LINDSEY JACOBS & ALYSSA PUGH

Incident Response Round-Up

KEYS 2026 HORIZONS

Sign into Tandem to participate in this session.

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the presenters' opinions.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

KEYS

2

Lindsey Jacobs
Software Specialist
Tandem, LLC

Alyssa Pugh
GRC Content Manager
Tandem, LLC

KEYS

3

SESSION AGENDA

1. Incident Response Foundations
2. Incident Response Compliance Update
3. Incident Response Scenarios

KEYS

4

Incident Response Foundations

KEYS

5

6

DEFINITION OF "INCIDENT"

Anything that threatens the confidentiality, integrity, or availability of systems or data.

Adapted from NIST

KEYS

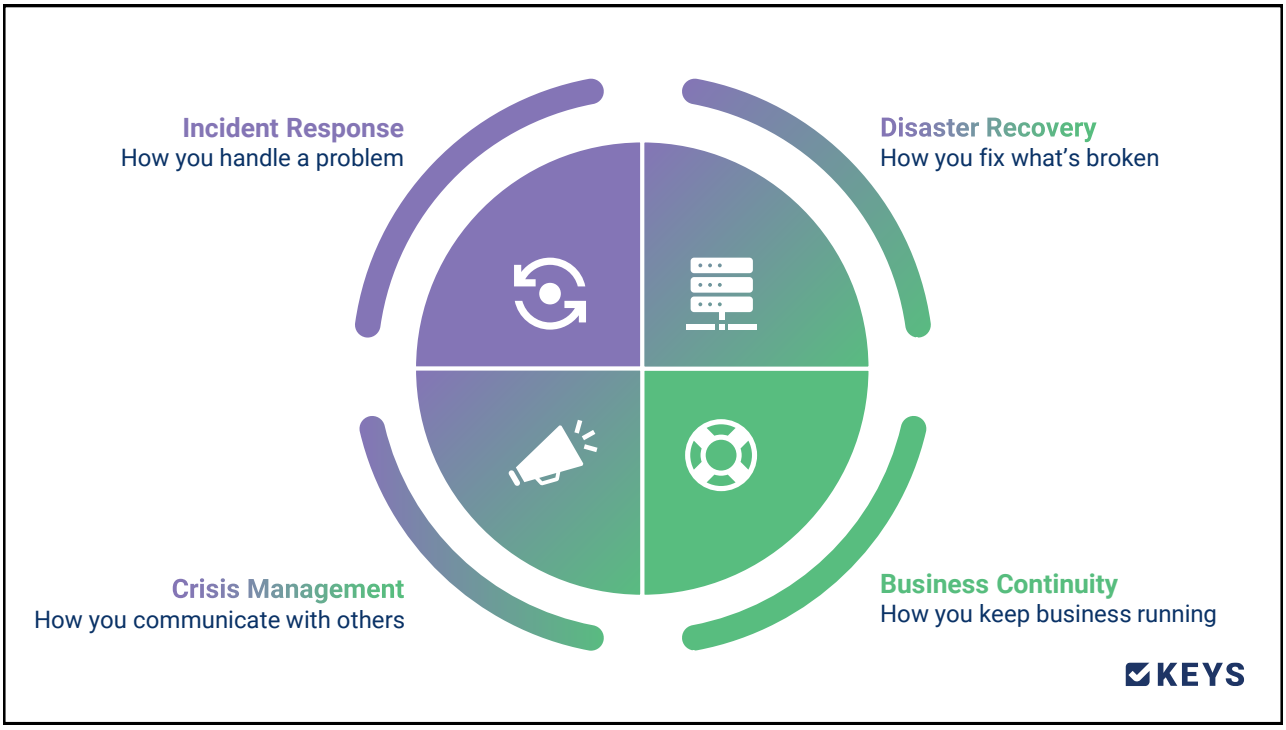
7

INCIDENT EXAMPLES

- Data Breach
- Account Takeover
- Human Error
- Social Engineering
- Malicious Code
- System Failure
- Natural Event
- Policy Violation
- Criminal Activity
- Third Party

KEYS

8



9

INCIDENT MANAGEMENT

A **process** of continuously preparing for, carrying out, and improving the organization's incident response activities.

