

LEVEL UP

Alyssa Pugh

Level Up Your Tabletop Exercises

Cybersecurity



1

Disclaimer

A Few Things First

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.

Original material is copyright © 2023 Tandem.



2



Alyssa Pugh

CISM, Security+
GRC Content Manager



3

Agenda

Here's the Plan

- About Tabletop Exercises
- 3 Tips for Your Tabletop
- Mini Tabletop Exercise



4



About Tabletop Exercises

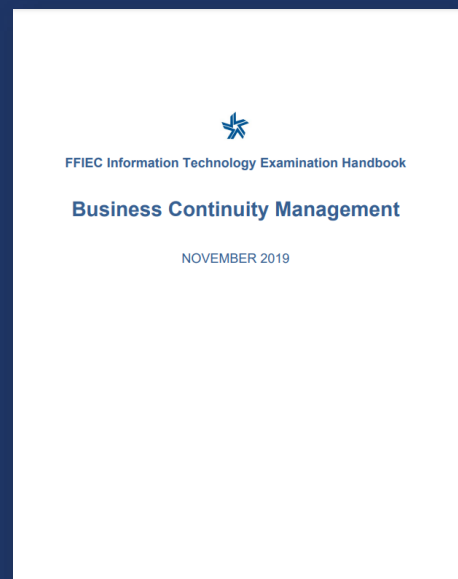
5

Definition

FFIEC BCM Booklet, Section VII.G.3 Tabletop Exercise

“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/vii-g-exercise-and-test-methods/vii-g-3-tabletop-exercise.aspx>



6

QUICK POLL

Show of hands if you have ever organized
or been part of a tabletop exercise.

QUICK POLL

On a scale of 1 – 5, how would you rate
your tabletop exercises?



7

Tabletop exercises are a pain point.
But they don't have to be.



8



3 Tips for Your Tabletop

9

TIP #1

As you're making a guest list for your tabletop, be sure to check it twice.



10

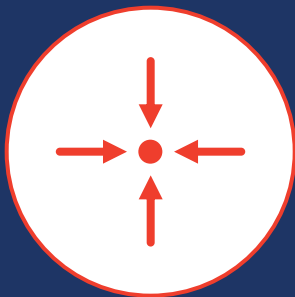
DISCUSSION QUESTION

When you have a tabletop exercise,
who do you invite?

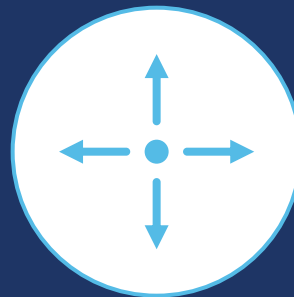


11

Who Gets Invited?



