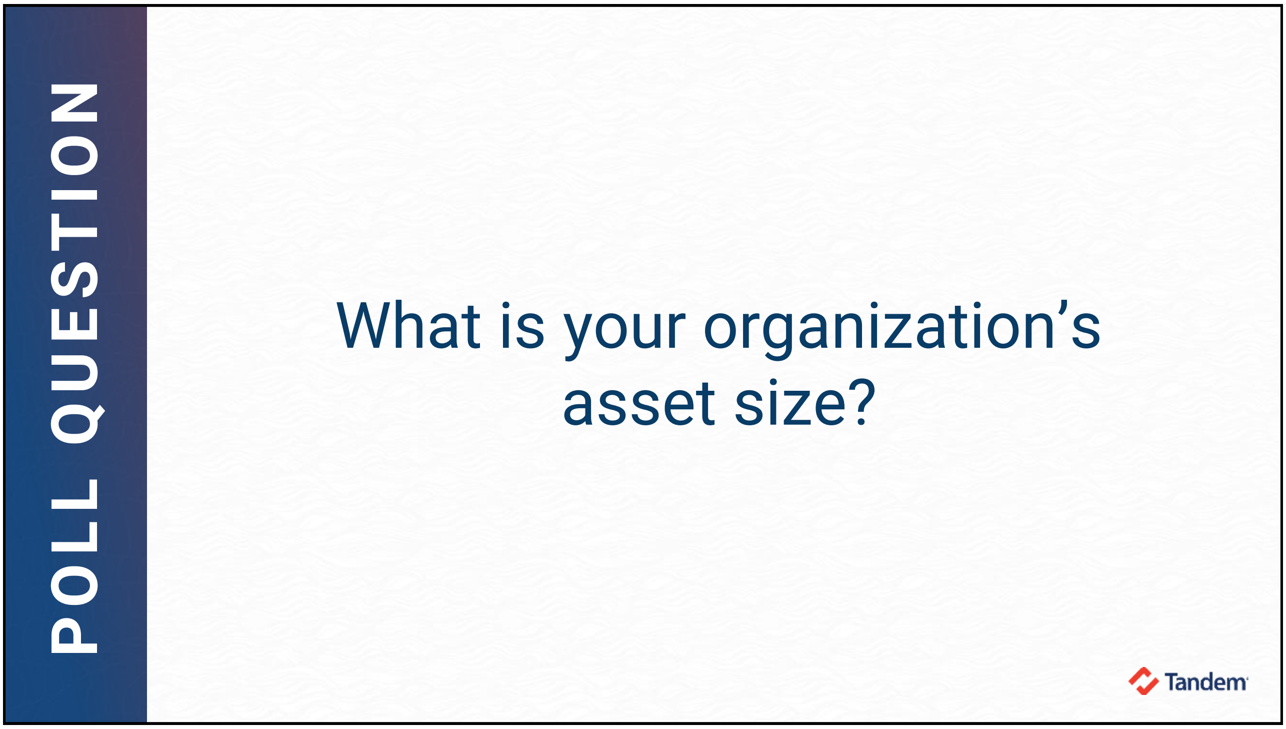


POLL QUESTION

What type of organization do you currently work for?

Tandem

5

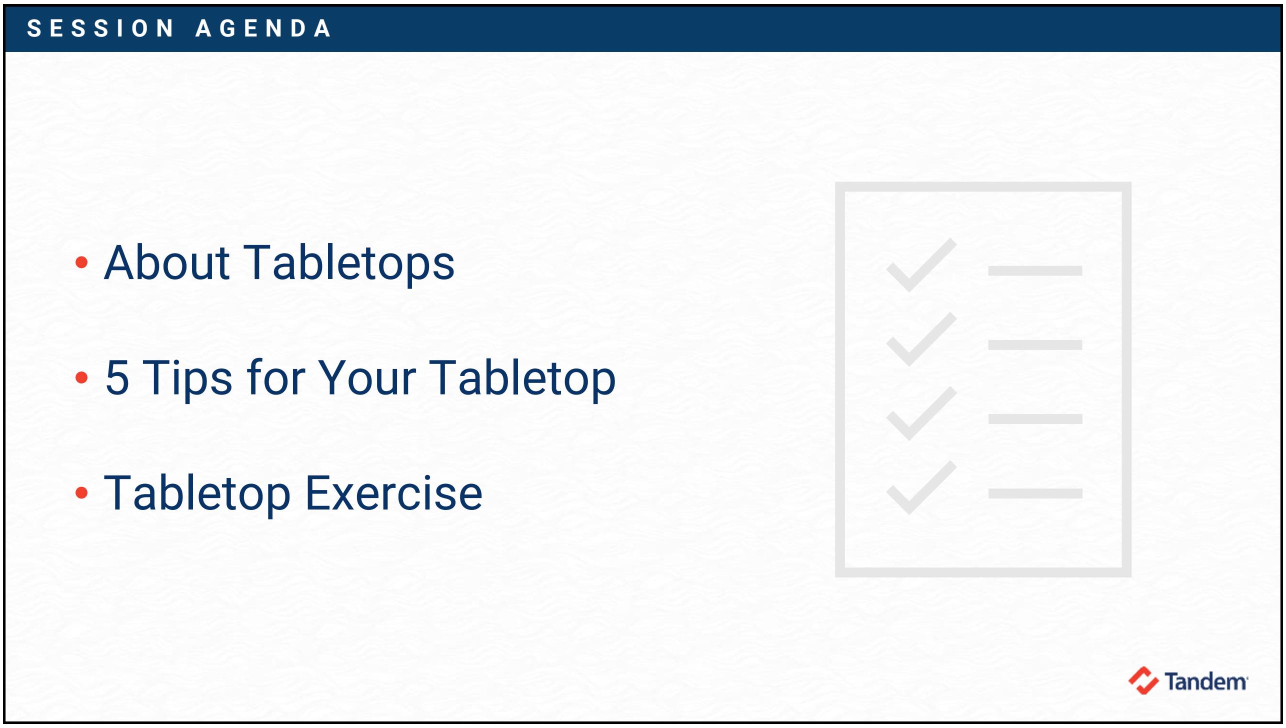


POLL QUESTION

What is your organization’s asset size?

Tandem

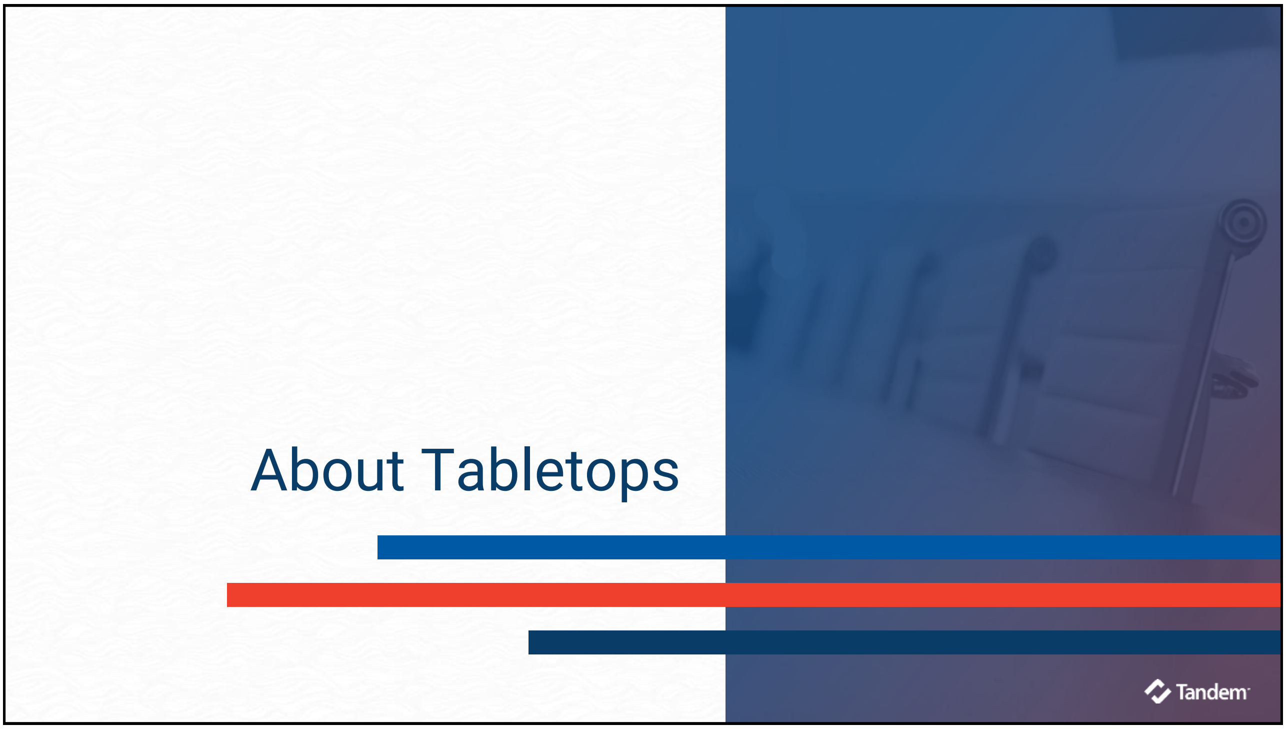
6



## SESSION AGENDA

- About Tabletops
- 5 Tips for Your Tabletop
- Tabletop Exercise

7



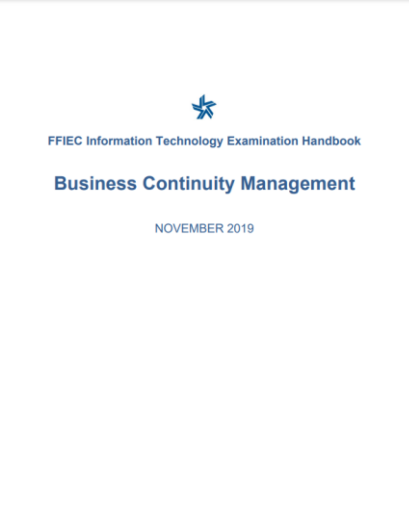
## About Tabletops

8

## DEFINITION

"A tabletop exercise (sometimes referred to as a walk-through) is a discussion during which personnel review their BCP-defined roles and discuss their responses during an adverse event simulation."

https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/vii-exercises-and-tests/viig-exercise-and-test-methods/viig3-tabletop-exercise



FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

Tandem

9

## NIST Cybersecurity Framework

### ID.IM-02

Improvements are identified from **security tests and exercises**, including those done in coordination with suppliers and relevant third parties.

- **Ex1:** Identify improvements for future incident response activities based on findings from incident response assessments (e.g., **tabletop exercises and simulations**, **tests**, internal reviews, independent audits).
- **Ex2:** Identify improvements for future business continuity, disaster recovery, and incident response activities based on **exercises** performed in coordination with critical service providers and product suppliers.
- **Ex3:** Involve internal stakeholders (e.g., senior executives, legal department, HR) in **security tests and exercises** as appropriate.

https://csrc.nist.gov/projects/cybersecurity-framework/filters#/csf/filters

## CISA Cybersecurity Performance Goals

### 2.S Incident Response (IR) Plans

Organizations have, maintain, update, and regularly **drill** IT and OT cybersecurity incident response plans for both common and organization-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, **tests or drills** are as realistic as feasible. IR plans are **drilled** at least annually and are updated within a risk-informed time frame following the lessons learned portion of any **exercise or drill**.

https://www.cisa.gov/cybersecurity-performance-goals-cpgs

## CIS Critical Security Controls

### 17.7 Conduct Routine Incident Response Exercises

Plan and conduct routine **incident response exercises and scenarios** for key personnel involved in the incident response process to prepare for responding to real-world incidents. **Exercises** need to test communication channels, decision-making, and workflows. Conduct **testing** on an annual basis, at a minimum.

https://www.cisecurity.org/controls/cis-controls-list

## CRI Profile

### ID.RA-05.04

The organization uses **scenario planning, table-top-exercises, or similar event analysis techniques** to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes.

