

Lindsey McReynolds

Creating an Effective Incident Response Plan



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 © 2022 Tandem.



2



Lindsey McReynolds

CSXF, Tandem Support Manager



3

Agenda

HERE'S THE PLAN

- What is Incident Management?
- Effective Incident Response Planning
- Tandem Implementation
- Questions & Answers



4



What is Incident Management?

5

FFIEC INFORMATION SECURITY BOOKLET:

“The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.”



6

Incident Management Program



Incident Management Policy*



Incident Response Plan



Incident Tracking



* Included in Tandem's Policy product



Creating an Effective Plan

Elements of an Effective Plan

1

Resource Identification

Classification Strategies

2

3

Handling Processes

Communication Guidelines

4



HOW TO BUILD EFFECTIVE



Resource Identification



Roles & Responsibilities

- Senior Management
- Chief Information Officer (CIO)
- Chief Technology Officer (CTO)
- Information Security Officer (ISO)
- Incident Response Team
- IT Management
- IT Operations Staff
- IT Support Staff
- Business Unit Management
- Employees
- Third-Party Service Providers

Testing Your Operational Resilience

Up Next at 11:50 AM
TANDEM TRACK



11

Roles & Responsibilities



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > ROLES & RESPONSIBILITIES

☰ Incident Management

Incident Response Plan
Incidents
+ Open

- Dashboard
- Introduction
- Glossary
- Roles & Responsibilities
- Incident Handling Process
- Severity
- Incident Handlers
- Committees/Teams
- Third Parties
- Contacts
- Services
- Categories

Edit Role

Details

Name *

Active

Responsibilities

Responsibilities of senior management (e.g., CEO, COO, CFO, CIO, CTO, etc.) include:

- Developing strategic plans and objectives.
- Setting the budget for resources necessary to achieve stated objectives.
- Maintaining a high level understanding of the information technology and information security risks facing the bank.
- Escalating issues to the Board of Directors when unable to implement an objective or agree on a course of action.

12

Incident Response Team



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > COMMITTEES/TEAMS

☰ Incident Management

Incident Response Plan

Incidents

+ Open

- Dashboard
- Introduction
- Glossary
- Roles & Responsibilities
- Incident Handling Process
- Severity
- Incident Handlers
- Committees/Teams
- Third Parties
- Contacts
- Services
- Categories
- Action Plans

Members

Membership Roles

Role
✎ ⊖ Leader =
✎ ⊖ Leader Assistant =
✎ ⊖ Member =

+ Membership Role

Employees

Name	Role
✎ ⊖ Lindsey McReynolds	Leader
✎ ⊖ Adam Stevens	Leader Assistant
✎ ⊖ Austin Lee	Member
✎ ⊖ Chris Hidalgo	Member

13

Incident Handlers

- Lead Handler
- Technical Lead
- Subject Matter Experts:
 - Operations
 - BSA/AML
 - Human Resources
 - Audit & Compliance
 - Public Relations
 - Legal



14

The screenshot shows the 'Incident Handlers' section of a web application. At the top right is the 'KEYS CONFERENCE' logo. The main heading is 'Incident Handlers' in large blue font. Below it is a breadcrumb trail: 'INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > INCIDENT HANDLERS'. A hamburger menu icon is followed by 'Incident Management'. The interface includes a top navigation bar with 'Incident Response Plan', 'Incidents', and a '+ Open' button. A dark blue sidebar on the left contains a menu with items: Dashboard, Introduction, Glossary, Roles & Responsibilities, Incident Handling Process, Severity, Incident Handlers (highlighted), Committees/Teams, Third Parties, Contacts, and Services. The main content area is titled 'Edit Handler Role' and contains a 'Details' section with a 'Name' field containing 'Human Resources' and an 'Active' checkbox. Below this is a 'Responsibilities' section with a rich text editor toolbar and a list of responsibilities for human resources.

