Brady Cook

Testing Your Operational Resilience

KEYS CONFERENCE

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.

KEYS CONFERENCE

2

Brady Cook

Tandem General Manager

KEYS CONFERENCE

3

FDITECH Sprint

FDIC Tech Lab

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

FDITECH

From Hurricanes to Ransomware: Measuring Resilience in the Banking World

KEYS CONFERENCE

4

FDITECH Sprint

Tandem Features

Action Plans | Scenarios | Test Incidents | Metrics | Peer Analysis

KEYS CONFERENCE

5

Agenda

HERE'S THE PLAN

- Exercise & Test Foundations
- Documenting Exercises & Tests
- Scenarios
- Incidents
- Reporting
- Training

KEYS CONFERENCE

6

Exercise & Test Foundations

7

"An exercise is a task or activity involving people and processes that is designed to validate one or more aspects of the BCP or related procedures. [...] A test is a type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment…"

- FFIEC IT Exam Handbook, BCM Booklet

8

"Effectively, the distinction between the two is that exercises address people, processes, and systems, whereas tests address specific aspects of a system."

- FFIEC IT Exam Handbook, BCM Booklet

KEYS CONFERENCE

9

Objectives

Exercises & Tests

- Provide assurance for the continuity and resilience of critical business functions
- Demonstrate RTOs and RPOs for services can be met
- Familiarize staff with recovery processes
- Verify personnel are adequately trained and knowledgeable of action plans
- Confirm action plans remain compatible with current environment
- Establish services can be restored at recovery locations
- Identify gaps and deficiencies

KEYS CONFERENCE

10

Methods

Exercises & Tests

- Tests
- Tabletop Exercises
- Functional Exercises
  - Full-Scale
  - Limited-Scale

KEYS CONFERENCE

11

Tests

Exercises & Tests

- Use quantifiable metrics to validate the operability of an IT system or system component as specified in the plan.
- Conduct them as close to an operational environment as possible.
- The scope can vary.
  - Individual system components
  - Entire systems
  - Comprehensive tests involving many systems
- Can help indicate problems in personnel training or in plans and procedures.

KEYS CONFERENCE

12

Exercises

Exercises & Tests

- Simulate an emergency to validate the viability of one or more aspects of a plan.
- Scenario-driven
- Involve personnel with roles and responsibilities in the plan meeting to validate the content of the plan.
- Often have additional situations presented to the personnel during the exercise.
- Can identify gaps and inconsistencies within plans and procedures.
- Can identify where personnel need additional training or changes to existing training.

KEYS CONFERENCE

13

Tabletop Exercises

Exercises & Tests

- Discussion-based exercises
- Personnel meet and discuss their roles and responses for an emergency scenario.
- A facilitator presents the scenario and asks participants questions to initiate discussion.
- Do not involve deploying equipment or other resources.

KEYS CONFERENCE

14

Functional Exercises

Exercises & Tests

- Personnel validate their operational readiness for emergency scenarios.
- Designed to exercise the functional aspects of the plan:
  - Roles and responsibilities of team members
  - Procedures
  - Assets
- Allow staff to execute their roles and responsibilities as they would in an actual situation.

KEYS CONFERENCE

15

BCP vs IRP

Exercises & Tests

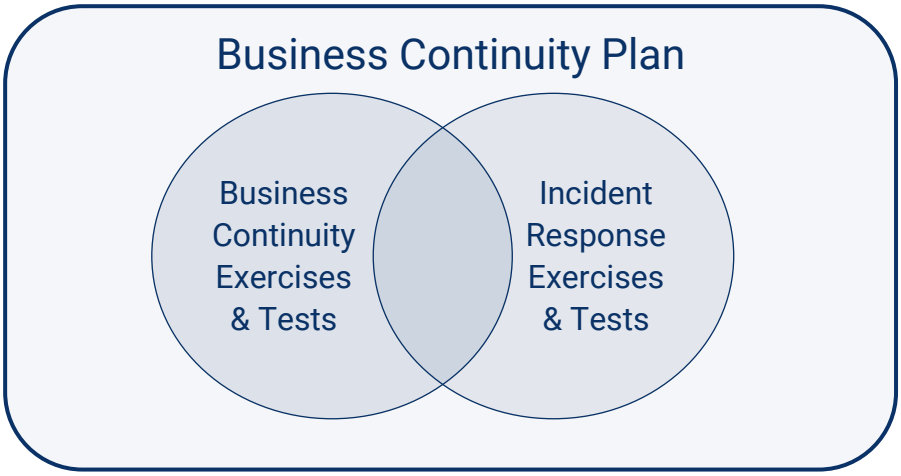
- FFIEC defines a security incident as "the attempted or successful unauthorized access, use, modification, or destruction of information systems or customer data."
- Some BCP tests only address the availability of systems or data to ensure a business function or process can either continue or be restarted.