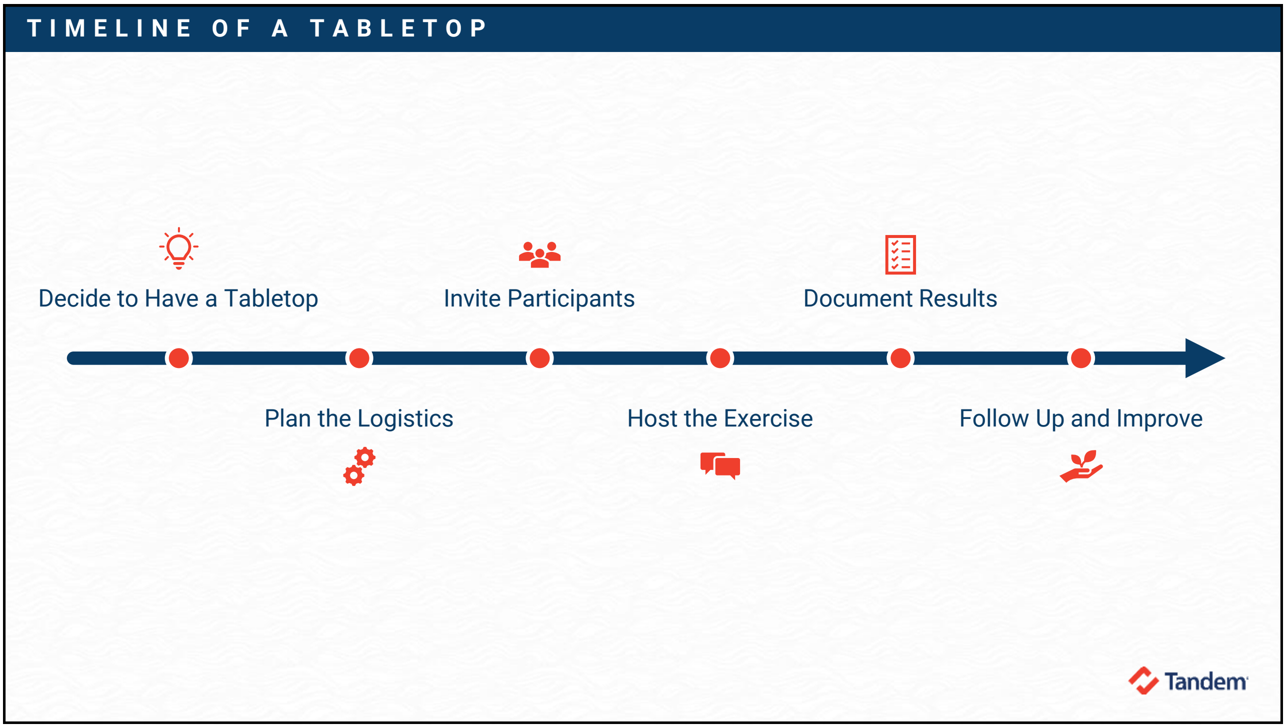
### ID.IM-04.08

The organization regularly reviews response strategy, incident management plans, recovery plans, and **associated tests and exercises** and updates them, as necessary, based on: (1) Lessons learned from incidents that have occurred (both internal and external to the organization); (2) Current cyber threat intelligence (both internal and external sources); (3) Recent and wide-scale cyber attack scenarios; (4) Operationally and technically plausible future cyber attacks; (5) Organizational or technical environment changes; and, (6) New technological developments.

https://cyberriskinstitute.org/the-profile/

Tandem

10



## TIMELINE OF A TABLETOP

Decide to Have a Tabletop

Plan the Logistics

Invite Participants

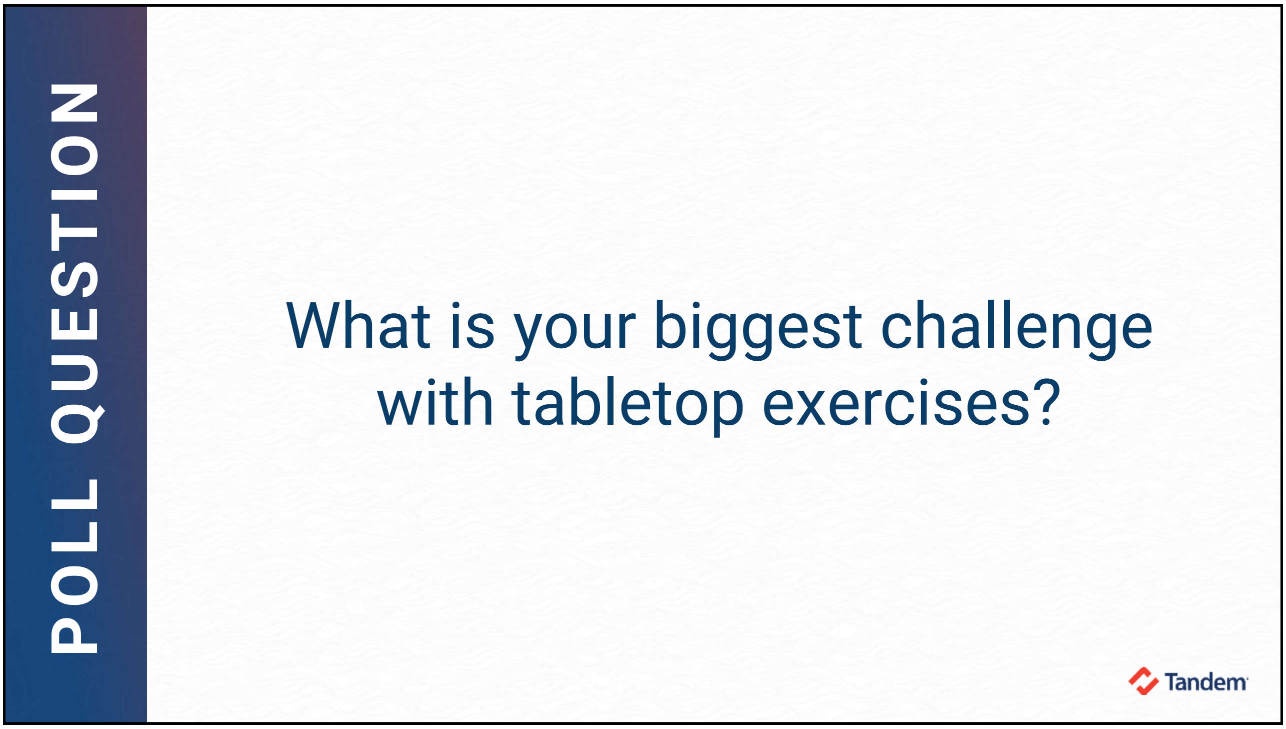
Host the Exercise

Document Results

Follow Up and Improve

Tandem

11



## POLL QUESTION

What is your biggest challenge with tabletop exercises?