INCIDENT RESPONSE PLAN

A **document** containing the organization's documented set of procedures for detecting, responding to, and recovering from incidents.

KEYS

10

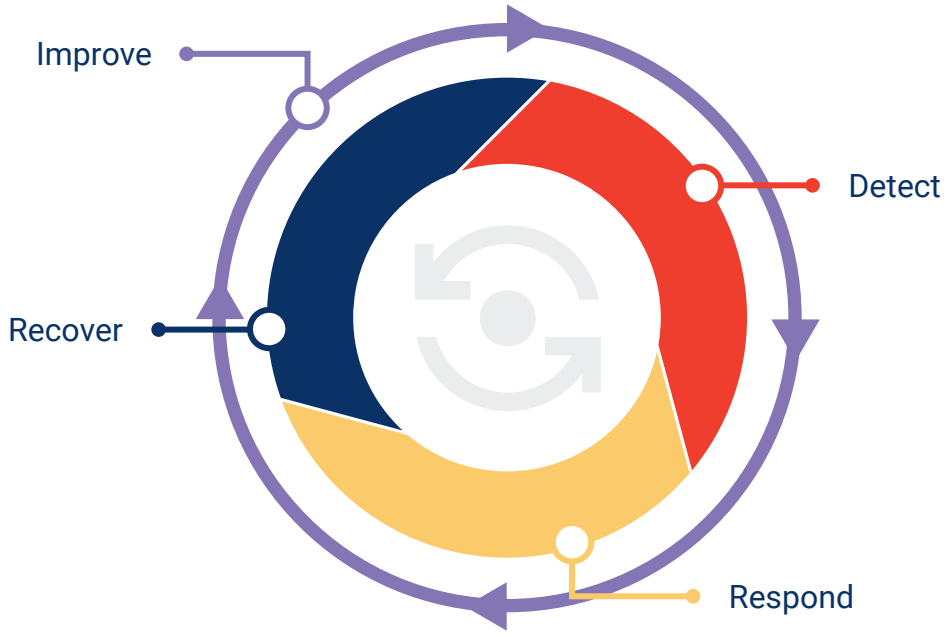
KEY TAKEAWAY

A plan without Incident Management is just paper.
Incident Management without a plan is a disaster.

KEYS

11

INCIDENT MANAGEMENT LIFECYCLE



KEYS

12

INCIDENT MANAGEMENT LIFECYCLE | IMPROVE EXAMPLES

- Confirm the root cause and all evidence were fully documented with the incident
- Document lessons learned from the incident
- Notify and educate employees of the attack

KEYS

13

INCIDENT RESPONSE | DETECT EXAMPLES

- **P**eople
- **L**ogs
- **A**lerts
- **N**ews

What happened?
Perform initial investigation and construct a chain of events.

How did it happen?
Determine the entry point and perform a root cause analysis.

What was affected?
Perform an impact assessment.

How do you know?
Look for indicators of compromise (IOCs) and document evidence.