KEYS CONFERENCE

16

BCP vs IRP

Exercises & Tests



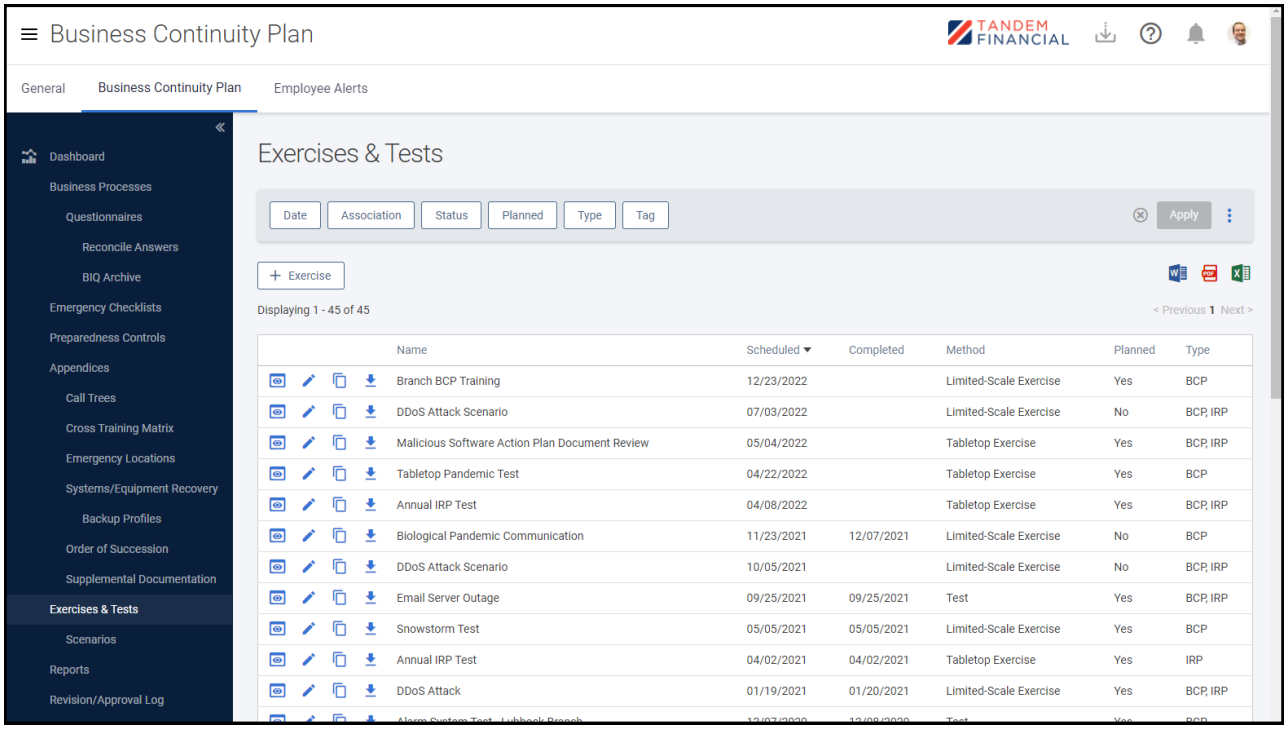
KEYS CONFERENCE

17

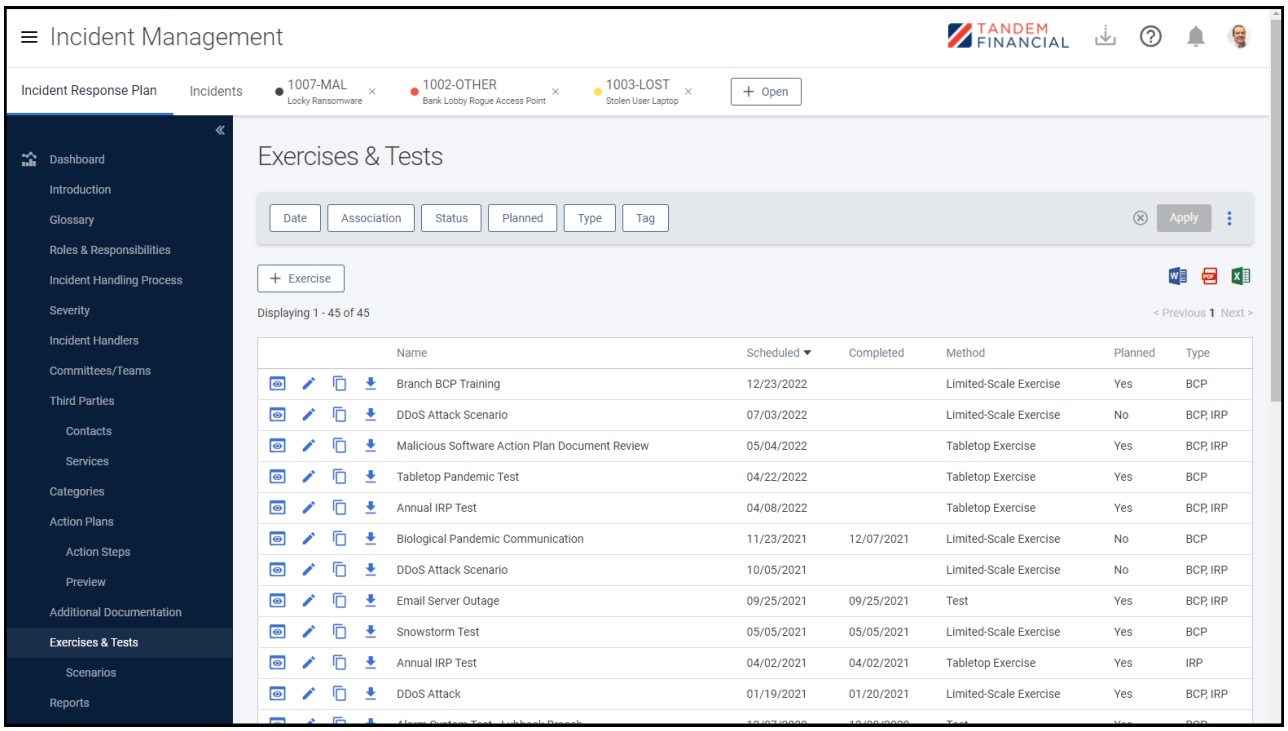
KEYS CONFERENCE

Documenting Exercises & Tests

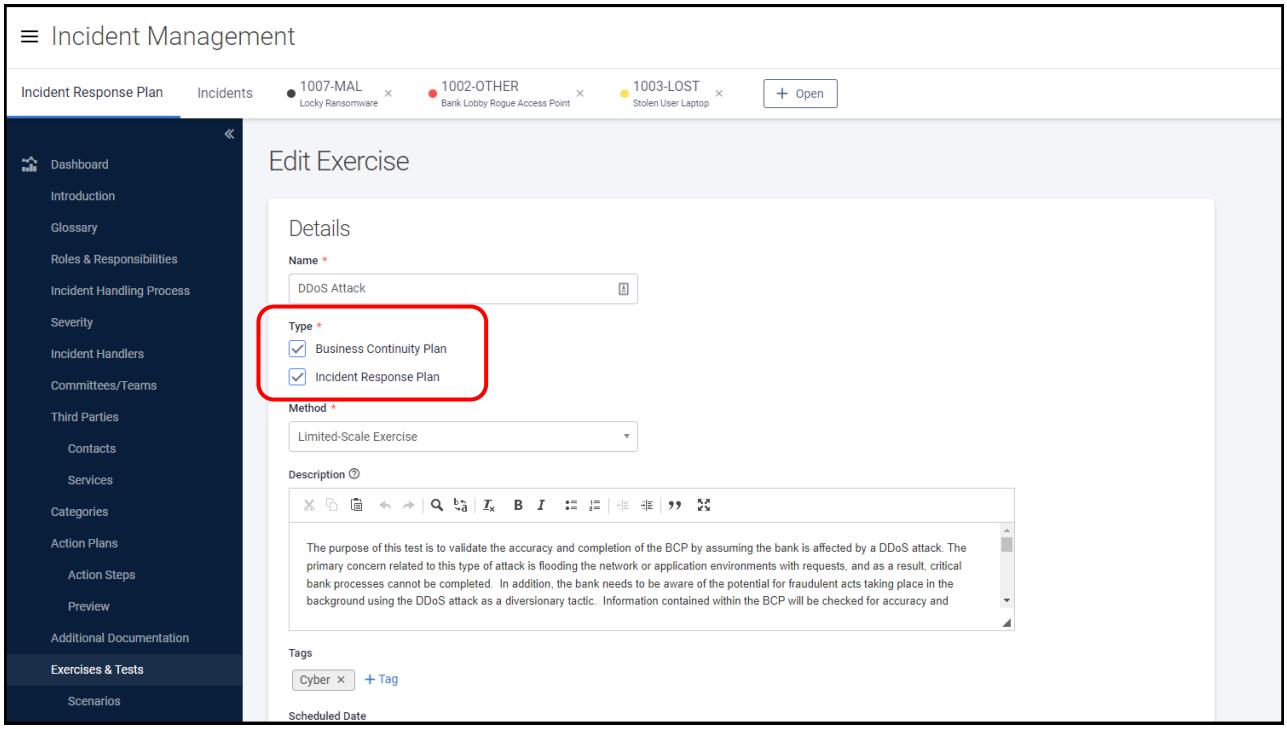
18


Business Continuity Plan
TANDEM FINANCIAL
General
Business Continuity Plan
Employee Alerts
Dashboard
Business Processes
Questionnaires
Reconcile Answers
BIQ Archive
Emergency Checklists
Preparedness Controls
Appendices
Call Trees
Cross Training Matrix
Emergency Locations
Systems/Equipment Recovery
Backup Profiles
Order of Succession
Supplemental Documentation
Exercises & Tests
Scenarios
Reports
Revision/Approval Log
Exercises & Tests
Date
Association
Status
Planned
Type
Tag
Apply
+ Exercise
Displaying 1 - 45 of 45
< Previous 1 Next >
Name
Scheduled
Completed
Method
Planned
Type
Branch BCP Training 12/23/2022 Limited-Scale Exercise Yes BCP
DDoS Attack Scenario 07/03/2022 Limited-Scale Exercise No BCP, IRP
Malicious Software Action Plan Document Review 05/04/2022 Tabletop Exercise Yes BCP, IRP
Tabletop Pandemic Test 04/22/2022 Tabletop Exercise Yes BCP
Annual IRP Test 04/08/2022 Tabletop Exercise Yes BCP, IRP
Biological Pandemic Communication 11/23/2021 12/07/2021 Limited-Scale Exercise No BCP
DDoS Attack Scenario 10/05/2021 Limited-Scale Exercise No BCP, IRP
Email Server Outage 09/25/2021 09/25/2021 Test Yes BCP, IRP
Snowstorm Test 05/05/2021 05/05/2021 Limited-Scale Exercise Yes BCP
Annual IRP Test 04/02/2021 04/02/2021 Tabletop Exercise Yes IRP
DDoS Attack 01/19/2021 01/20/2021 Limited-Scale Exercise Yes BCP, IRP