Incident Handlers

INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > INCIDENT HANDLERS

Incident Management

Incident Response Plan Incidents + Open

- Dashboard
- Introduction
- Glossary
- Roles & Responsibilities
- Incident Handling Process
- Severity
- Incident Handlers**
- Committees/Teams
- Third Parties
- Contacts
- Services

Edit Handler Role

Details

Name *
Human Resources

Active

Responsibilities

Responsibilities of human resources include:

- Overseeing any personnel and disciplinary issues related to incidents involving bank personnel.
- Preserving and documenting evidence.
- Communicating with legal advisors and the lead incident handler on incidents involving bank personnel.

15

The slide features the 'KEYS CONFERENCE' logo in the top right corner. The main title is 'HOW TO BUILD EFFECTIVE Classification Strategies', with 'Classification Strategies' in a large, bold, blue font. On the right side, there is a large, light gray graphic of a tag with a hole at the top and three horizontal lines on it.

HOW TO BUILD EFFECTIVE Classification Strategies



16

Why Classify?

1

Communicate
Nature of the
Incident

2

Know what
Plans to
Implement

3

Enable
Trend
Analysis



17

Classification Methods

NIST SP 800-61 Rev. 2

Category

- Common attack vectors
- Basis for defining procedures
- Examples:
 - Account Takeover
 - Criminal Activity
 - Data Breach
 - Lost/Stolen Asset
 - Third Party
 - Unauthorized Use

Severity

- Prioritization
- Factors:
 - Functional Impact
 - Information Impact
 - Recoverability
- Example Levels:
 - TBD
 - Insignificant
 - Low
 - Medium
 - High
 - Extreme



18

Categories

INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > CATEGORIES

Incident Management

Incident Response Plan Incidents 1020-LOST Stolen Laptop + Open

- Dashboard
- Incidents
- Peer Analysis
- Reports
- Download Documents
- Knowledge Base
- Settings

Incidents

Keyword Severity Status Occurrence Date Reported Date Category Primary Category Tag

+ Create Incident

Displaying 1 - 17 of 17

ID	Name	Severity
1020-LOST	Stolen Laptop	Extreme
1016-THIRD	SolarWinds	High
1015-NATURE	Datacenter Site Power Outage	High
1014-SOCIAL	Phishing Attempt	Insignificant

19

Categories

INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > CATEGORIES

Incident Management

Incident Response Plan Incidents + Open

- Dashboard
- Introduction
- Glossary
- Roles & Responsibilities
- Incident Handling Process
- Severity
- Incident Handlers
- Committees/Teams
- Third Parties
- Contacts
- Services
- Categories