KEYS

14

INCIDENT RESPONSE | RESPOND EXAMPLES

Isolate Affected Areas

Disable Compromised Accounts

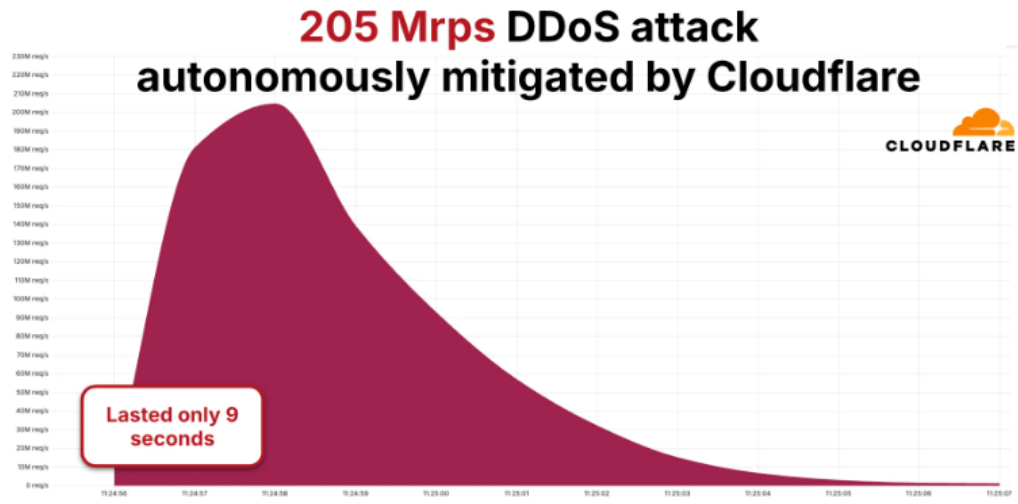
Heighten Security Awareness

Block Malicious Traffic

KEYS

15

INCIDENT RESPONSE | RESPOND EXAMPLES



https://blog.cloudflare.com/ddos-threat-report-2025-q4/

KEYS

16

INCIDENT RESPONSE | RESPOND EXAMPLES

Top 10 most-attacked industries: 2025 Q4

https://blog.cloudflare.com/ddos-threat-report-2025-q4/

KEYS

17

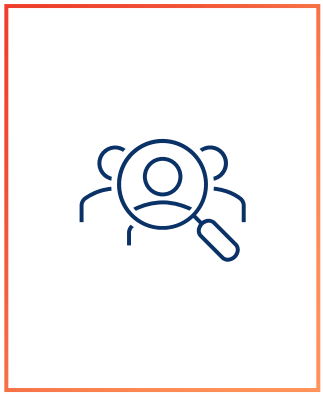
INCIDENT RESPONSE | RECOVER EXAMPLES

- Restore Clean Backups
- Remediate Vulnerabilities
- Repair Affected Files
- Reset Authentication Tokens
- Rebuild Compromised Systems
- Replace Ineffective Controls

KEYS

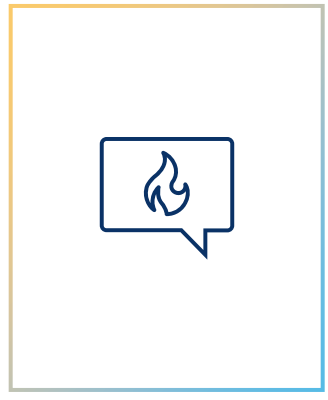
18

INCIDENT RESPONSE | OTHER KEY ELEMENTS



Roles & Responsibilities

Classification Standards



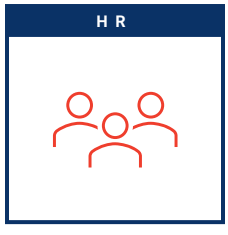
Communication Guidelines

KEYS

19

INCIDENT RESPONSE | ROLES & RESPONSIBILITIES

Incident Response Team



KEYS

20

GUESS WHO?

Lead Incident Handler

Human Resources

Senior Management

KEYS

21

INCIDENT RESPONSE | CLASSIFICATION STANDARDS

Nature

- Scope and Scale
- Active vs. Contained
- Intent / Cause
- Recurrence Pattern

Impact

- Operational
- Financial
- Legal
- Reputational

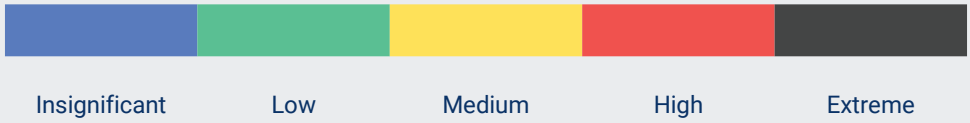
Recovery

- Timeframe
- Restoration Costs
- Complexity
- Dependencies

KEYS

22

INCIDENT RESPONSE | CLASSIFICATION STANDARDS



Your severity rating doesn't have to be perfect.

Your severity rating can change over time.

KEYS

23

HOW SEVERE IS IT ANYWAY?

- An employee reported they just accidentally clicked on a phishing link.
- The employee adds that they attempted to login to the website after clicking the link.
- IT resets the password immediately and finds no suspicious activity.
- The employee says it actually happened two weeks ago.
- Review of logs shows the account was accessed from an unfamiliar location before the reset.
- The employee was granted admin access to the payroll system last week.
- A full review of recent payroll changes is initiated and the next payroll run needs to be delayed.
- And then you woke up and realized, it was all just a dream.