Tandem

12

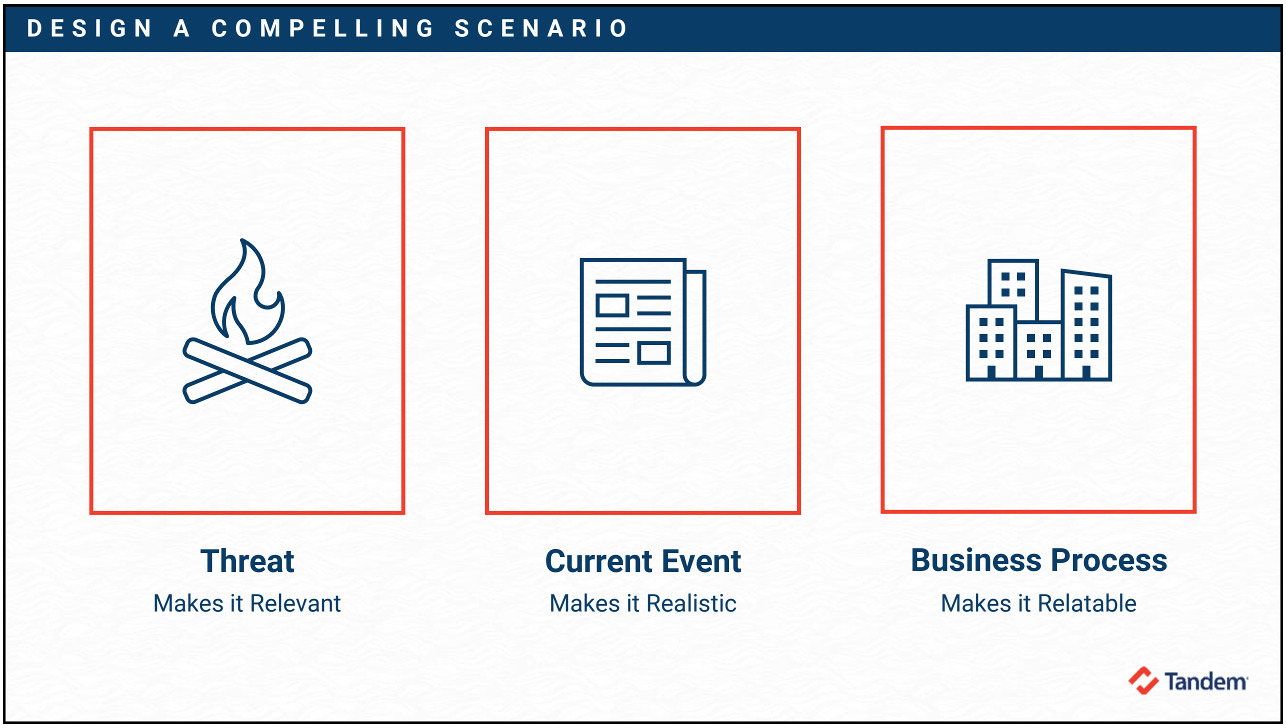
# 5 Tips for Your Tabletop

13

TIP #1

# Design a Compelling Scenario

14



## DESIGN A COMPELLING SCENARIO

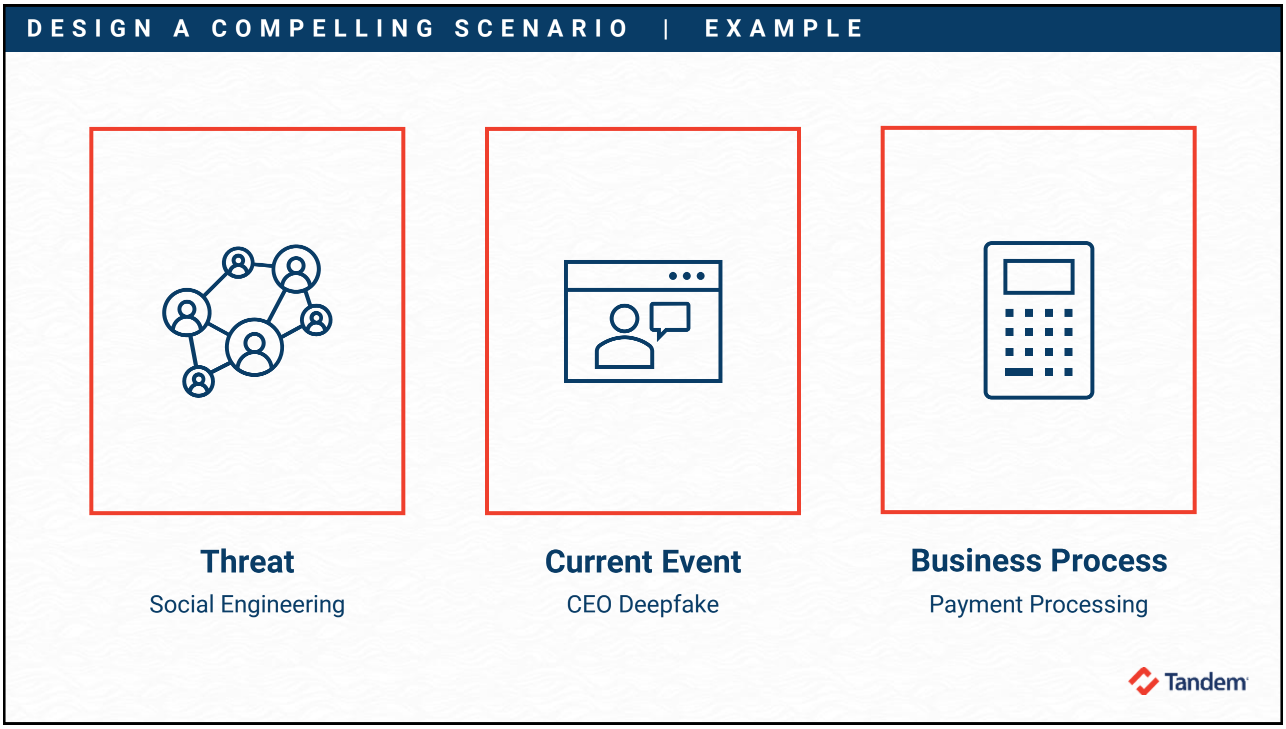
**Threat**
Makes it Relevant

**Current Event**
Makes it Realistic

**Business Process**
Makes it Relatable

Tandem

15



## DESIGN A COMPELLING SCENARIO | EXAMPLE

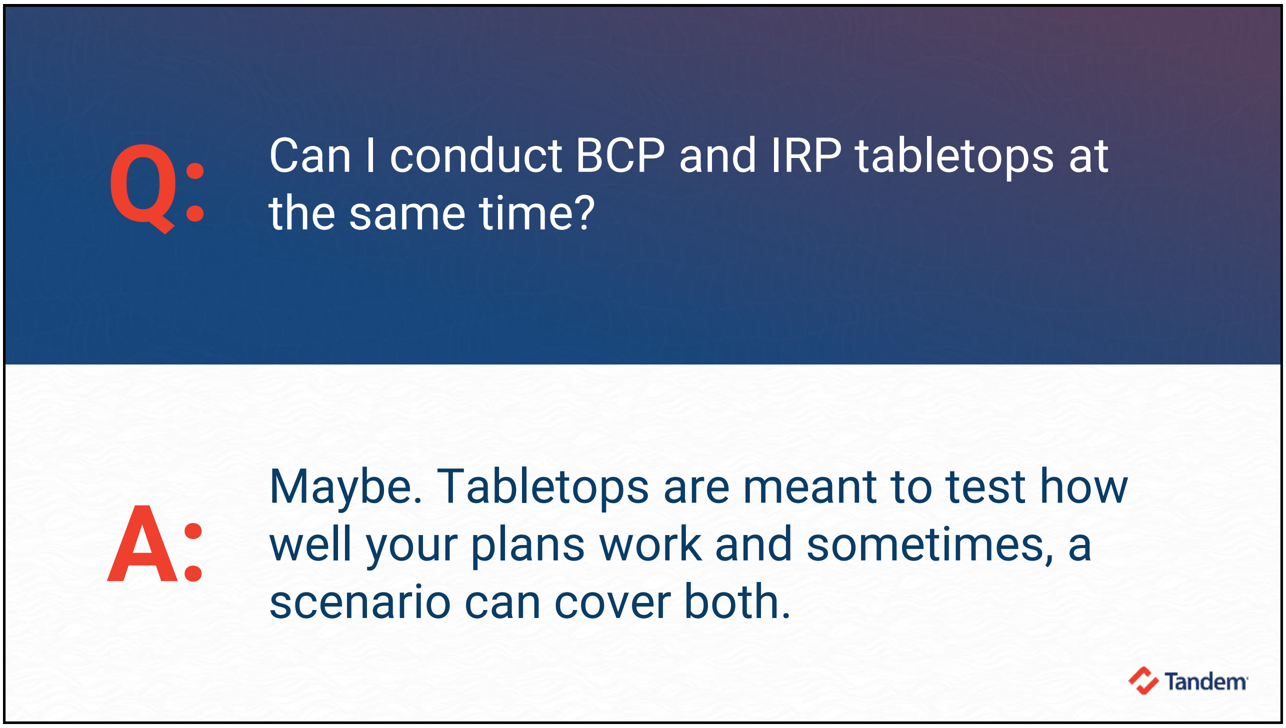
**Threat**
Social Engineering

**Current Event**
CEO Deepfake

**Business Process**
Payment Processing

Tandem

16



Q: Can I conduct BCP and IRP tabletops at the same time?

A: Maybe. Tabletops are meant to test how well your plans work and sometimes, a scenario can cover both.

Tandem

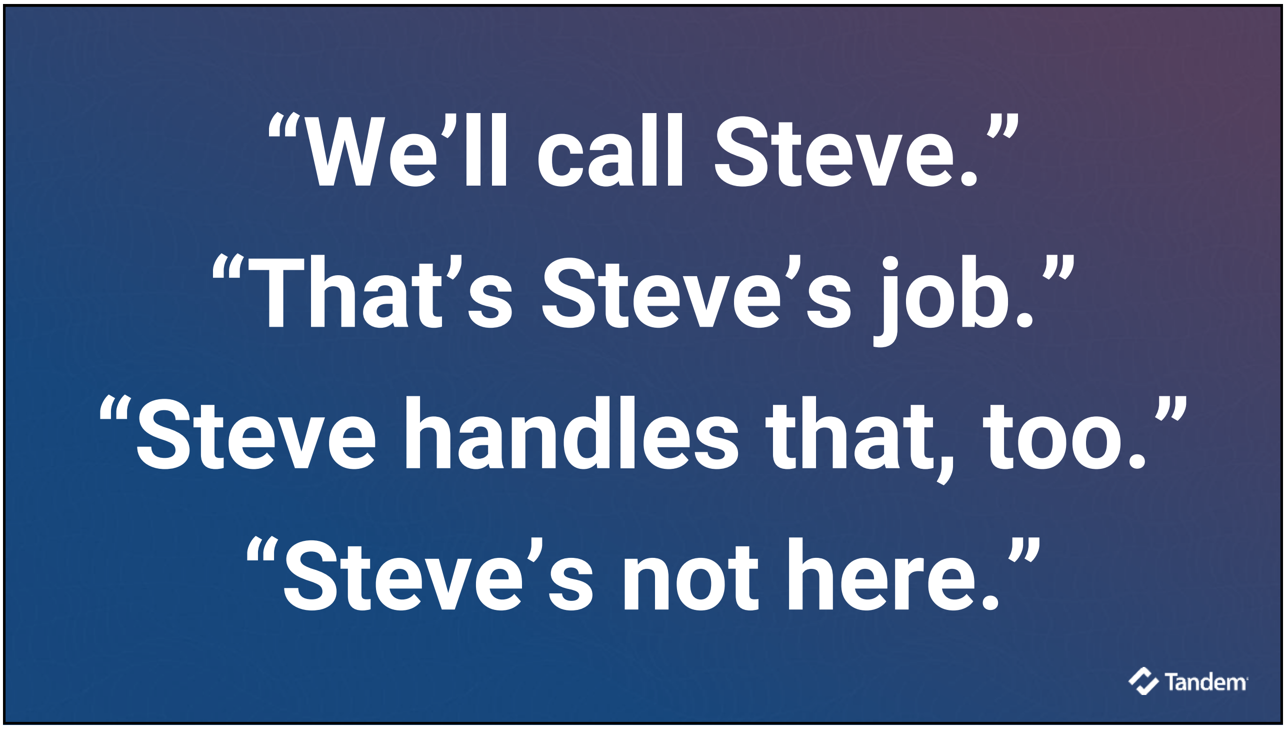
17

TIP #2

## Gather the Right Team

Tandem

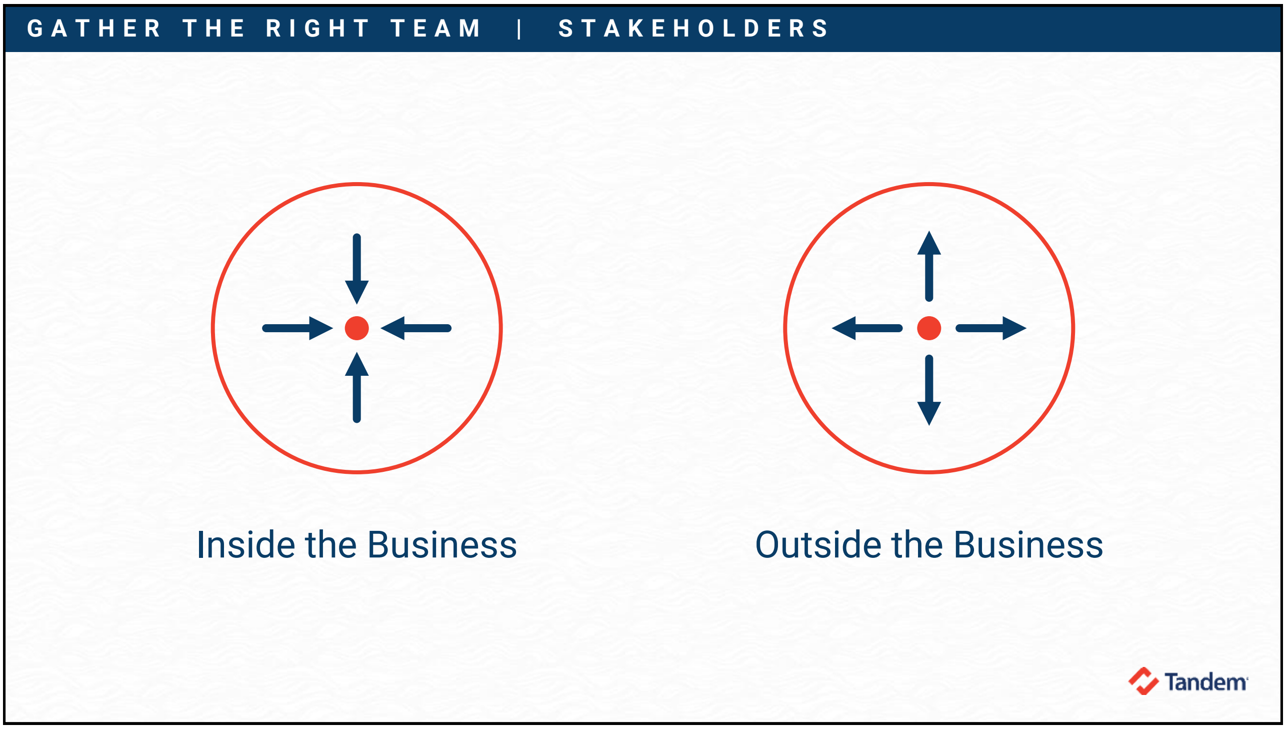
18



“We’ll call Steve.”
“That’s Steve’s job.”
“Steve handles that, too.”
“Steve’s not here.”