Subcategories

Name
Desktop
External / Removable Media
Laptop
Mobile Device

+ Subcategory

20

Severity Levels



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > SEVERITY

21

Trend Reporting



INCIDENT MANAGEMENT > INCIDENTS > DASHBOARD

Incident Management

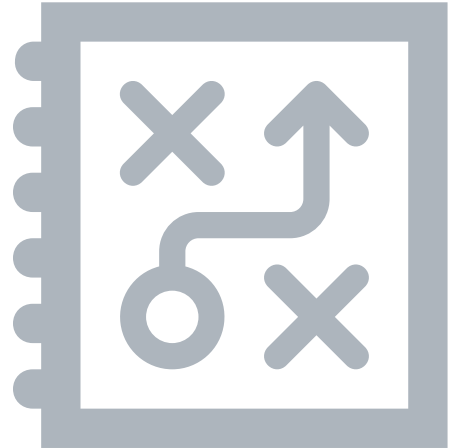
Incident Response Plan Incidents + Open

22

HOW TO BUILD EFFECTIVE



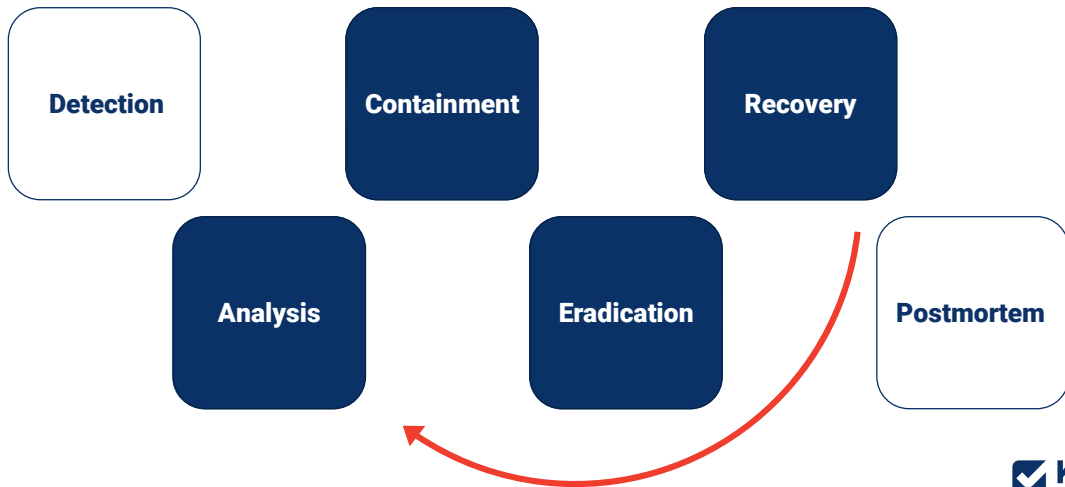
Handling Processes



23

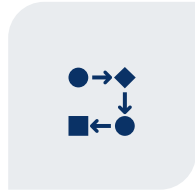
Incident Handling Process

NIST SP 800-61 Rev. 2



24

Handling Approaches



Handling Processes



Action Plans
(a.k.a Playbooks)



Action Steps



25

Handling Approaches

Detection

Eradication

Analysis

Recovery

Containment

Postmortem

Stage: Analysis

Handling Process:
Determine scope, origins, occurrence patterns....

Action Plan: Phishing

1. Determine if the message was forwarded to another employee
2. Determine if malware was introduced as a result of the attack.
3.



26

Incident Handling Process



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > INCIDENT HANDLING PROCESS

Incident Management

Incident Response Plan Incidents + Open

- Dashboard
- Introduction
- Glossary
- Roles & Responsibilities
- Incident Handling Process**
- Severity
- Incident Handlers
- Committees/Teams
- Third Parties
- Contacts
- Services
- Categories
- Action Plans
- Action Steps

Edit Analysis Handling Process

✕ 📄 🗑️ ↶ ↷ 🔍 🗑️ ✎ Styles - [Grid] [List] [Table] [Quote] [Image] [Link]

If a detected incident is determined to be legitimate, an initial analysis will be performed to identify factors such as the incident's scope, origins, occurrence patterns, and recurrence details. With this information, handlers will categorize the incident. See the Categories section for additional information.

During analysis, handlers will also determine the incident's severity. A severity rating will be assigned to the incident based on an evaluation of the following factors:

- Functional Impact:** The level to which processes or systems may be affected by the incident.
- Information Impact:** The incident's effect on the confidentiality, integrity, or availability of private or restricted data.
- Recoverability:** The amount of time it may take to fully recover from the incident.

Based on the estimated impact, the severity rating will be used to prioritize the incident and help ensure appropriate escalation procedures are followed. If the incident is determined to be a "Notification Incident," notice will be provided to the primary federal regulator as soon as possible and within 36 hours of the determination, in accordance with 12 CFR Part 304 Subpart C - Computer-Security Incident Notification.

As the handling process progresses, the severity rating may be reevaluated, as additional information becomes available. See the Severity and Communication Guidelines sections for additional information.

27

Action Plans



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > ACTION PLANS

Incident Response Plan Incidents + Open

Dashboard Introduction Glossary Roles & Responsibilities **Incident Handling Process** Severity Incident Handlers Committees/Teams Third Parties Contacts Services Categories Action Plans Action Steps

Edit Action Step

Name *

Determine if the message was forwarded to another employee.

Stage

Analysis

Additional Details

✕ 📄 🗑️ ↶ ↷ 🔍 🗑️ ✎ B I [Grid] [List] [Table] [Quote] [Image] [Link]

Work with IT Team to investigate if message was forwarded on to anyone else.