KEYS

24

INCIDENT RESPONSE | COMMUNICATION GUIDELINES

- Who needs to know?
- When do you need to notify them?
- What do you need to say?

KEYS

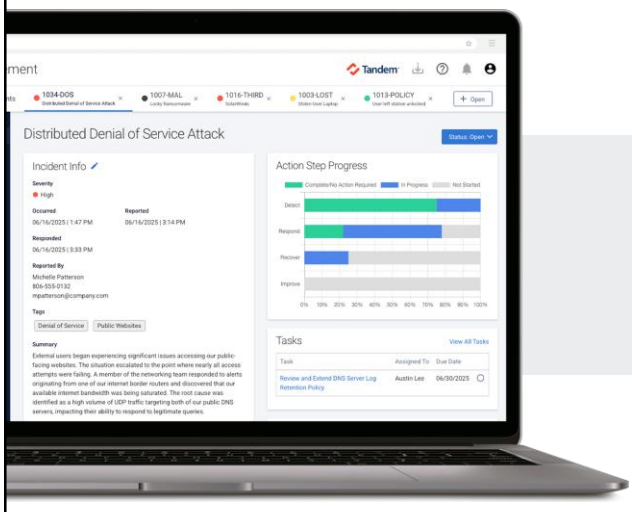
25

INCIDENT RESPONSE | COMMUNICATION GUIDELINES

1. Board Members & Management
2. Affected / All Personnel
3. Customers / Members
4. Insurance Agencies
5. Federal & State Regulators
6. Law Enforcement
7. Third-Party Service Providers
8. Payment Providers
9. Nationwide Consumer Reporting Agencies
10. Other Stakeholders

KEYS

26



KEYS

Tandem Incident Management Software

27

Incident Response Compliance Update

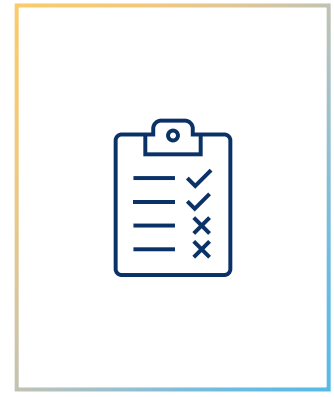
KEYS

28

INCIDENT RESPONSE COMPLIANCE

Regulations

Guidance



Frameworks

KEYS

29

INCIDENT RESPONSE REGULATIONS

KEYS

No Changes

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

OCC 12 CFR Part 30 | **FRB** 12 CFR Part 208 | **FDIC** 12 CFR Part 364

Recent Changes

Standards for Safeguarding Customer Information (06/2023) | **FTC** 16 CFR Part 314.4(h)

Cyber Risk Management (01/2025) | **FCA** 12 CFR Part 609

Procedures to Safeguard Customer Information, Including Response Programs for Unauthorized Access to Customer Information and Customer Notice (12/2025 & 06/2026) | **SEC** 17 CFR Part 248.30(3)

Pending Changes

Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (02/2026)

NCUA 12 CFR Part 748

30

NOTIFICATION REQUIREMENTS

FEDERAL

Examples:

- FDIC, FRB, OCC Computer-Security Incident Notification Requirements **(Apr. 2022)**
- NCUA Cyber Incident Notification Requirements (Sep. 2023) *
- CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (TBD 2026)

STATE

Examples:

- TX Admin Code Title 7, § 3.24 - Computer-Security Incident Notice **(Sep. 2022)**
- TX B&C Code § 521.053 – Data Breach Notice (Sep. 2023)
- NYDFS General Business Law § 899-aa – Data Breach Notice (Dec. 2024)

* *Under Review – Comments Due Feb. 2026*

KEYS

31

INCIDENT RESPONSE GUIDANCE


FFIEC IT Examination Handbook — Business Continuity Management

V.F.1 Incident Response

Incident response helps management minimize the disruption of services or loss of information from an adverse event. 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). As shown in figure 4, the incident response team should coordinate communication with the noted stakeholders. Management should align incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security), outsourced services (e.g., contracted incident response obligations), and verify that the procedures are considered during planning and BCP development.