Tandem

19



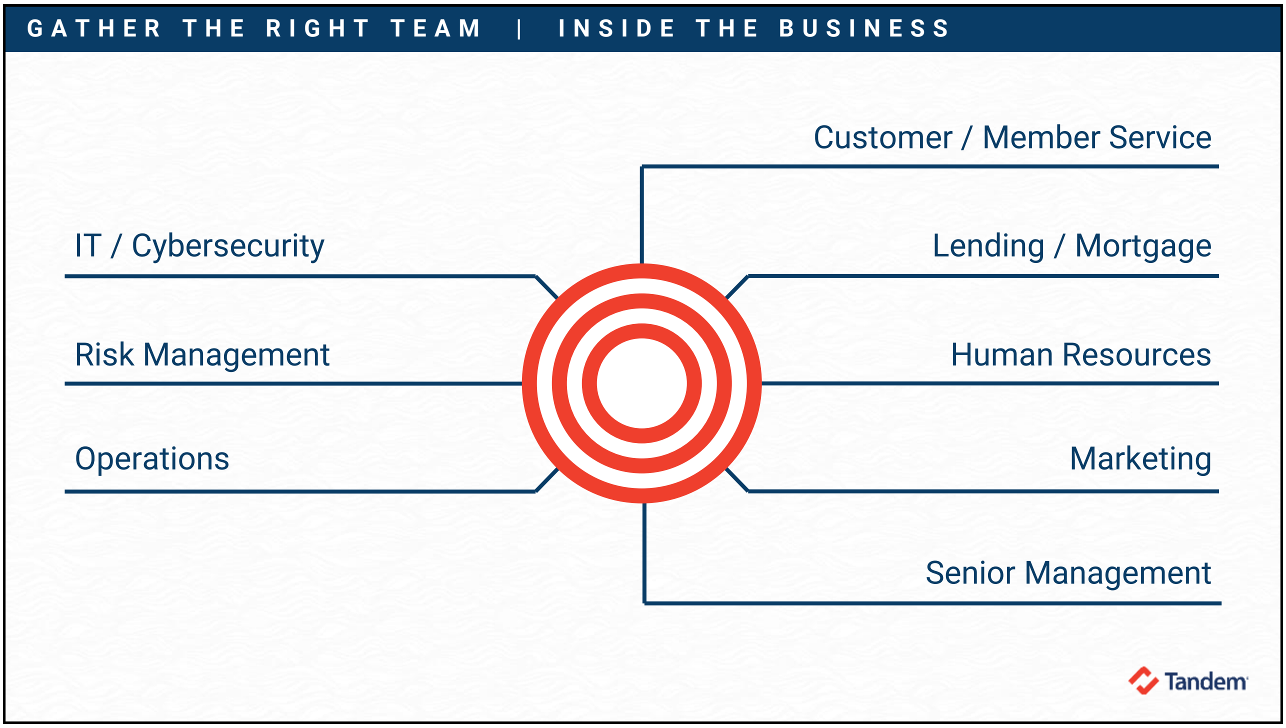
GATHER THE RIGHT TEAM | STAKEHOLDERS

Inside the Business

Outside the Business

Tandem

20



## GATHER THE RIGHT TEAM | INSIDE THE BUSINESS

IT / Cybersecurity

Risk Management

Operations

Customer / Member Service

Lending / Mortgage

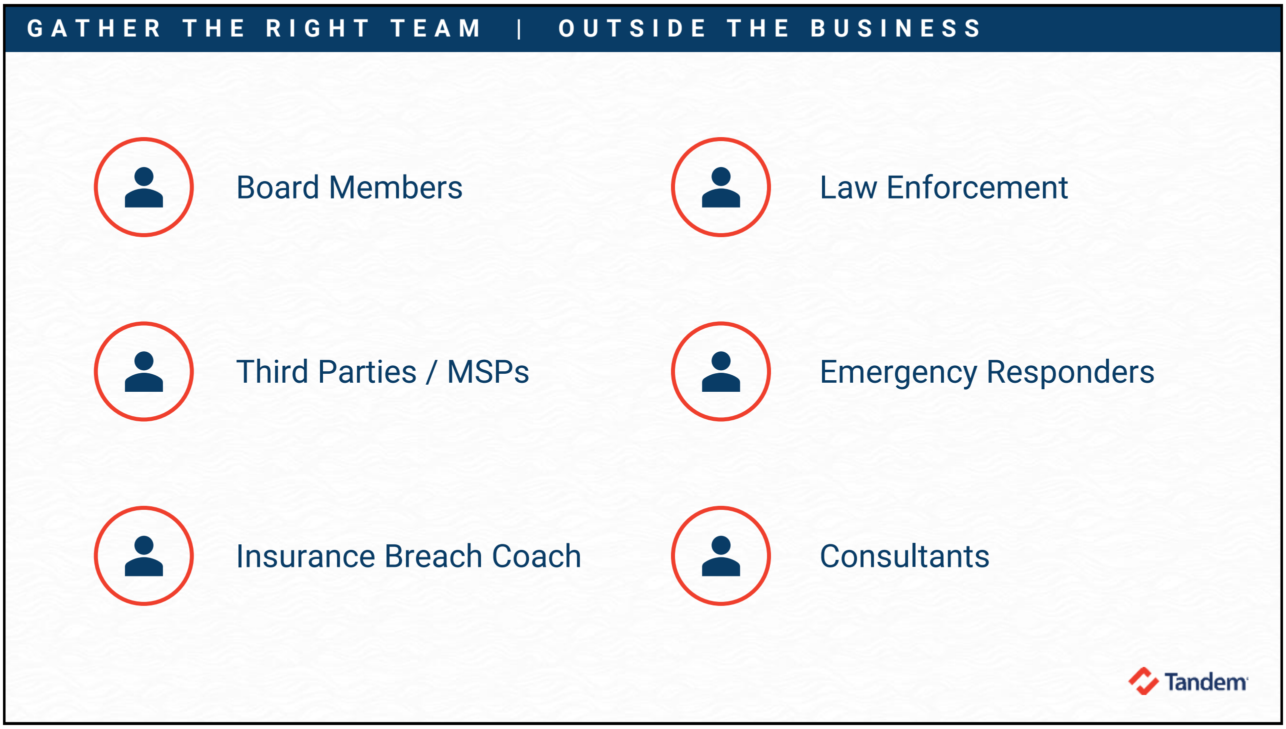
Human Resources

Marketing

Senior Management

Tandem

21

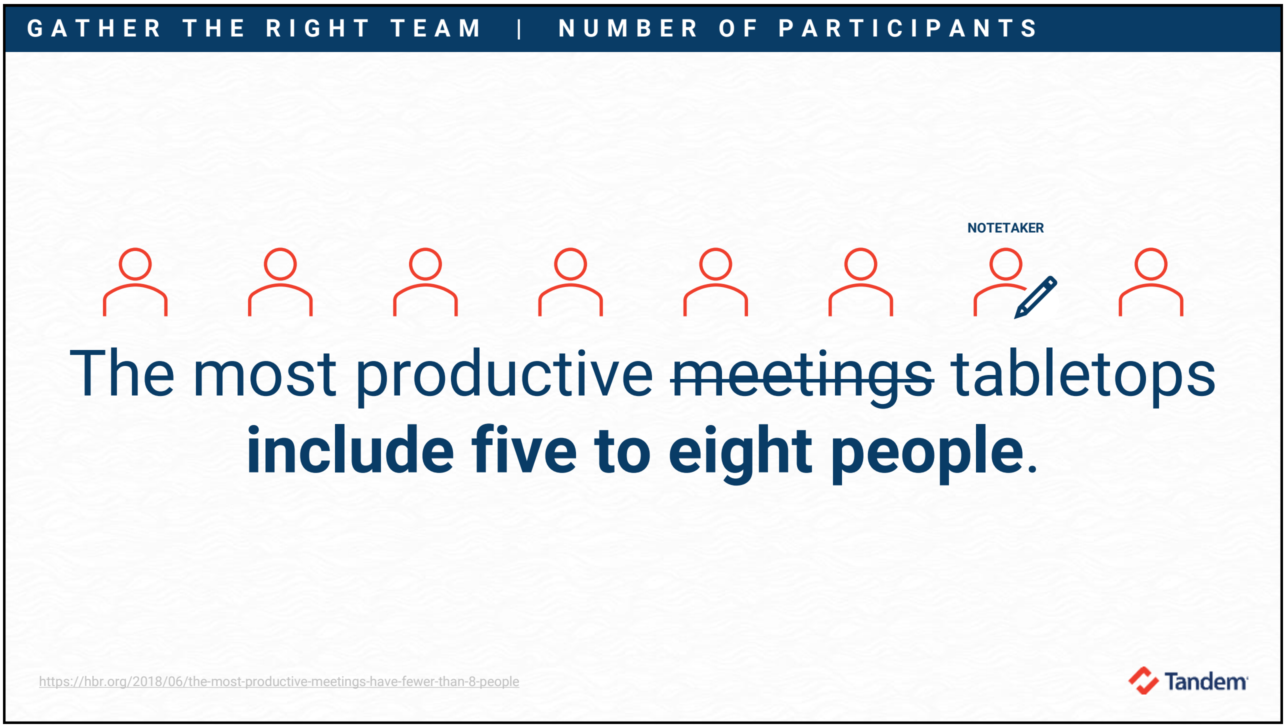


## GATHER THE RIGHT TEAM | OUTSIDE THE BUSINESS

- Board Members
- Third Parties / MSPs
- Insurance Breach Coach
- Law Enforcement
- Emergency Responders
- Consultants

Tandem

22



GATHER THE RIGHT TEAM | NUMBER OF PARTICIPANTS

The most productive ~~meetings~~ tabletops **include five to eight people**.