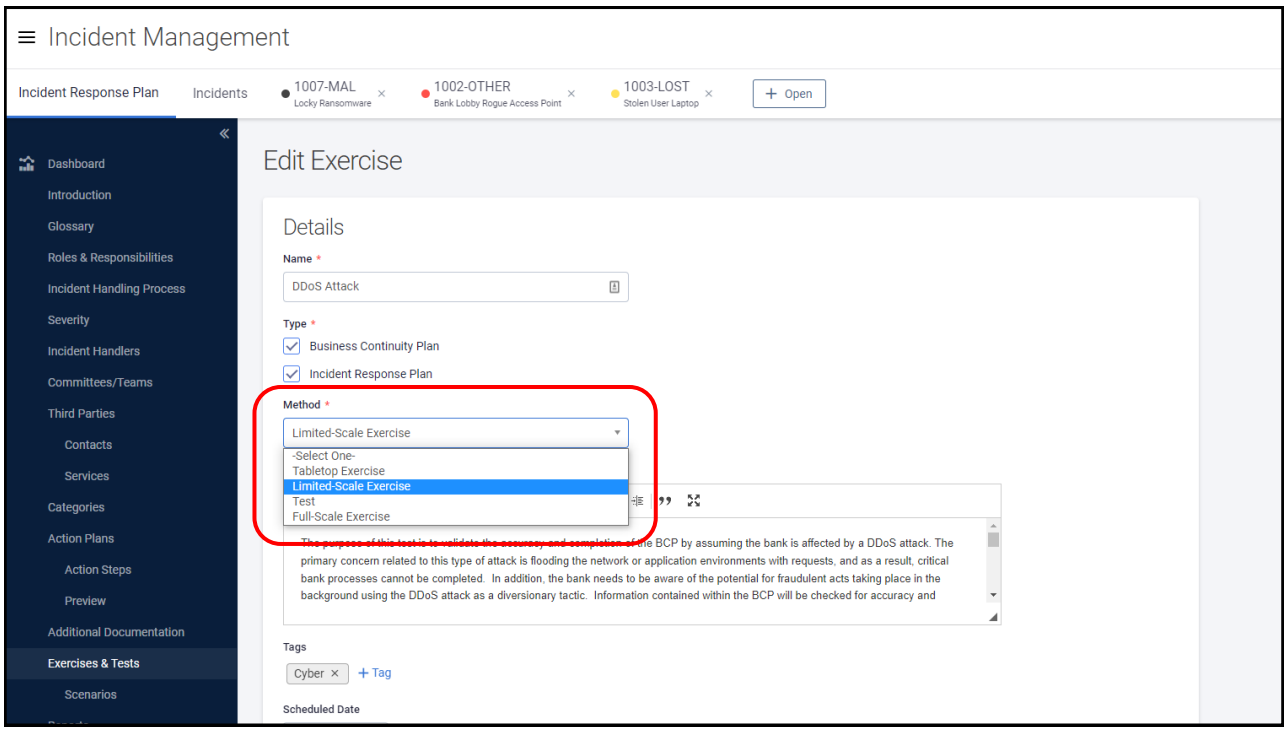
19


Incident Management
TANDEM FINANCIAL
Incident Response Plan
Incidents
1007-MAL
Locky Ransomware
1002-OTHER
Bank Lobby Rogue Access Point
1003-LOST
Stolen User Laptop
+ Open
Dashboard
Introduction
Glossary
Roles & Responsibilities
Incident Handling Process
Severity
Incident Handlers
Committees/Teams
Third Parties
Contacts
Services
Categories
Action Plans
Action Steps
Preview
Additional Documentation
Exercises & Tests
Scenarios
Reports
Exercises & Tests
Date
Association
Status
Planned
Type
Tag
Apply
+ Exercise
Displaying 1 - 45 of 45
< Previous 1 Next >
Name
Scheduled
Completed
Method
Planned
Type
Branch BCP Training 12/23/2022 Limited-Scale Exercise Yes BCP
DDoS Attack Scenario 07/03/2022 Limited-Scale Exercise No BCP, IRP
Malicious Software Action Plan Document Review 05/04/2022 Tabletop Exercise Yes BCP, IRP
Tabletop Pandemic Test 04/22/2022 Tabletop Exercise Yes BCP
Annual IRP Test 04/08/2022 Tabletop Exercise Yes BCP, IRP
Biological Pandemic Communication 11/23/2021 12/07/2021 Limited-Scale Exercise No BCP
DDoS Attack Scenario 10/05/2021 Limited-Scale Exercise No BCP, IRP
Email Server Outage 09/25/2021 09/25/2021 Test Yes BCP, IRP
Snowstorm Test 05/05/2021 05/05/2021 Limited-Scale Exercise Yes BCP
Annual IRP Test 04/02/2021 04/02/2021 Tabletop Exercise Yes IRP
DDoS Attack 01/19/2021 01/20/2021 Limited-Scale Exercise Yes BCP, IRP