Figure 4: Incident Response Team (Adapted From NIST SP 800-61, Rev. 2)

Management should designate a spokesperson(s) to communicate with the news media. Management should consider various, pre-planned response scenarios approved by the board and senior management. Communication with the news media and via social media may be important for disseminating accurate information. Social media monitoring during an event can help management resolve conflicting messages and proactively respond to issues and concerns.

November 2019 — 32

FFIEC Information Technology Examination Handbook (1)


America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Federal Incident Notification Guidelines

These guidelines are effective April 1, 2017. DIAs are permitted to continue reporting incidents using the previous guidance until said date. For questions, please email cyberliaison@cisa.dhs.gov.

This document provides guidance to Federal Government departments and agencies (D/As); state, local, tribal, and territorial government entities; Information Sharing and Analysis Organizations; and foreign, commercial, and private-sector organizations for submitting incident notifications to the Cybersecurity and Infrastructure Security Agency (CISA).

The Federal Information Security Modernization Act of 2014 (FISMA) defines "incident" as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." [1] FISMA requires federal Executive Branch civilian agencies to notify and consult with CISA regarding information security incidents involving their information and information systems, whether managed by a federal agency, contractor, or other source. [2] This includes incidents involving control systems, which include supervisory control and data acquisition (SCADA) systems, distributed control

CISA Incident Response & Reporting Guidance (2)


FARM CREDIT ADMINISTRATION
Examination Manual

EM-31.7

Category: Board & Management Operations
Topic: Information Technology & Security
Published: 1/17/2025

Overview

The *Information Technology & Security* topic provides guidance on evaluating the effectiveness of a Farm Credit System (System) institution's information technology (IT) and security processes to determine if sufficient internal controls are in place to support critical business functions and protect information assets. IT operations are the use of computers, networks, applications, databases, and other electronic devices to create, process, store, and use various forms of electronic data to support critical business functions. Information security is the process by which a financial institution protects the creation, collection, storage, use, transmission, and disposal of sensitive information, including the protection of hardware and infrastructure used to store and transmit such information. Cybersecurity is the process of protecting information assets and data by preventing, detecting, and responding to cyberattacks. Development and acquisition include creating, procuring, or changing software, hardware, and tools that support critical business functions. Payment systems are the mechanism, rules, institutions, people, markets, and agreements that make the exchange of payments possible. Electronic commerce (e-commerce) is the use of technology for business purposes. Adequate governance, risk management, and controls over IT operations and security is imperative.

FCA's procedures and processes for examining IT and security in System institutions incorporate the guidance published by the Federal Financial Institutions Examination Council (FFIEC) in the IT Examination Handbook InfoBase (IT Handbook). The IT Handbook is a series of booklets that cover various IT subject areas. The FFIEC maintains the IT Handbook, and it revises the individual booklets periodically to reflect changes in the IT industry and federal regulatory guidance. FCA's guidance below includes content, references, and links to the applicable FFIEC IT booklets and is applicable to all banks, associations, and service corporations. The formality and complexity of an institution's IT and security program depends on the institution's size, staffing, complexity of operations, scope of IT activities, and business risk profile. Additionally, System institutions often outsource various IT activities and services. Examiner application of this guidance should be differentiated based on these factors. Examiners can also refer to the National Institute of Standards and Technology for additional guidance and as an example of industry standards.

Examination Procedures and Guidance

General

1. Governance & Management:

Evaluate the adequacy of overall governance and management of IT operations and security activities.

FCA Examination Manual — Page 1
Information Technology & Security

FCA Information Technology & Security Exam Manual (3)

KEYS

32

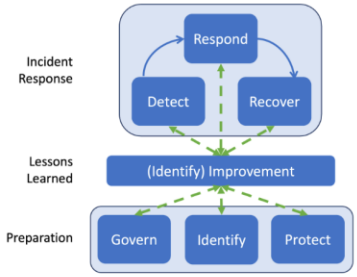
Incident Response

Overview

In April 2025, NIST finalized Special Publication (SP) 800-61 Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*.

NIST SP 800-61 Revision 3 seeks to assist organizations with incorporating cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities as described by the NIST Cybersecurity Framework (CSF) 2.0. Doing so can help organizations prepare for incident responses, reduce the number and impact of incidents that occur, and improve the efficiency and effectiveness of their incident detection, response, and recovery activities. This revision supersedes SP 800-61 Revision 2, *Computer Security Incident Handling Guide*.