People Inside
the Business

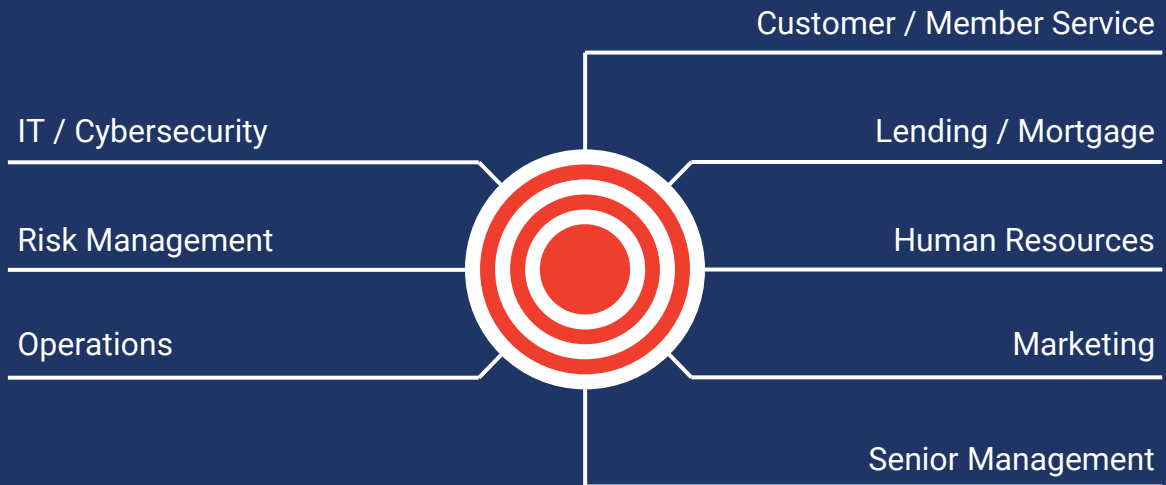


People Outside
of the Business



12

People Inside the Business



13

LEVEL UP



14

People Outside the Business



Board Members



Law Enforcement



Third Parties / MSPs



Emergency Response



Insurance Breach Coach



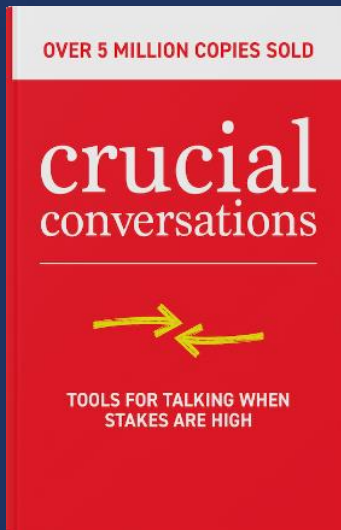
Auditor / Consultant

15

LEVEL UP



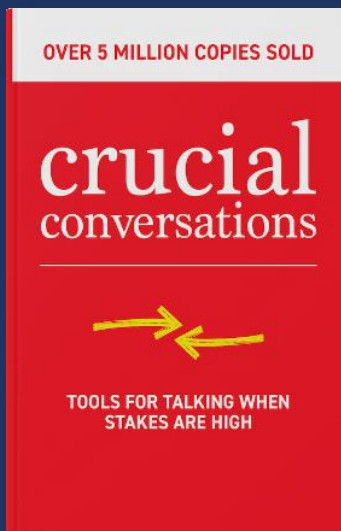
16



Pool of Shared Meaning



17



“As the Pool of Shared Meaning grows, it helps people in two ways. First, as individuals are exposed to more accurate and relevant information, they make better choices. In a very real sense, the Pool of Shared Meaning is a measure of a group’s IQ. The larger the shared pool, the smarter the decisions. And even though many people may be involved in a choice, when people openly and freely share ideas, the increased time investment is more than offset by the quality of the decision.”



18

INVITE OTHERS



19

TIP #2

**Channel your inner
Paul Hollywood.
Be looking for
style and
substance.**



20

DISCUSSION QUESTION

What do you do to make your exercises more interesting?



21

Style & Substance

1

Encourage
Discussion

2

Make it
Real

3

Use Plot
Twists



22

Encourage Discussion



Schedule for a reasonable time (e.g., 1 – 2 hours).



Describe tabletops as a “discussion” or an “exercise.”



Ask a lot of questions. Make the questions specific.

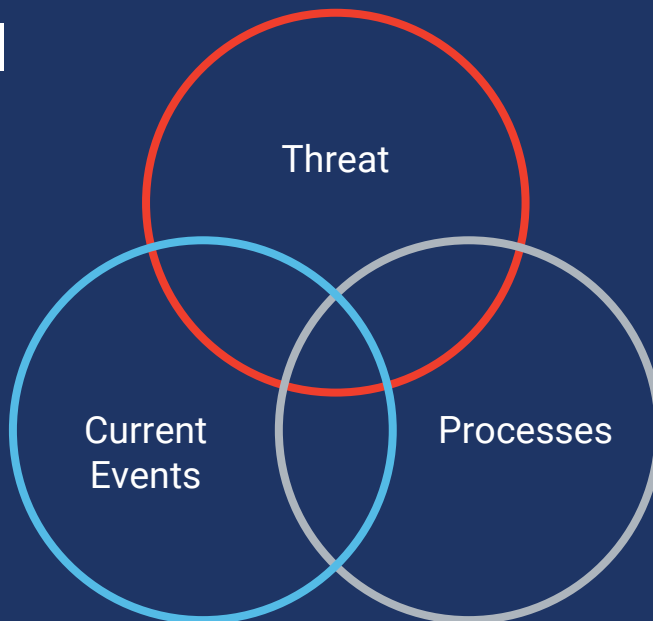


Make the exercise real.



23

Make it Real



24

Banks sought record Fed liquidity in wake of SVB collapse

By Michael S. Derby



An eagle tops the U.S. Federal Reserve building's facade in Washington, July 31 Ernst

NEW YORK, March 16 (Reuters) - Banks sought record amounts of liquidity from the Federal Reserve over recent days in the wake of Silicon Valley Bank and Signature Bank, which in turn helped curb bank efforts to shrink the size of its balance sheet, Fed data showed.

Factbox: Timeline of Ohio train derailment containing hazardous chemicals cargo

Reuters



An aerial view shows a plume of smoke, following a train derailment that forced residents to evacuate their homes in East Palestine, Ohio, U.S., February 6, 2023. REUTERS/Alan Fre

Feb 14 (Reuters) - A timeline of events since a Norfolk Southern Railroad-operated train derailed near East Palestine, Ohio, while carrying hazardous materials from Illinois to Pennsylvania.

Thousands without power as California storms bring rain, snow and cold

By Sharon Bernstein



Feb 25 (Reuters) - Nearly 85,000 households and businesses were without power in the Los Angeles area on Saturday, as storms continued to pummel parts of California, bringing snow to higher elevations and dumping rain and hail in the flatlands.