https://hbr.org/2018/06/the-most-productive-meetings-have-fewer-than-8-people

Tandem

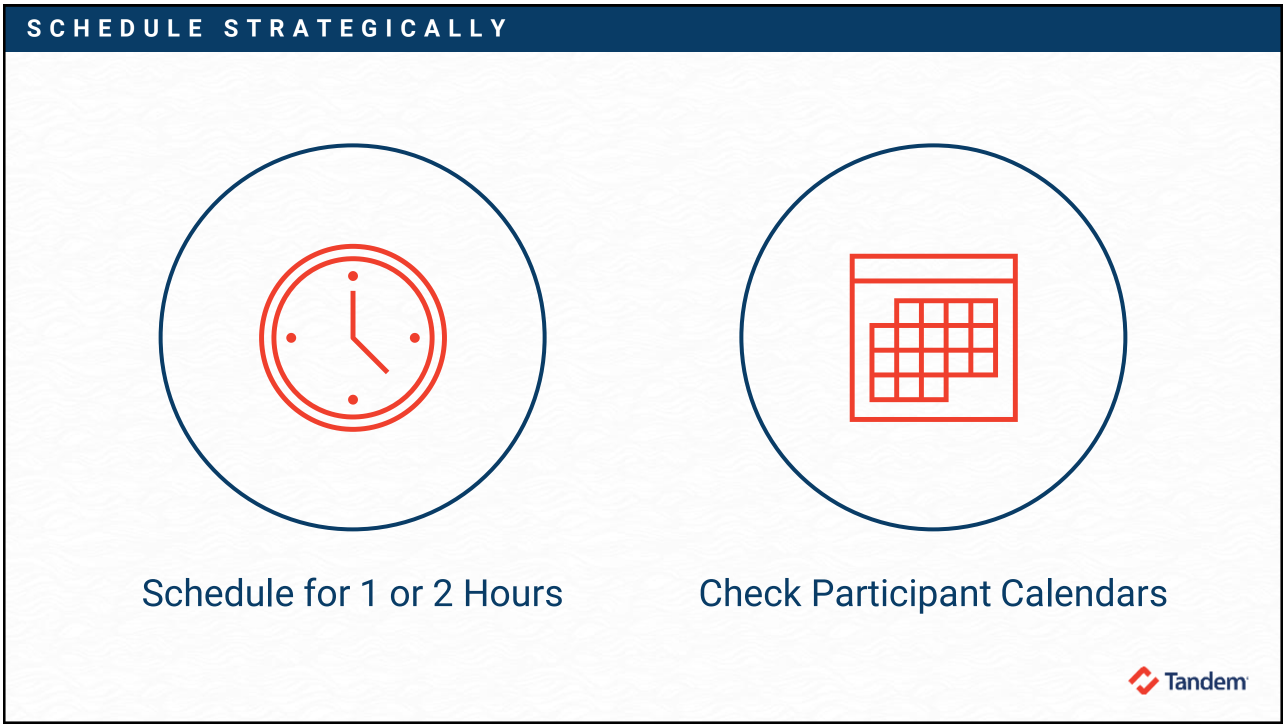
23

TIP #3

## Schedule Strategically

Tandem

24

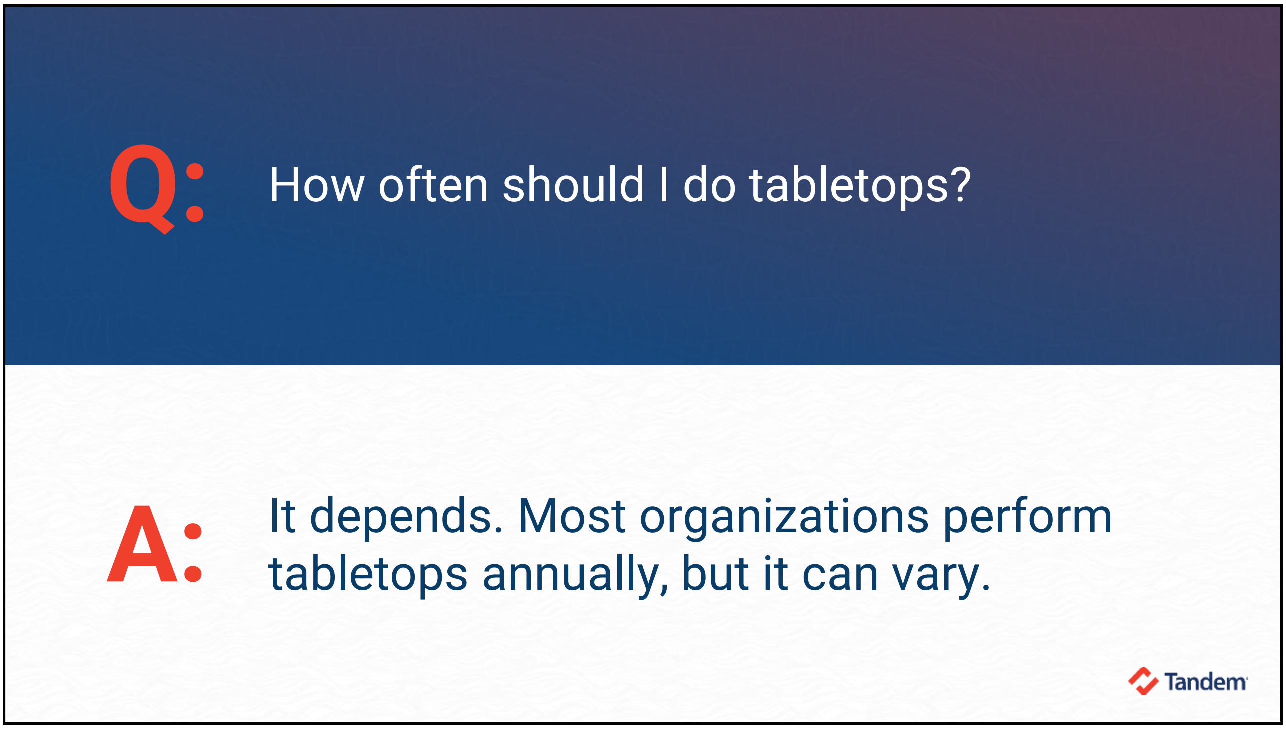


## SCHEDULE STRATEGICALLY

Schedule for 1 or 2 Hours

Check Participant Calendars

25



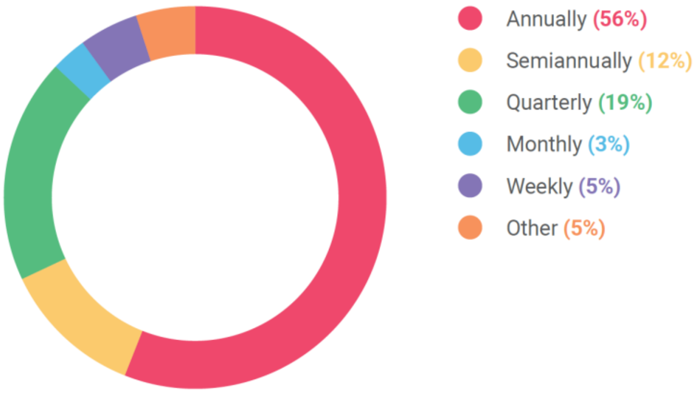
Q: How often should I do tabletops?

A: It depends. Most organizations perform tabletops annually, but it can vary.

26

## SCHEDULE STRATEGICALLY | STATE OF CYBERSECURITY REPORT

### BCP EXERCISE & TEST FREQUENCY



https://tandem.app/report

Tandem

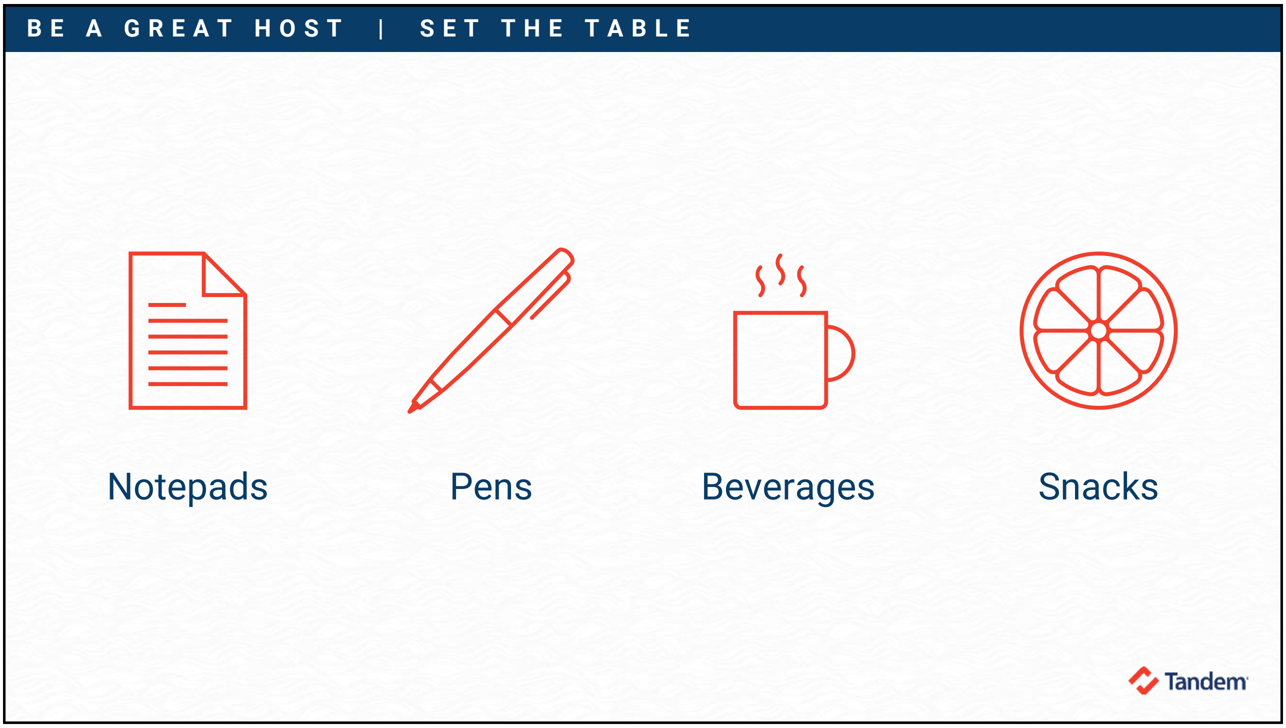
27

TIP #4

# Be a Great Host

Tandem

28



## BE A GREAT HOST | SET THE TABLE

Notepads

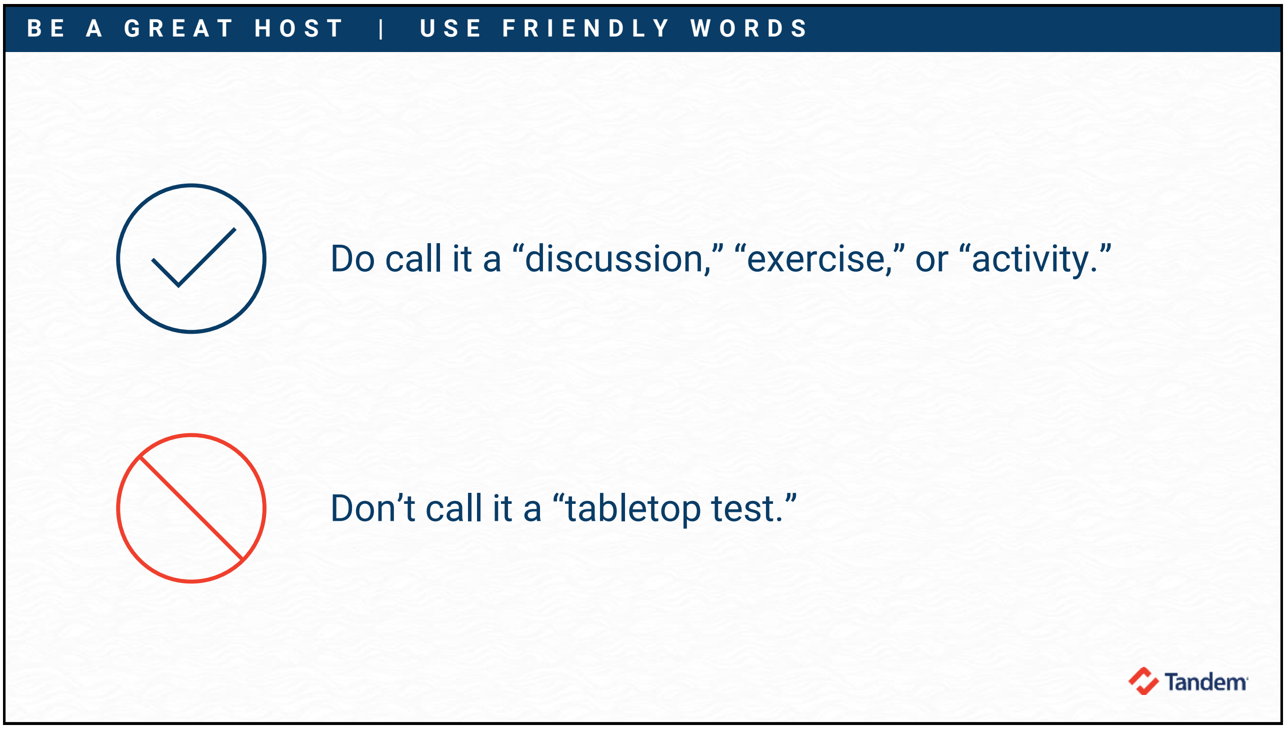
Pens

Beverages

Snacks

Tandem

29



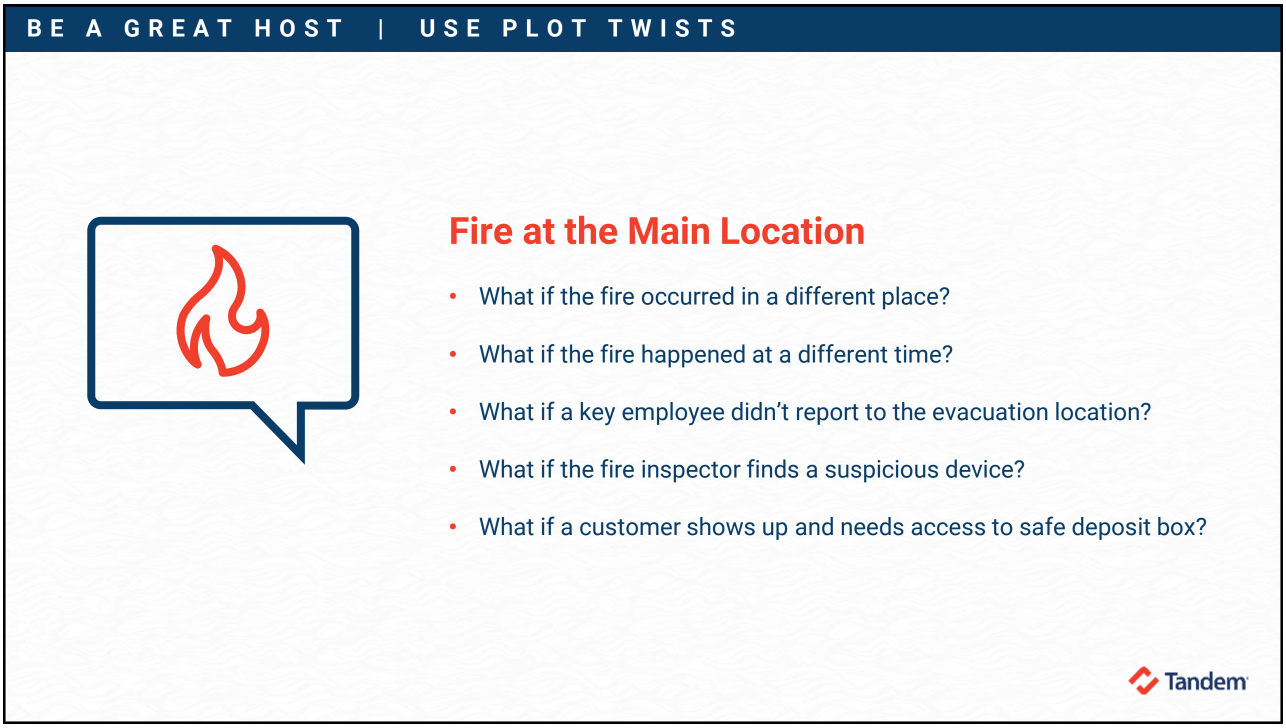
## BE A GREAT HOST | USE FRIENDLY WORDS

✓ Do call it a “discussion,” “exercise,” or “activity.”