The new incident response life cycle model used in this publication is shown in the figure. The bottom level reflects that the preparation activities of Govern, Identify, and Protect are not part of the incident response itself. Rather, they are much broader cybersecurity risk management activities that also support incident response. Incident response is shown in the top level of the figure: Detect, Respond, and Recover. Additionally, the need for continuous improvement is indicated as the middle level with the Improvement Category within the Identify Function and the dashed green lines. Lessons learned from performing all activities in all Functions are fed into Improvement, and those lessons are analyzed, prioritized, and used to inform all of the Functions.



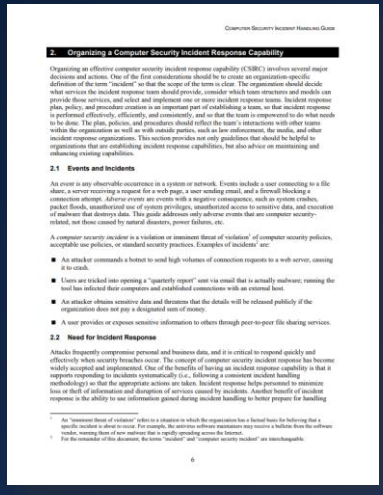
https://csrc.nist.gov/projects/incident-response

KEYS

33

REVISION 2 (BEFORE)

https://csrc.nist.gov/pubs/sp/800/61/r2/final



Computer Security Incident Handling Guide

2. Organizing a Computer Security Incident Response Capability

Organizing an effective computer security incident response capability (CSIRC) involves several major decisions and actions. One of the first considerations should be to create an organization-specific definition of the term "incident" so that the scope of the term is clear. The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done. The plan, policies, and procedures should reflect the team's interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations. This section provides not only guidelines that should be helpful to organizations that are establishing incident response capabilities, but also advice on maintaining and enhancing existing capabilities.

2.1 Events and Incidents

An *event* is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. *Adverse events* are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

A *computer security incident* is a violation or imminent threat of violation[1] of computer security policies, acceptable use policies, or standard security practices. Examples of incidents[2] are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

2.2 Need for Incident Response

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. The concept of computer security incident response has become widely accepted and implemented. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling

[1] An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet.
[2] For the remainder of this document, the terms "incident" and "computer security incident" are interchangeable.

6

REVISION 3 (AFTER)

https://csrc.nist.gov/pubs/sp/800/61/r3/final

NIST SP 800-61r3
April 2025

Incident Response Recommendations and Considerations for Cyber Risk Management

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			R2: Tune the continuous monitoring technologies to reduce false positives and false negatives to acceptable levels.
DE.CM-01	Networks and network services are monitored to find potentially adverse events	High	**R1:** Monitoring should include wired and wireless networks, network communications and flows, network services (e.g., DNS and BGP), and the presence of unauthorized or rogue networks within facilities.
DE.CM-02	The physical environment is monitored to find potentially adverse events	High	**R1:** Monitoring the physical environment should include all successful and failed access attempts into all controlled areas, the movement of people and equipment into and out of secure areas of facilities, and signs of tampering with physical access controls.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	High	**R1:** Monitoring personnel activity and technology usage should include anomalous user activity or unusual patterns of activity, authentication and logical access attempts, and the use of deception technology.
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	High	**R1:** Monitoring external service provider activities and services should include remote and on-site administration and maintenance activities that providers perform on organizational systems and deviations from expected behavior by cloud-based services, internet service providers, and other service providers.
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	High	**R1:** Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks, exfiltration, and other adverse events. **R2:** Monitor authentication attempts to identify attacks against credentials and unauthorized credential use. **R3:** Monitor software and hardware configurations for deviations from security baselines. **R4:** Monitor hardware and software, including cybersecurity protection mechanisms, for signs of tampering, failure, or compromise. **R5:** Monitor endpoints for cyber health issues (e.g., missing patches, malware infections, or unauthorized software), and redirect endpoints with issues to a remediation environment before access is authorized.