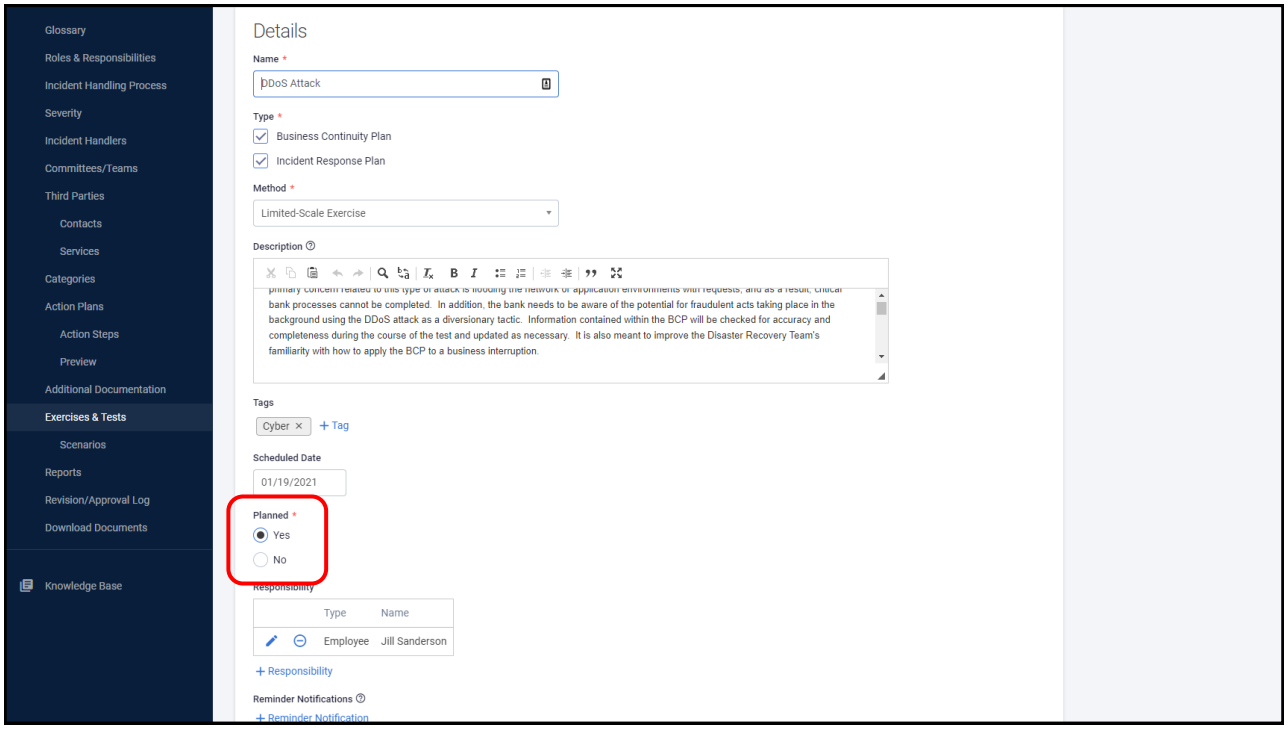
20


Incident Management
Incident Response Plan
Incidents
1007-MAL
Locky Ransomware
1002-OTHER
Bank Lobby Rogue Access Point
1003-LOST
Stolen User Laptop
Open
Dashboard
Introduction
Glossary
Roles & Responsibilities
Incident Handling Process
Severity
Incident Handlers
Committees/Teams
Third Parties
Contacts
Services
Categories
Action Plans
Action Steps
Preview
Additional Documentation
Exercises & Tests
Scenarios
Edit Exercise
Details
Name *
DDoS Attack
Type *
Business Continuity Plan
Incident Response Plan
Method *
Limited-Scale Exercise
Description
The purpose of this test is to validate the accuracy and completion of the BCP by assuming the bank is affected by a DDoS attack. The primary concern related to this type of attack is flooding the network or application environments with requests, and as a result, critical bank processes cannot be completed. In addition, the bank needs to be aware of the potential for fraudulent acts taking place in the background using the DDoS attack as a diversionary tactic. Information contained within the BCP will be checked for accuracy and
Tags
Cyber
+ Tag
Scheduled Date

21


Incident Management
Incident Response Plan
Incidents
1007-MAL
Locky Ransomware
1002-OTHER
Bank Lobby Rogue Access Point
1003-LOST
Stolen User Laptop
Open
Dashboard
Introduction
Glossary
Roles & Responsibilities
Incident Handling Process
Severity
Incident Handlers
Committees/Teams
Third Parties
Contacts
Services
Categories
Action Plans
Action Steps
Preview
Additional Documentation
Exercises & Tests
Scenarios
Edit Exercise
Details
Name *
DDoS Attack
Type *
Business Continuity Plan
Incident Response Plan
Method *
Limited-Scale Exercise
-Select One-
Tabletop Exercise
Limited-Scale Exercise
Test
Full-Scale Exercise
primary concern related to this type of attack is flooding the network or application environments with requests, and as a result, critical
bank processes cannot be completed. In addition, the bank needs to be aware of the potential for fraudulent acts taking place in the
background using the DDoS attack as a diversionary tactic. Information contained within the BCP will be checked for accuracy and
Tags
Cyber
+ Tag
Scheduled Date

22



23

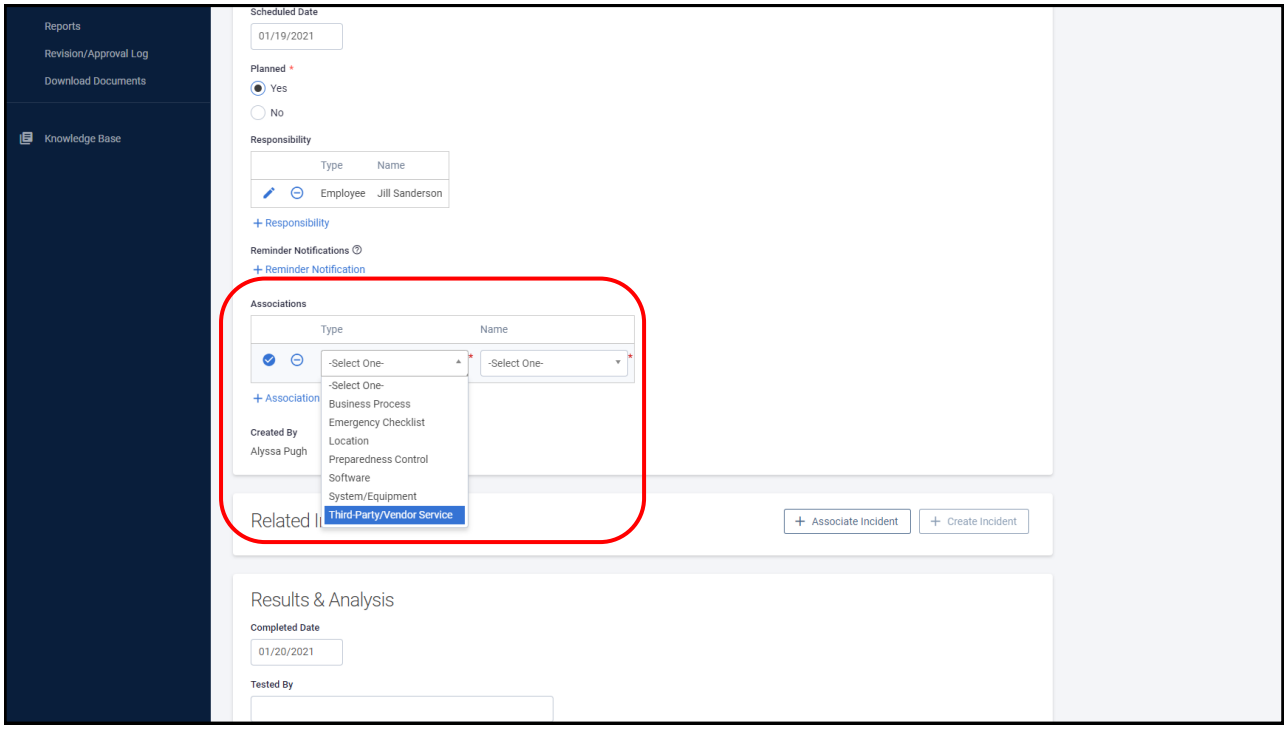
Unplanned

Exercises & Tests

- Often the best exercises and tests of your plan is when it is put into action during an actual event or business disruption.
- Record these situations and results of the events.