🚫 Don’t call it a “tabletop test.”

Tandem

30



BE A GREAT HOST | USE PLOT TWISTS

## Fire at the Main Location

- What if the fire occurred in a different place?
- What if the fire happened at a different time?
- What if a key employee didn’t report to the evacuation location?
- What if the fire inspector finds a suspicious device?
- What if a customer shows up and needs access to safe deposit box?

31

TIP #5

# Expect the Unexpected

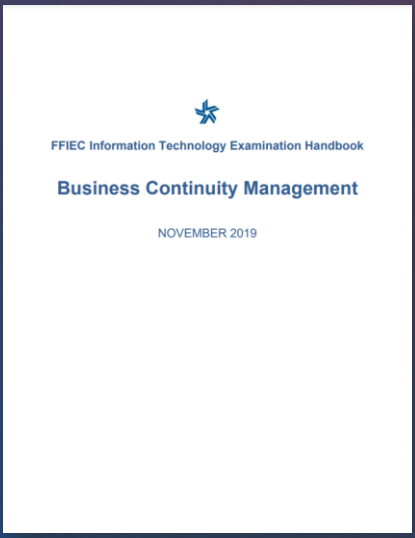
32

## FFIEC GUIDANCE

Features of a tabletop exercise may include the following: […]

- Role playing with simulated responses, critical steps, recognizing difficulties, and resolving problems.
- Clarifying critical plan elements, as well as problems noted during exercises.
- Creating action plans to correct issues.

https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/vii-exercises-and-tests/viig-exercise-and-test-methods/viig3-tabletop-exercise



FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

Tandem

33

## EXPECT THE UNEXPECTED | FOUR OUTCOMES

Potential Errors

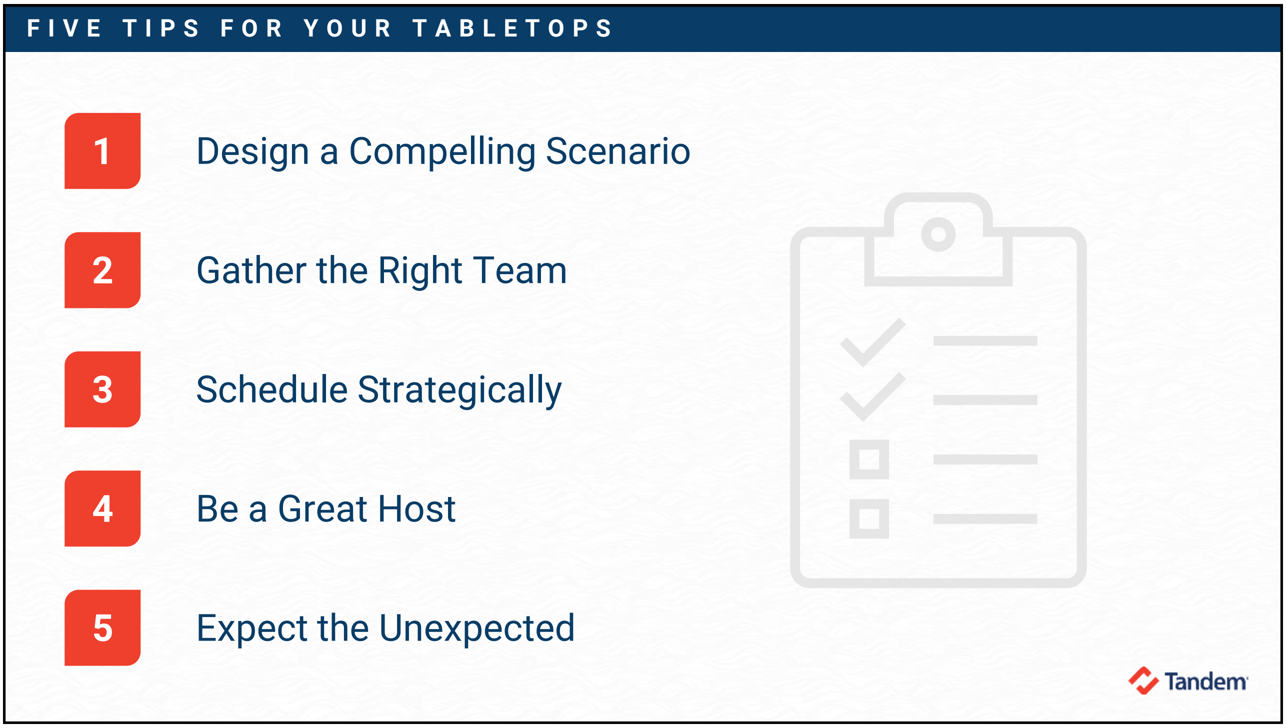
Imperfect Results

Lessons Learned

Action Items

Tandem

34

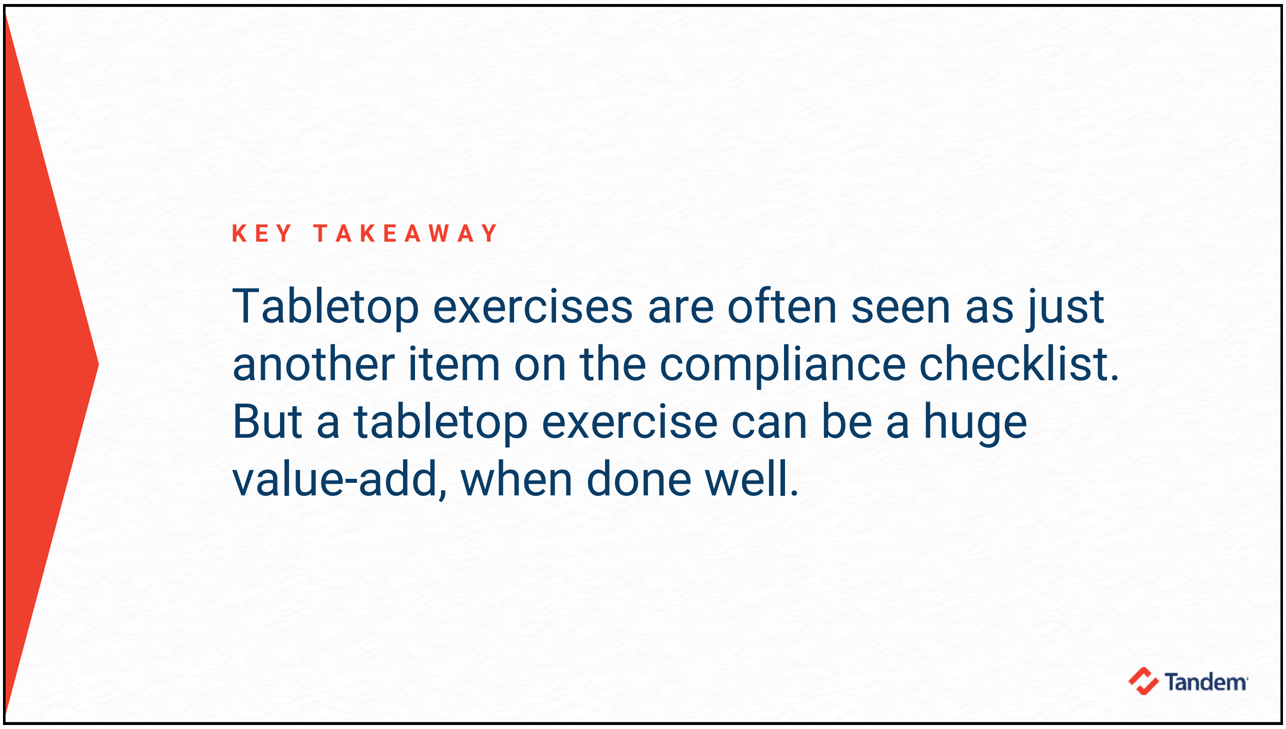


## FIVE TIPS FOR YOUR TABLETOPS

1. Design a Compelling Scenario
2. Gather the Right Team
3. Schedule Strategically
4. Be a Great Host
5. Expect the Unexpected

Tandem

35

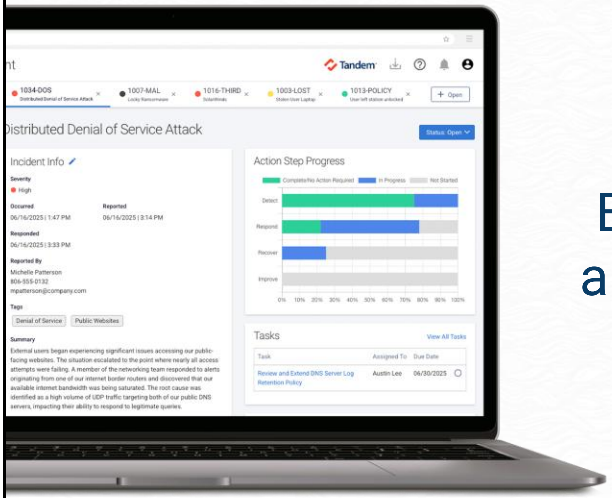


KEY TAKEAWAY

Tabletop exercises are often seen as just another item on the compliance checklist. But a tabletop exercise can be a huge value-add, when done well.

Tandem

36



nt

1034-DOS Distributed Denial of Service Attack ×
1007-MAL Locky Ransomware ×
1016-THIRD SolarWinds ×
1003-LOST Stolen User Laptop ×
1013-POLICY User left station unlocked ×
+ Open

Distributed Denial of Service Attack

Status: Open

Incident Info

Severity
High

Occurred
06/16/2025 | 1:47 PM

Reported
06/16/2025 | 3:14 PM

Responded
06/16/2025 | 3:33 PM

Reported By
Michelle Patterson
806-555-0132
mpatterson@company.com

Tags
Denial of Service
Public Websites

Summary
External users began experiencing significant issues accessing our public-facing websites. The situation escalated to the point where nearly all access attempts were failing. A member of the networking team responded to alerts originating from one of our internet border routers and discovered that our available internet bandwidth was being saturated. The root cause was identified as a high volume of UDP traffic targeting both of our public DNS servers, impacting their ability to respond to legitimate queries.

Action Step Progress

Tasks

View All Tasks

| Task | Assigned To | Due Date | |
|---|---|---|---|
| Review and Extend DNS Server Log Retention Policy | Austin Lee | 06/30/2025 | ○ |

TANDEM SOFTWARE

# Business Continuity Plan and Incident Management

Tandem.App

37

SUBMIT YOUR QUESTIONS!