<https://www.reuters.com/markets/us/banks-sought-record-fed-liquidity-wake-svb-collapse-2023-03-16/>
<https://www.reuters.com/world/us/timeline-ohio-train-derailment-containing-hazardous-chemicals-cargo-2023-02-15/>
<https://www.reuters.com/world/us/thousands-without-power-california-storms-bring-rain-snow-cold-2023-02-25/>



25

Use Plot Twists

Fire at the Main Location

- An employee did not report to the evacuation location.
- Fire inspector says a suspicious device was found.
- The device was in the back office with the wire and ACH workstations.
- You have a customer who needs to get something out of her safe deposit box.



26

LEVEL UP



27

TIP #3

**Aim for the stars.
But be ready for
things to catch fire
in the process.**



28

4 Outcomes to Expect



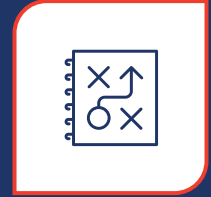
Potential
Errors



Imperfect
Results



Lessons
Learned



Action
Items



29

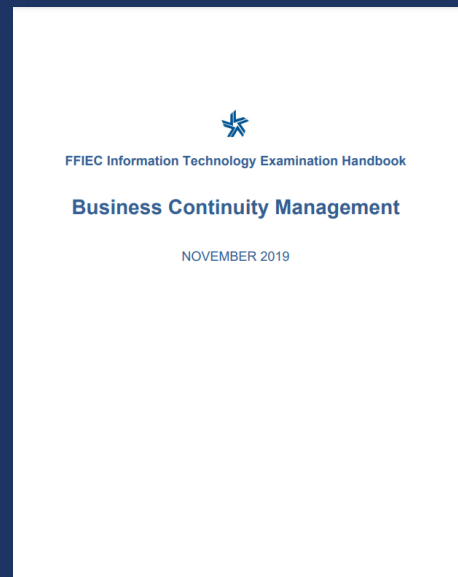
Guidance

FFIEC BCM Booklet, Section VII.G.3 Tabletop Exercise

“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/vii-g-exercise-and-test-methods/vii-g3-tabletop-exercise.aspx>



30



31



32

3 Tips for Your Tabletop

1

Invite Others

2

Build Experience

3

Expect Growth



33



Mini Tabletop Exercise

34

Instructions

- **Step 1:** Group Up with People
- **Step 2:** Designate a Group Speaker
- **Step 3:** Give Me a Thumbs Up when Done



35

Scenario

You are at the KEYS Conference. While you are out of the office, someone impersonating you emails your accounts payable department. The email asks them to update your direct deposit account information.



36

DISCUSSION QUESTIONS

1. What social engineering training does your company provide? Does it cover impersonation?
2. What are some ways the accounts payable team could recognize the request as a fraudulent attempt?
3. Would the accounts payable team report the email to anyone? If so, how?
4. **Plot Twist!** Other employees are reporting the issue occurred to them, too. How would this change your company's investigation and response?
5. **Plot Twist!** All of the account changes were made by one person. How would this change your company's investigation and response?

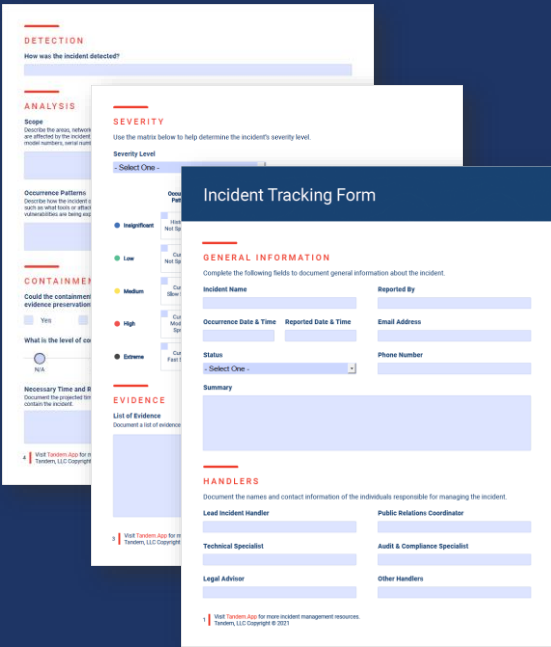


37

GROUP DISCUSSION



38





The image shows a stack of three forms from the Tandem Incident Tracking Form. The top form is the 'Incident Tracking Form' with sections for Detection, Analysis, Severity, General Information, Evidence, and Handlers. The middle form is the 'ANALYSIS' form with sections for Scope, Occurrence Patterns, and Containers. The bottom form is the 'DETECTION' form with a section for How was the incident detected?

RESOURCE

Tandem Incident Tracking Form

[Download Now](#)

39

THANKS FOR JOINING!

Level Up Your Tabletop Exercises

Alyssa Pugh
GRC Content Manager | Tandem, LLC
apugh@tandem.app

LEVEL UP



40