KEYS CONFERENCE

24



25

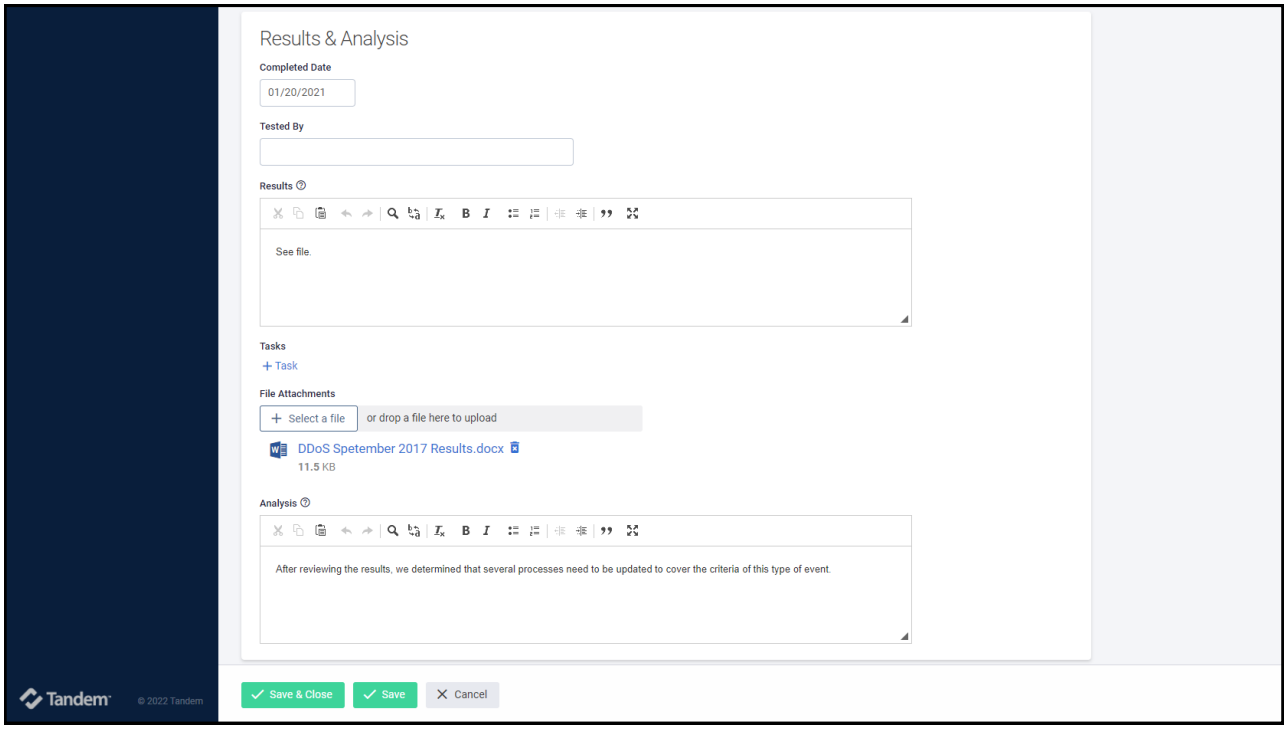
After Action Review

Exercises & Tests

- Record dates and locations
- Compare objectives and results
- Material deviations from the plans
- Problems identified and lessons learned
- Assignment of responsibility for timely resolution of issues identified

KEYS CONFERENCE

26



27

KEYS CONFERENCE

Scenarios

28

Developing Scenarios

Exercises & Tests

- Management should develop realistic exercise and test scenarios based on risk.
- Provide participants with situations that will inspire responses to help achieve the exercise objectives.
- Consider threats that could affect third-party service providers.
- Include communication processes with applicable stakeholders.

KEYS CONFERENCE

29

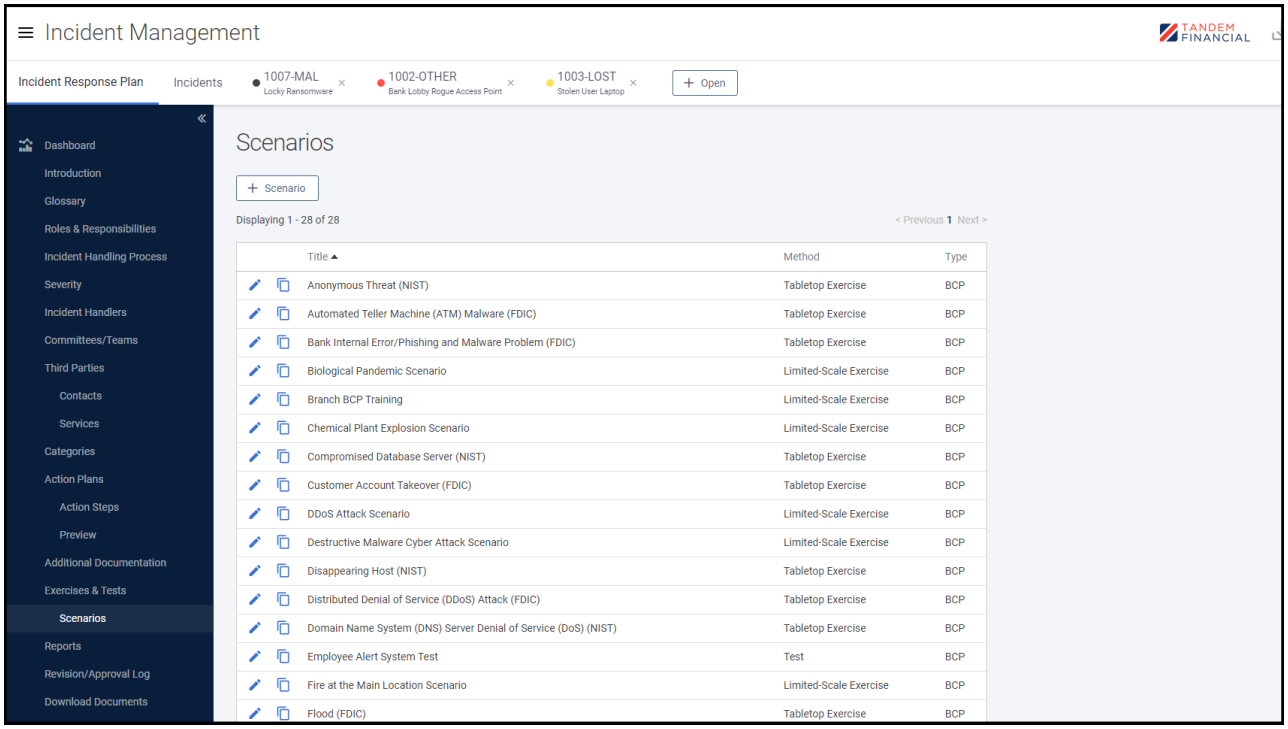
Template Scenarios

Exercises & Tests

- Tandem Scenarios
- NIST Computer Security Incident Handling Guide
- FDIC Cyber Challenge
- Create your template for common scenarios

KEYS CONFERENCE

30



31

Operational Activities

Exercises & Tests

"Tests are often performed as part of standard operational activities, such as restoring a backup, moving a server from one room to another, upgrading or patching operating systems or applications, or changing hardware components […]. **Combining tests with operational activities is generally more efficient than performing them separately and is also less likely to negatively impact operations.**"