Tandem

38

# Tabletop Exercise

Tandem

39

BOOSTconsulting™

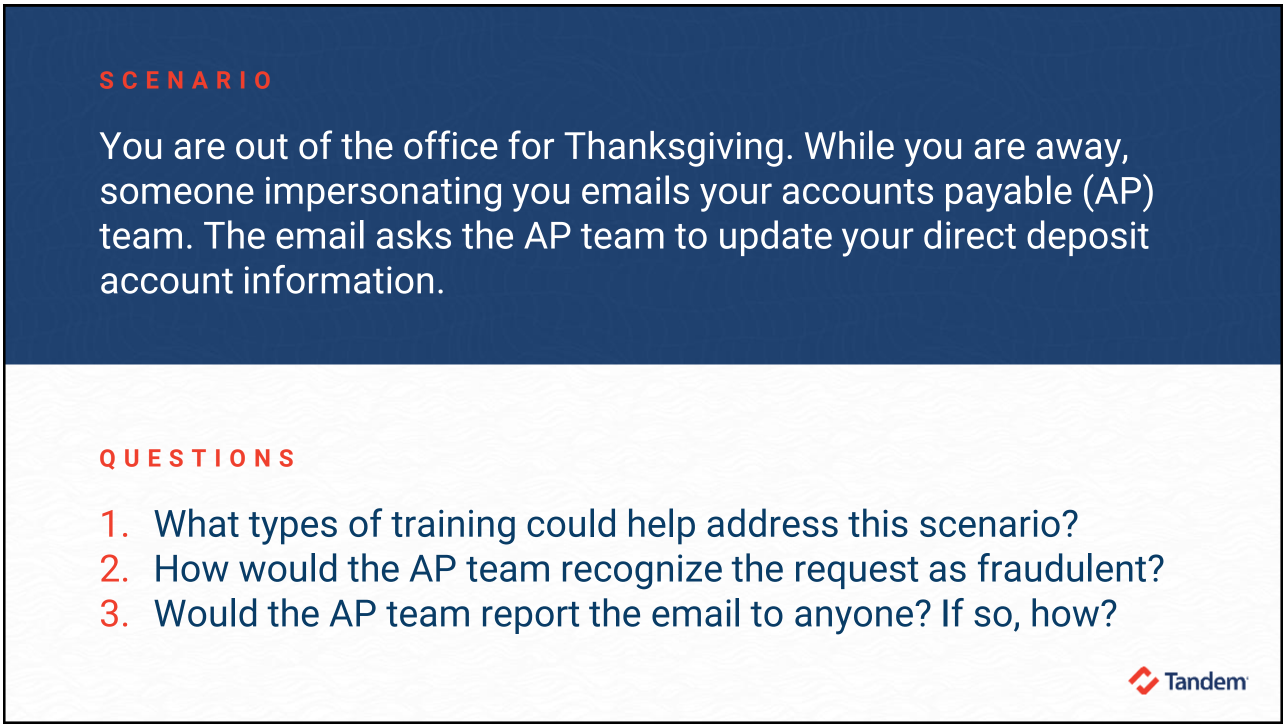
David Hernandez

Missy Oliver

Troy Sell

Tandem

40



SCENARIO

You are out of the office for Thanksgiving. While you are away, someone impersonating you emails your accounts payable (AP) team. The email asks the AP team to update your direct deposit account information.

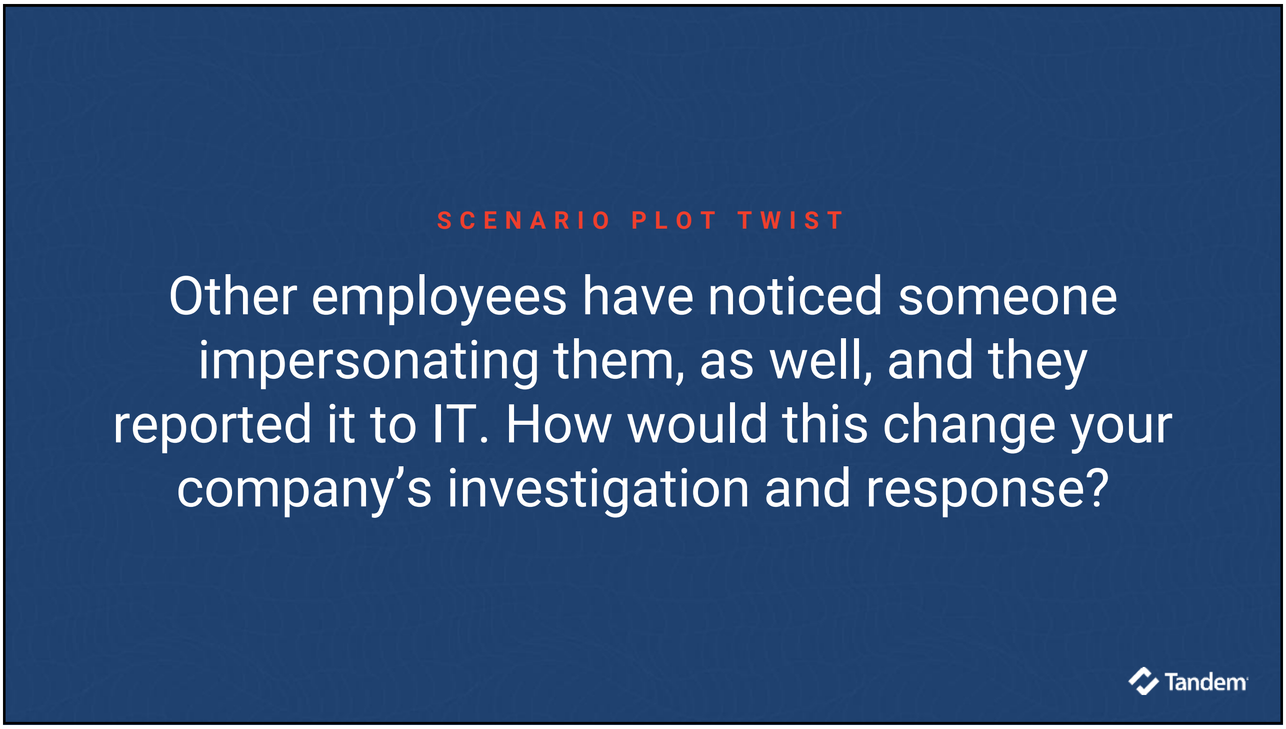
QUESTIONS

1. What types of training could help address this scenario?
2. How would the AP team recognize the request as fraudulent?
3. Would the AP team report the email to anyone? If so, how?

41

PLOT TWIST!

42

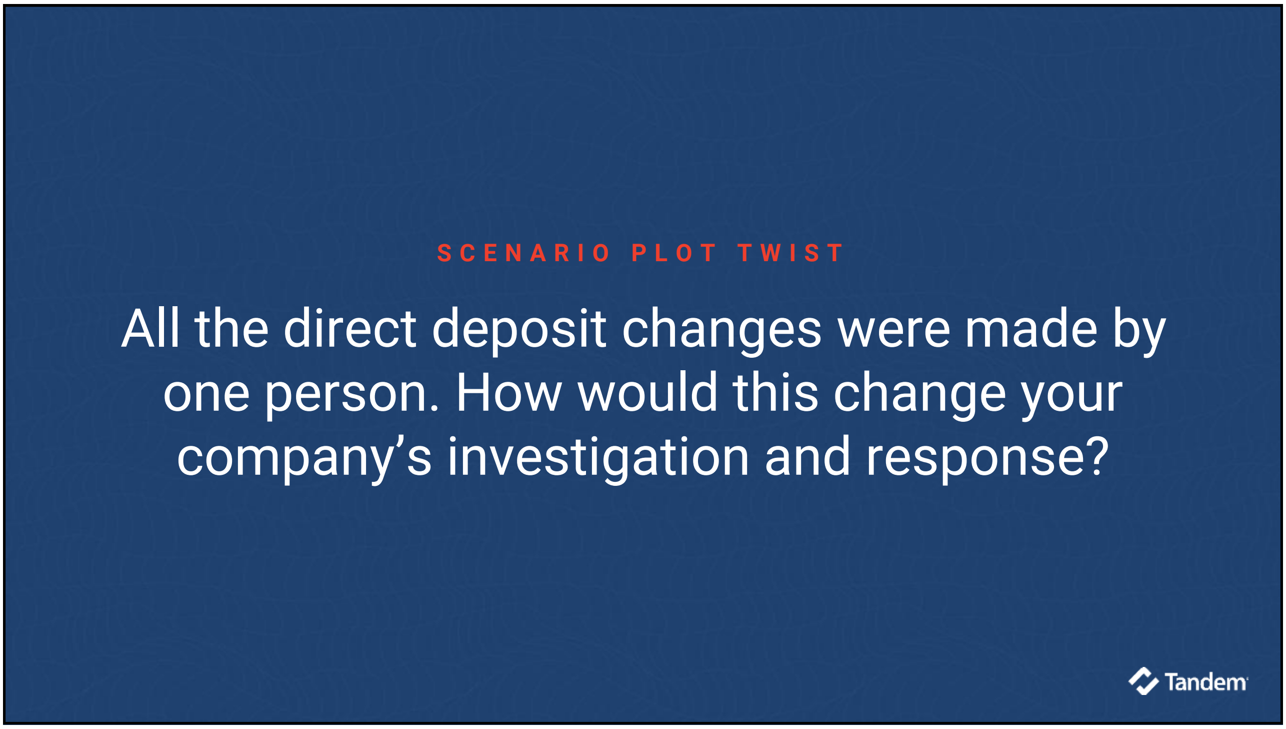


SCENARIO PLOT TWIST

Other employees have noticed someone impersonating them, as well, and they reported it to IT. How would this change your company’s investigation and response?

43

44

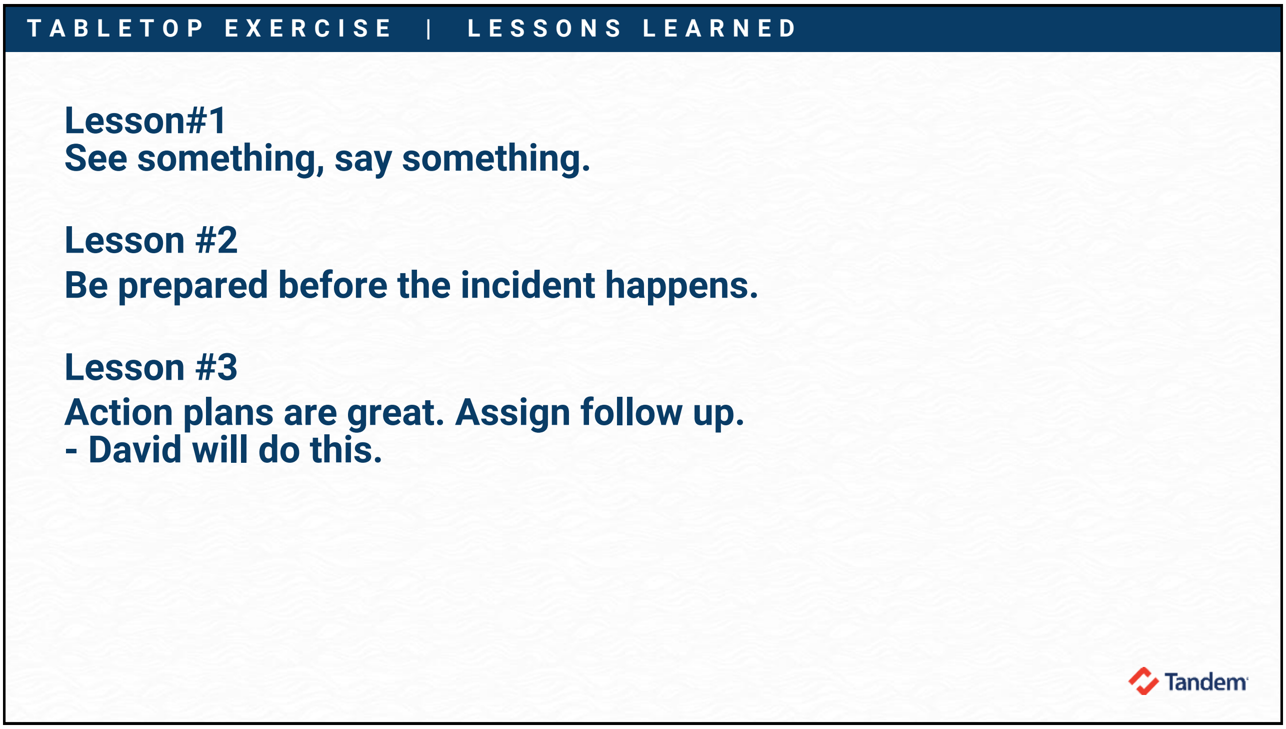


SCENARIO PLOT TWIST

All the direct deposit changes were made by one person. How would this change your company's investigation and response?