24

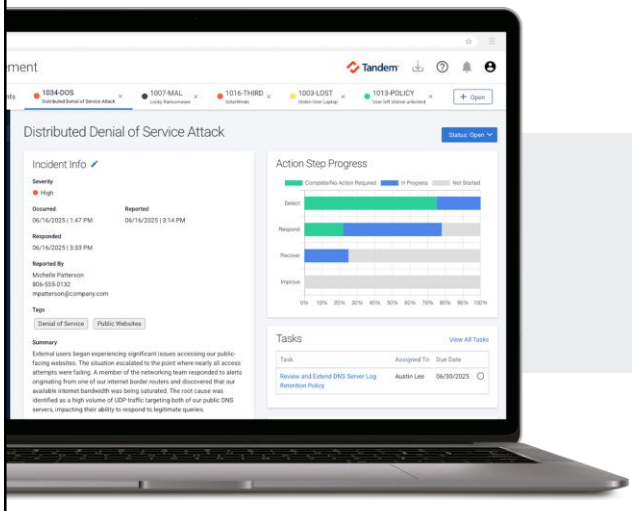
KEYS

34

REVISION 2 (BEFORE)	REVISION 3 (AFTER)
Detection	Detect
Analysis	
Containment	Respond
Eradication	
Recovery	Recover
Post-Incident Activity	Improve

35

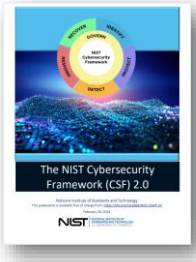
KEYS



Tandem Incident Management Software

36

FRAMEWORKS

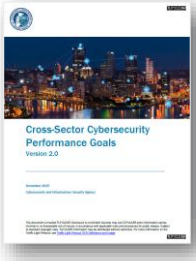


NIST CSF

- **Last Updated:** Feb. 2024
- **Functions:** Detect, Respond, Recover
- 32 Outcomes

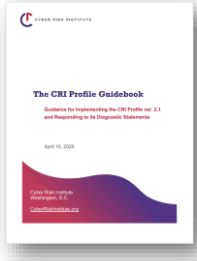
CIS CONTROLS

- **Last Updated:** Jun. 2024
- **Functions:** Detect, Respond, Recover
- Incident Response Management Control
- 34 Safeguards



CISA CPGS

- **Last Updated:** Dec. 2025
- **Functions:** Detect, Respond, Recover
- 6 Practices



CRI PROFILE

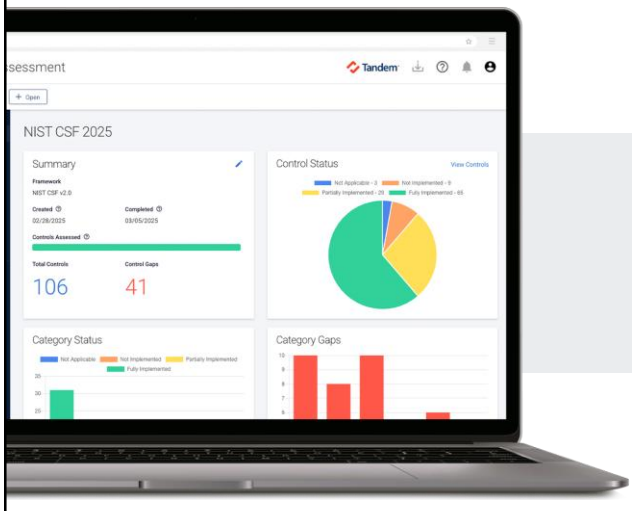
- **Last Updated:** Apr. 2025
- **Functions:** Detect, Respond, Recover
- 51 Diagnostic Statements