- NIST SP 800-84

KEYS CONFERENCE

32

Incidents

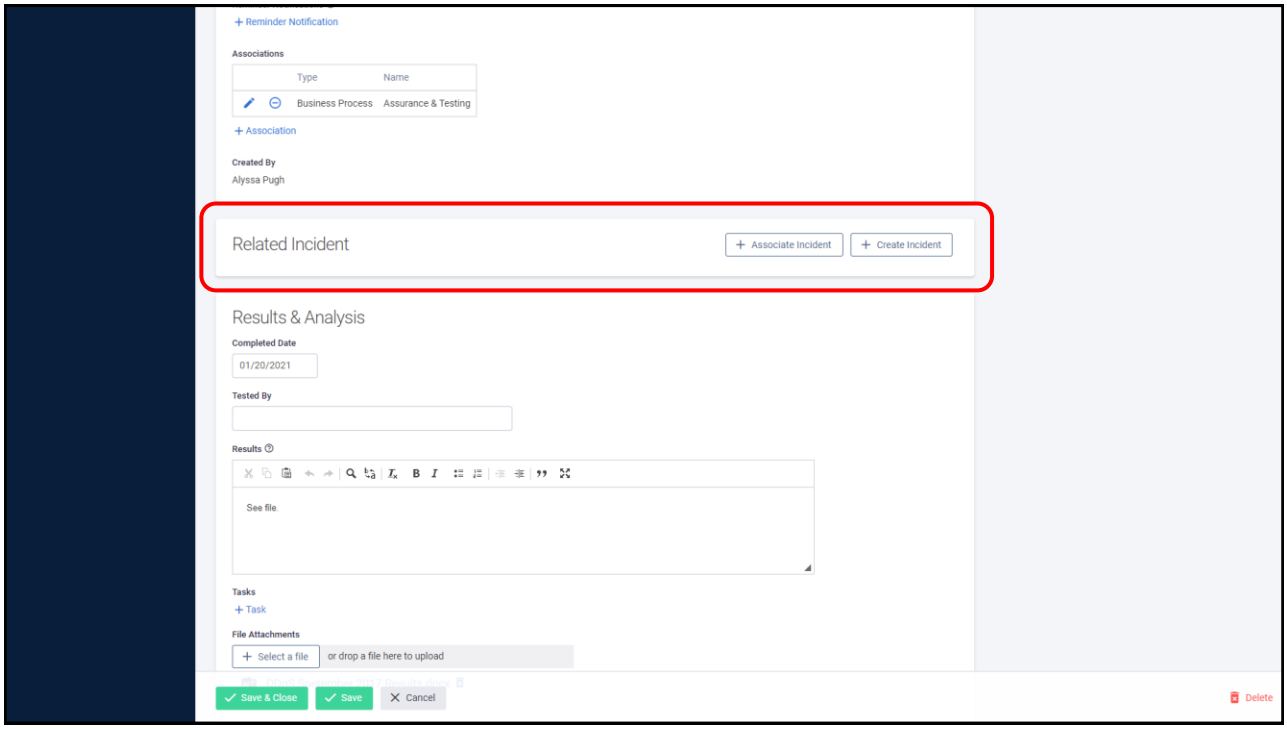
33

Associating Incidents

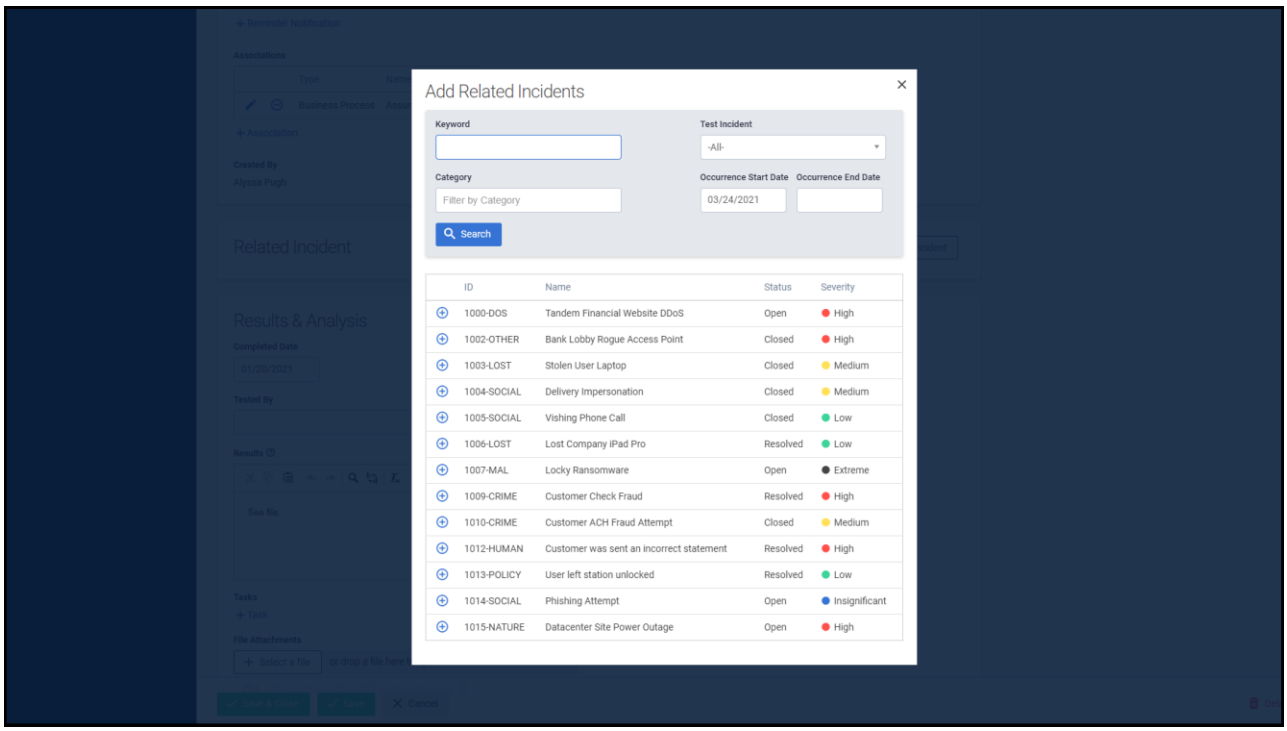
Exercises & Tests

- Associate Incidents with an Exercise/Test
- Only available for customers with both BCP and IM subscriptions
- Validate your action plans and processes

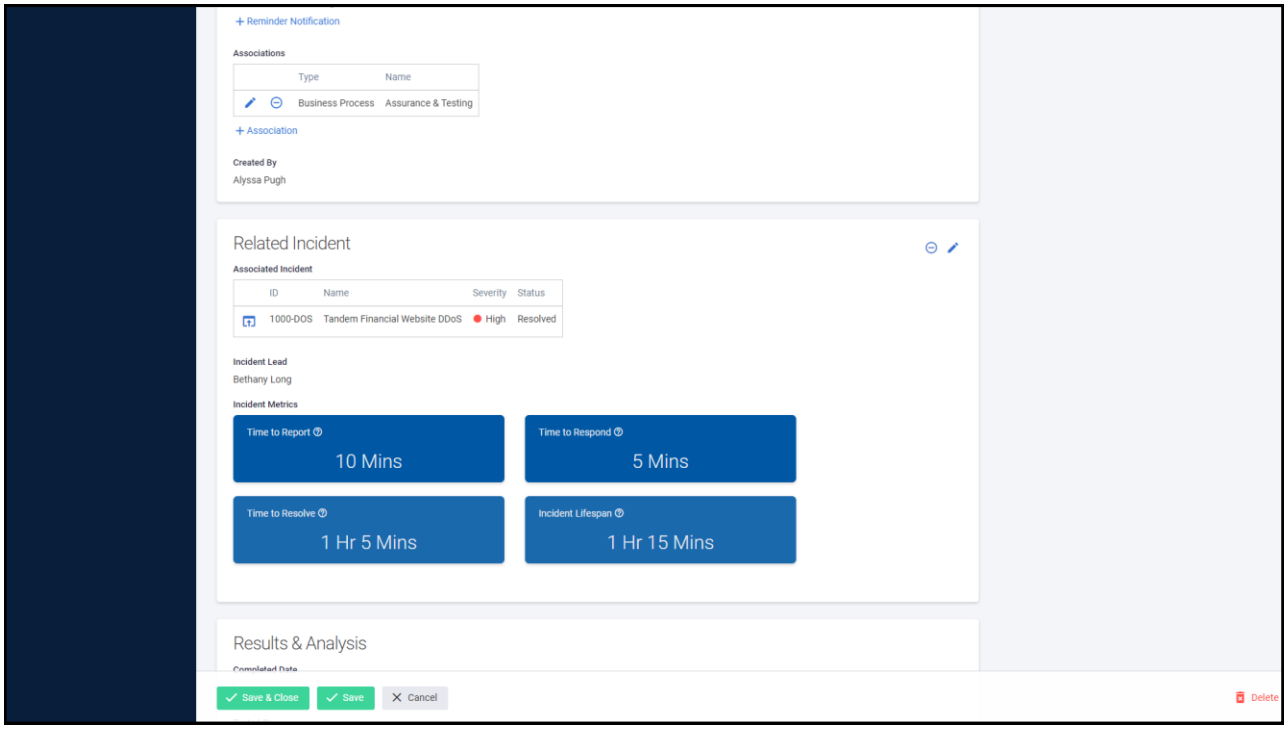
34


+ Reminder Notification
Associations
Type
Name
Business Process
Assurance & Testing
+ Association
Created By
Alyssa Pugh
Related Incident
+ Associate Incident
+ Create Incident
Results & Analysis
Completed Date
01/20/2021
Tested By
Results
See file.
Tasks
+ Task
File Attachments
+ Select a file
or drop a file here to upload
Save & Close
Save
Cancel
Delete