Tandem

45



TABLETOP EXERCISE | LESSONS LEARNED

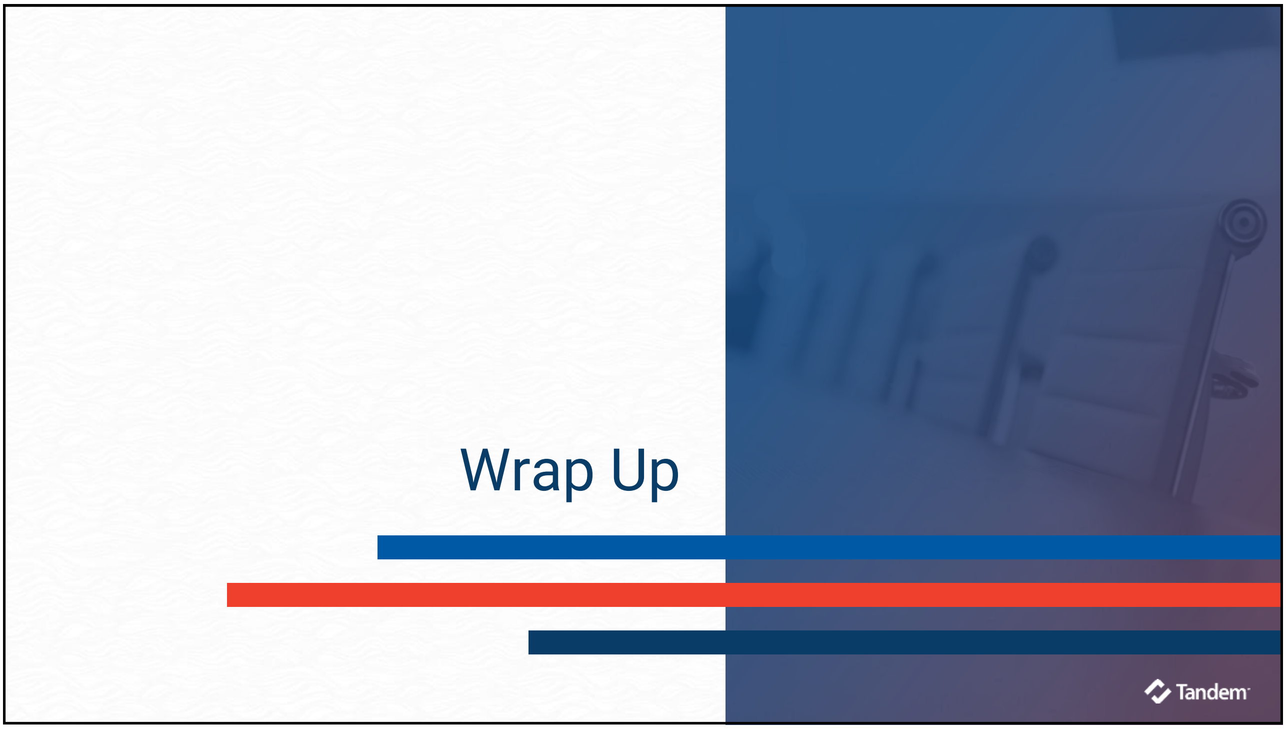
**Lesson#1**
**See something, say something.**

**Lesson #2**
**Be prepared before the incident happens.**

**Lesson #3**
**Action plans are great. Assign follow up.**
**- David will do this.**

Tandem

46



## Wrap Up

47

BOOSTconsulting™

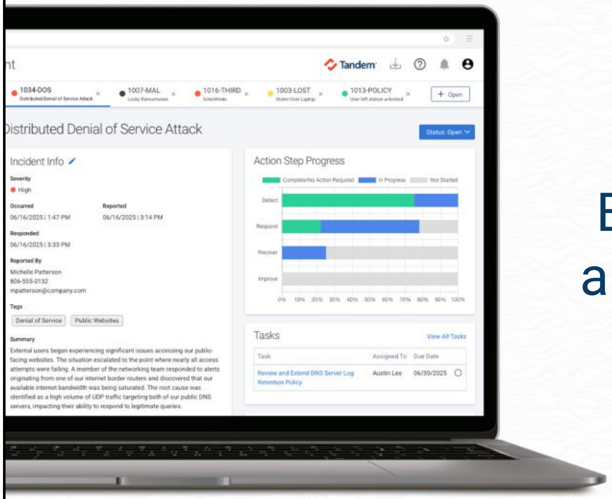
Virtual ISO (VISO)

Consulting on Retainer

Tandem Workshops

CONETRIX.COM/BOOST

48



nt

Tandem

1034-DOS Distributed Denial of Service Attack ×
1007-MAL Locky Ransomware ×
1016-THIRD SolarWinds ×
1003-LOST Stolen User Laptop ×
1013-POLICY User left station unlocked ×
+ Open

Distributed Denial of Service Attack

Status: Open

Incident Info

Severity
● High

Occurred
06/16/2025 | 1:47 PM

Reported
06/16/2025 | 3:14 PM

Responded
06/16/2025 | 3:33 PM

Reported By
Michelle Patterson
806-555-0132
mpatterson@company.com

Tags
Denial of Service | Public Websites

Summary
External users began experiencing significant issues accessing our public-facing websites. The situation escalated to the point where nearly all access attempts were failing. A member of the networking team responded to alerts originating from one of our internet border routers and discovered that our available internet bandwidth was being saturated. The root cause was identified as a high volume of UDP traffic targeting both of our public DNS servers, impacting their ability to respond to legitimate queries.

Action Step Progress

Tasks

View All Tasks

| Task | Assigned To | Due Date | |
|---|---|---|---|
| Review and Extend DNS Server Log Retention Policy | Austin Lee | 06/30/2025 | ○ |

TANDEM SOFTWARE

# Business Continuity Plan and Incident Management

Tandem.App

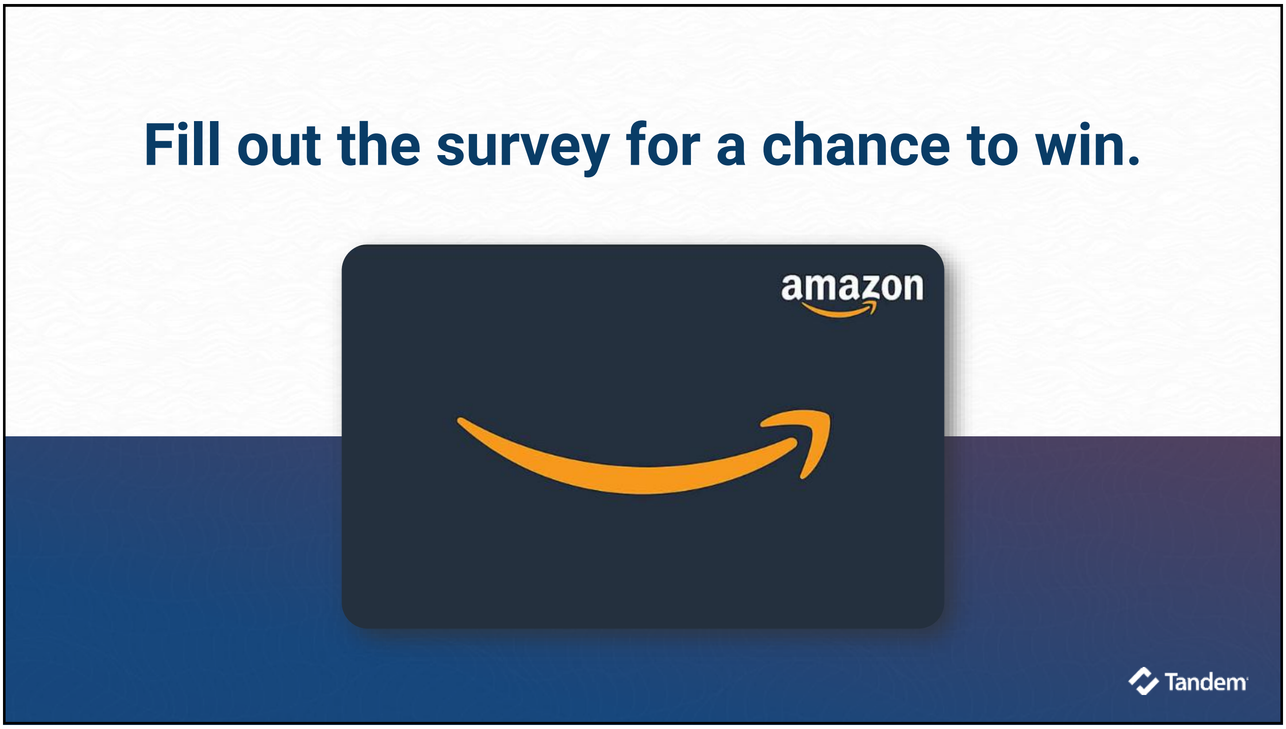
49

# Get a Free Hat!

1. Fill out the survey.
2. Schedule a sales meeting.
3. Get a cool hat.

Tandem

50



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

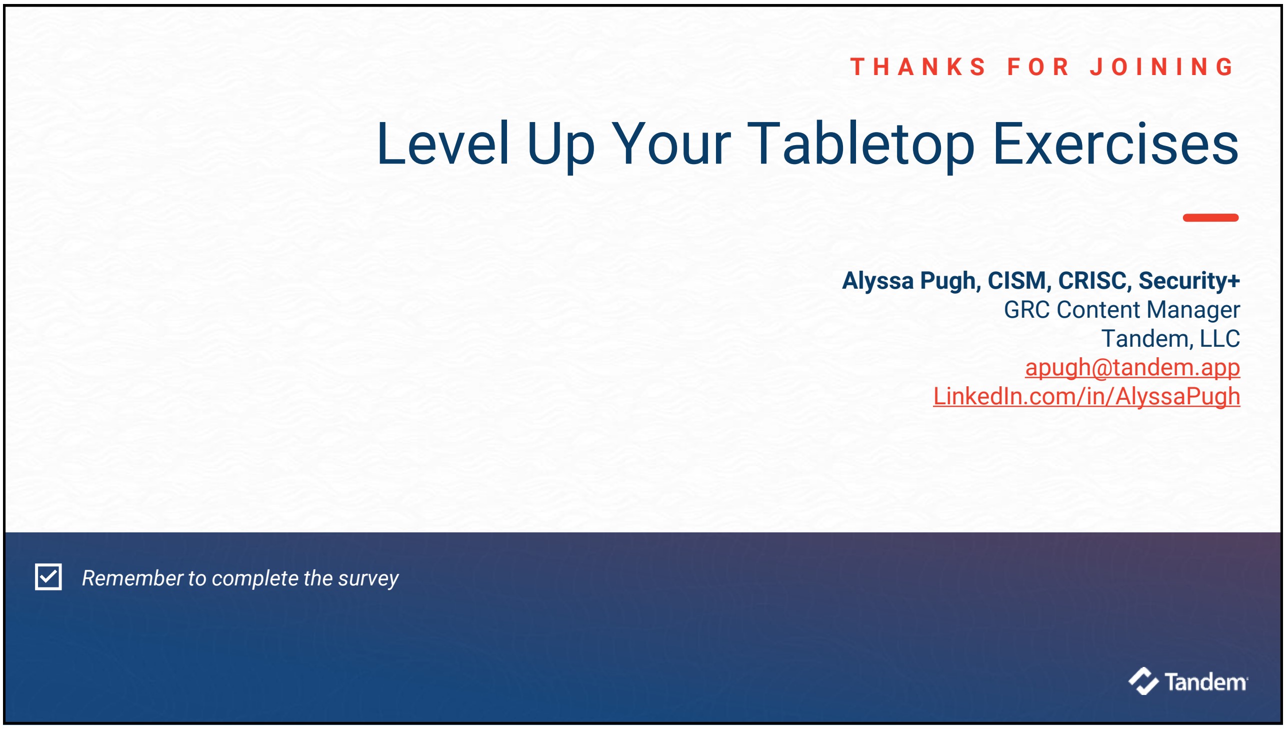
51

## KEYS CONFERENCE

April 7 – 9, 2026 | Lubbock, Texas

SEATS ARE LIMITED | REGISTER NOW | TANDEM.APP/KEYS

52



THANKS FOR JOINING

# Level Up Your Tabletop Exercises

**Alyssa Pugh, CISM, CRISC, Security+**
GRC Content Manager
Tandem, LLC
apugh@tandem.app
LinkedIn.com/in/AlyssaPugh

☑ *Remember to complete the survey*

Tandem

53