Tags

+ Tag

Responsibility

Type	Name
Position	IT Staff

+ Responsibility

File Attachments

+ Select a file or drop a file here to upload

Instructions.docx 37.5 KB

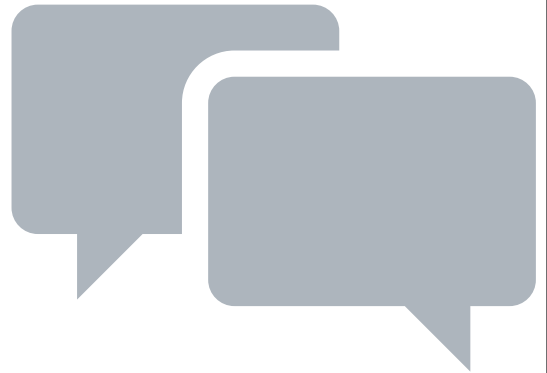
Save Cancel

28

HOW TO BUILD EFFECTIVE



Communication Guidelines



29

Communication



Internal
Communication



Third Party
Communication



Customer
Communication



30

Internal Communication



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > ADDITIONAL DOCUMENTATION

- Employees
- Incident Response Team
- Handlers
- Affected Areas
- Management

31

Handler Notifications



INCIDENT MANAGEMENT > INCIDENTS > [OPEN INCIDENT] > HANDLERS > NOTIFY INCIDENT HANDLERS

☰ Incident Management

Incident Response Plan Incidents 1008-CRIME x + Open
Customer Wire Fraud

- Dashboard
- Incident
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Postmortem
- Handlers**
- Tasks
- Evidence
- Timeline
- Download Documents

Notify Incident Handlers

Recipients *

Handler

✎ ⓧ Adam Stevens

+ Handler

Email Reply To

lmcreynolds@tandem.app

Subject *

Incident #1008-CRIME

Email Message *

✕ 📎 ↶ ↷ 🔍 🗨️ ⚡ **B** **I** 🌐 📏 🗑️ 🔄

You have been added as a handler for one of your bank's incidents. Follow the instructions below to access this incident in Tandem.

- Go to <https://secure.tandem.app> and sign in
- Once signed into Tandem, click the primary menu in the upper left corner of the screen and select Incident Management. On the following page, you will see the list of opened incidents.

32

Third Party Communication



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > ADDITIONAL DOCUMENTATION

- Law Enforcement
- Regulators
- Financial Crimes Enforcement Network (FinCEN)
- Payment Providers
- Insurance Agencies
- Vendors

33

Customer Communication



INCIDENT MANAGEMENT > INCIDENT RESPONSE PLAN > ADDITIONAL DOCUMENTATION

- Describe the incident
- Provide timeline
- Describe remediation measures
- Provide organization contact info
- Remind to stay cautious
- Explain fraud alerts
- Explain credit reports
- Provide FTC contact info

34

Documenting Communication



INCIDENT MANAGEMENT > INCIDENTS > [OPEN INCIDENT] > TIMELINE

Incident Management

Incident Response Plan Incidents ● 1007-MAL × Locky Ransomware + Open

Timeline

1007-MAL | Locky Ransomware Show Hidden

Add comment...

01/18/2022 | 11:09 AM | Lindsey McReynolds
Escalated to ISO

01/18/2022 | 10:14 AM | Chris Hidalgo
Incident Created
Severity - Extreme
Primary Category - Malicious Code: Ransomware

01/18/2022 | 9:20 AM | Ed Smith
Incident Reported

11/27/2021 | 8:11 AM |
Incident Occurred

35

Elements of an Effective Plan

1

Resource Identification

2

Classification Strategies

3

Handling Processes

4

Communication Guidelines



36



37

A purple circle with a white refresh icon (two curved arrows) on a dark blue background. To the right, the text reads "DON'T FORGET!" in red, followed by "Fill out the survey to get your sticker!" in white. The "KEYS CONFERENCE" logo is in the top right corner.

38



THANKS FOR JOINING!

Creating an Effective Incident Response Plan

Lindsey McReynolds
CSXF, Tandem Support Manager

39

Upcoming Sessions

TANDEM

Testing Your Operational Resilience

Brady Cook, Tandem

RISK & COMPLIANCE


A Chat with Your Friendly Examiner

Ruth Norris, Texas Department of Banking

CYBERSECURITY

Cybersecurity Session

TBD



40