35


Add Related Incidents
Keyword
Test Incident
-All-
Category
Filter by Category
Occurrence Start Date
03/24/2021
Occurrence End Date
Search
ID
Name
Status
Severity
1000-DOS
Tandem Financial Website DDoS
Open
High
1002-OTHER
Bank Lobby Rogue Access Point
Closed
High
1003-LOST
Stolen User Laptop
Closed
Medium
1004-SOCIAL
Delivery Impersonation
Closed
Medium
1005-SOCIAL
Vishing Phone Call
Closed
Low
1006-LOST
Lost Company iPad Pro
Resolved
Low
1007-MAL
Locky Ransomware
Open
Extreme
1009-CRIME
Customer Check Fraud
Resolved
High
1010-CRIME
Customer ACH Fraud Attempt
Closed
Medium
1012-HUMAN
Customer was sent an incorrect statement
Resolved
High
1013-POLICY
User left station unlocked
Resolved
Low
1014-SOCIAL
Phishing Attempt
Open
Insignificant
1015-NATURE
Datacenter Site Power Outage
Open
High

36



37

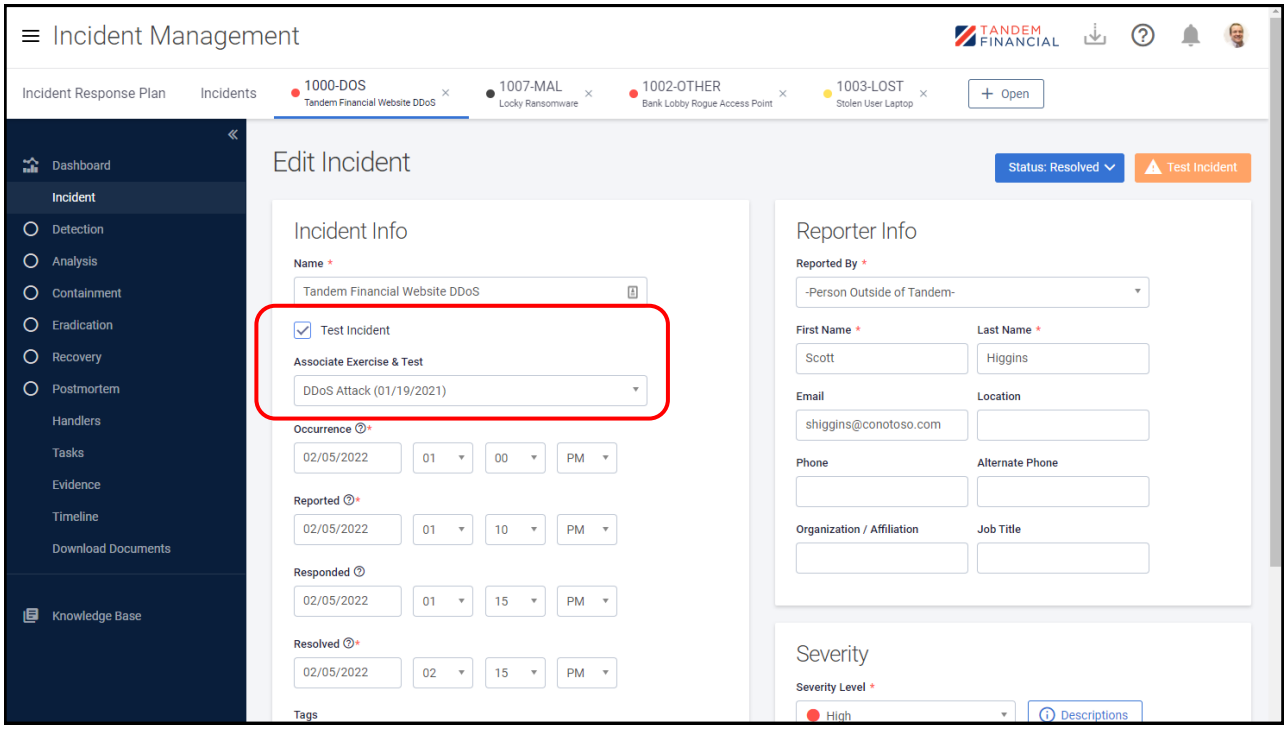
Test Incidents

Exercises & Tests

- Don't affect global metrics
- Excluded from global downloads
- Clearly identified as tests
- New search filters

KEYS CONFERENCE

38



39

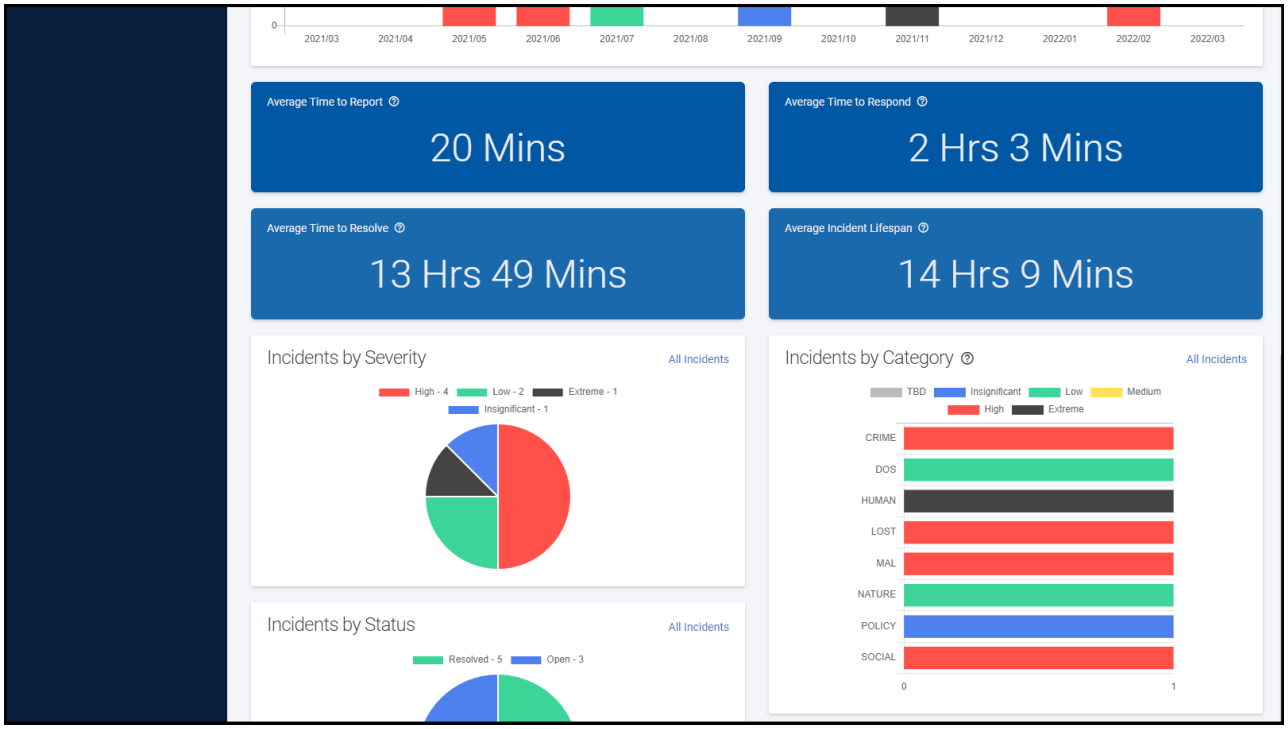
Global Incident Metrics

Exercises & Tests

- Average Time to Report
- Average Time to Respond
- Average Time to Resolve
- Average Incident Lifespan

KEYS CONFERENCE

40



41

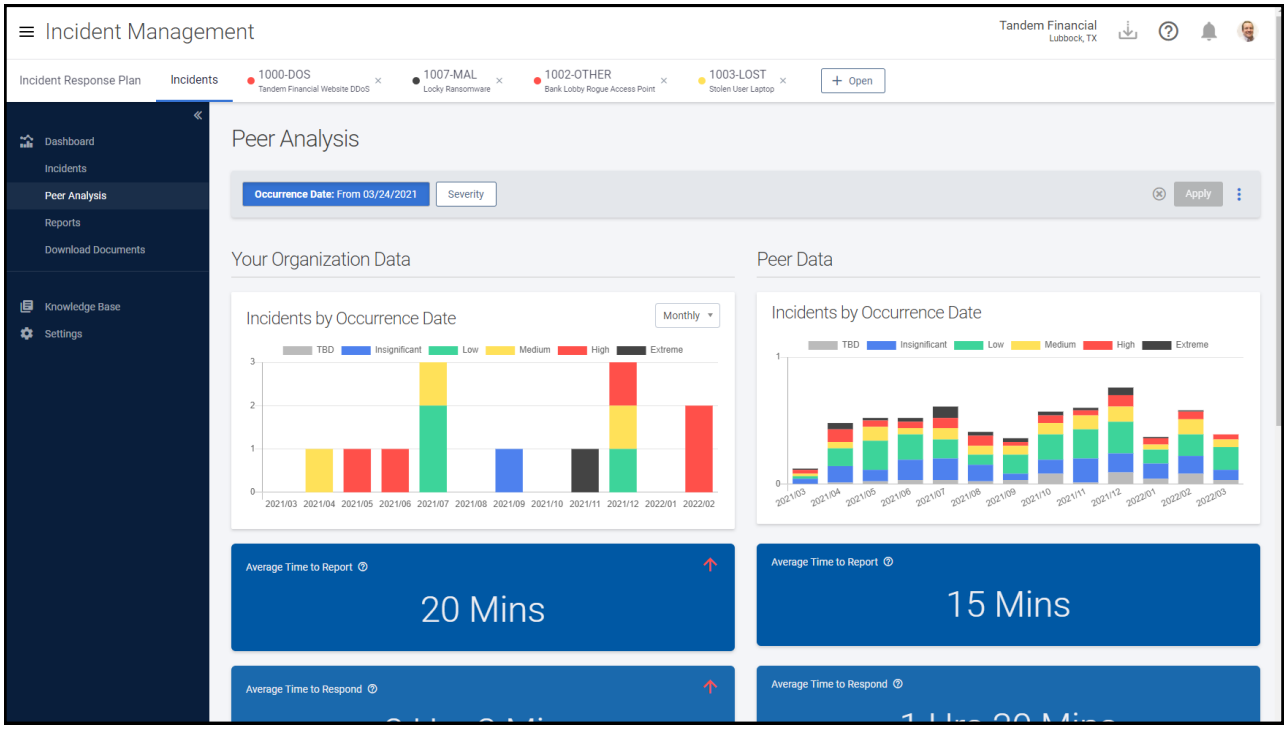
Peer Analysis

Exercises & Tests

- Incidents by Occurrence Date
- Metrics
- Incidents by Severity

KEYS CONFERENCE

42



43

KEYS CONFERENCE

Reporting

44

Program & Policy

Exercises & Tests

- IRP - Exercise & Test Program
- BCP - Exercise and Test Program

KEYS CONFERENCE

45

Program & Policy

Exercises & Tests

- Purpose
- Objectives
- Policy
- Frequency
- Responsibilities

KEYS CONFERENCE

46

Plan

Exercises & Tests

- Enter a future **Schedule Date** for planned exercises/tests
- Future tests are included in downloads
- Search by **Status**
- Set **Reminder Notifications** on the exercise/test

KEYS CONFERENCE

47

Documents

Exercises & Tests

- Word, PDF, and Excel downloads
  - Download Documents Page
  - Exercises & Tests Index Page
- Included in BCP and IRP downloads
- Incident Download
  - Summary
  - Details

KEYS CONFERENCE

48

KEYS CONFERENCE

Training

49

Employee Training

Security Incident Management Training Course

- What qualifies as a security incident?
- How can security incidents affect the organization?
- Their part of the IRP
- Preventing Security Incidents
- Detecting Security Incidents
- Responding to Security Incidents

KEYS CONFERENCE

50

Guidance

Exercises & Tests

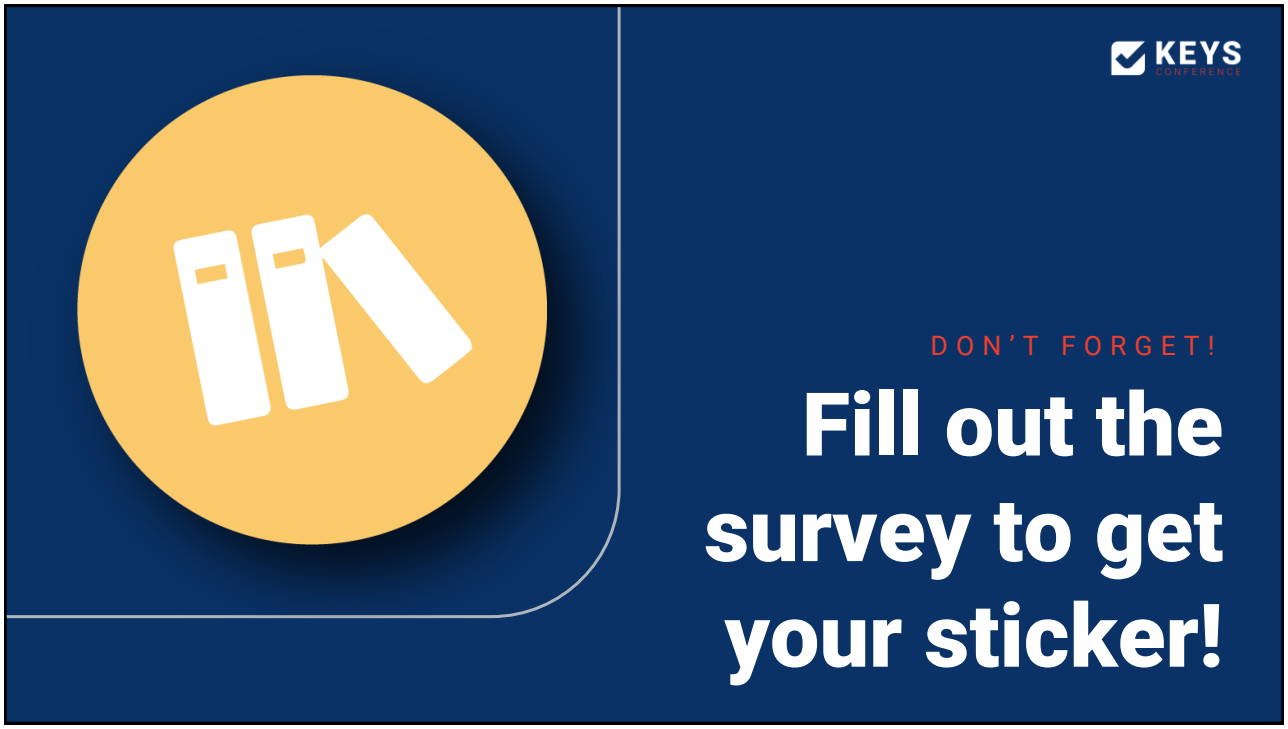
- FFIEC IT Exam Handbooks
  - Business Continuity Management
  - Information Security
  - Architecture, Infrastructure, and Operations
- NIST SP 800-61 R2
  - Computer Security Incident Handling Guide
- NIST SP 800-84
  - Guide to Test, Training, and Exercise programs for IT Plans and Capabilities

KEYS CONFERENCE

51

KEYS CONFERENCE

52


KEYS
CONFERENCE
DON'T FORGET!
Fill out the survey to get your sticker!

53


KEYS
CONFERENCE
THANKS FOR JOINING!
Testing Your Operational Resilience
Brady Cook
Tandem General Manager

54

Upcoming Sessions

TANDEM

Many Birds, One Stone: Using Asset-Based Risk Assessments for More Than Your Assets

Samantha Torrez, Tandem

RISK & COMPLIANCE

Phishing Psychology

Leticia Saiid, CoNetrix / Tandem

CYBERSECURITY

The ISO's Guide to Managing Ransomware

Alyssa Pugh, Tandem

KEYS CONFERENCE

55