KEYS

https://secure.tandem.app/KnowledgeBaseArticles/Show?id=5816&categoryId=1018

37

KEYS



Tandem Cybersecurity Assessment Software

38

Incident Response Scenarios

KEYS

39

INCIDENT RESPONSE SCENARIOS

SCENARIO 1

Shadow AI Application

SCENARIO 2

Social Engineering

SCENARIO 3

Supply Chain Compromise

KEYS

40

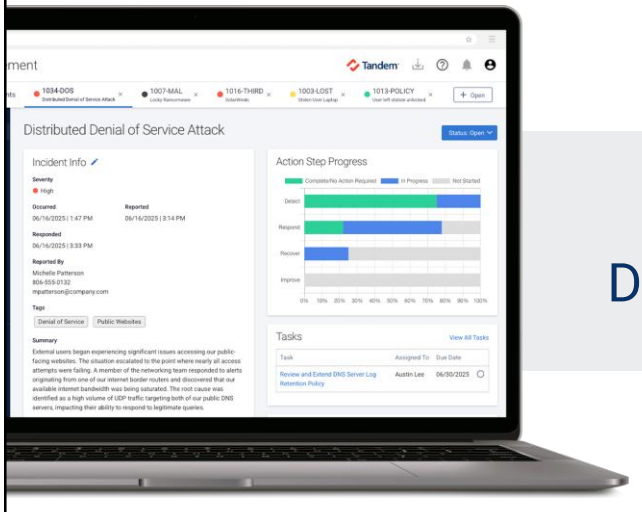
SCENARIO 1 | STORY & EXAMPLE

Shadow AI Application

KEYS

41

KEYS



Incident Tracking: Data Breach Walkthrough

42

QUICK PHONE CALL BREAK (SORRY!)

KEYS

43

IS THIS AN INCIDENT?

Yes

Maybe

No

KEYS

44

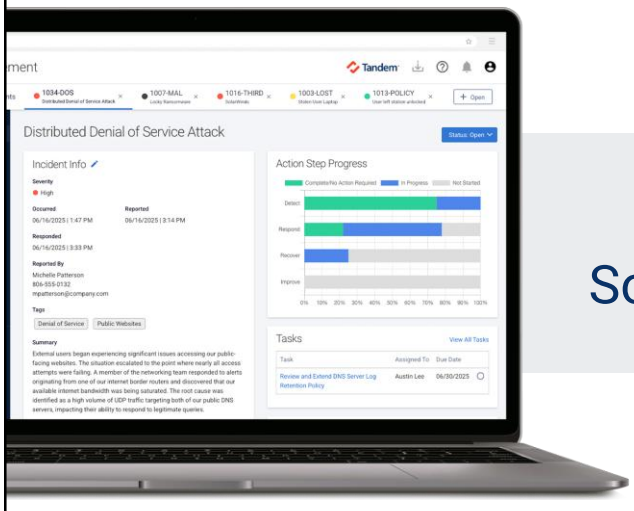
SCENARIO 2 | WALKTHROUGH

Social Engineering

KEYS

45

KEYS



Incident Tracking: Social Engineering Incident

46

Incident Management > Incidents > Open [Social Engineering – Unauthorized Account Information Disclosure]

KEYS

47

SCENARIO 3 | TABLETOP EXERCISE

Supply Chain Attack

KEYS

48

SUPPLY CHAIN ATTACK SCENARIO

The financial institution begins receiving alerts from their anti-malware system that suspicious activity was detected on the network. Investigation shows firewall rules were changed recently without approval.

Discussion Questions

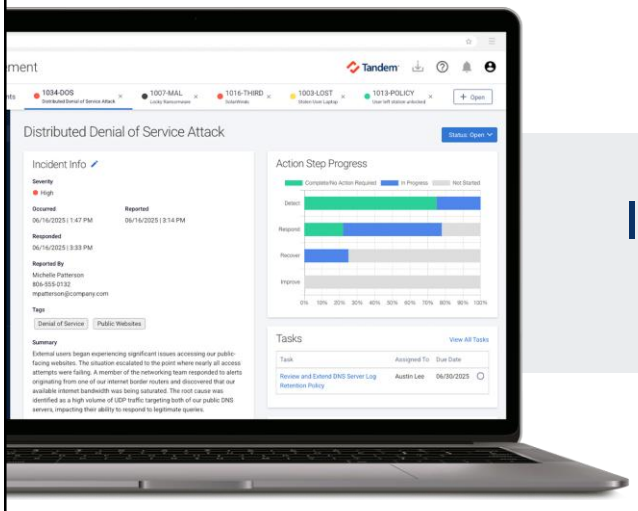
1. Would you consider this to be an incident?
2. What would your next steps be?
3. What resources would you use to investigate this?
4. How would you document this in Tandem?

Related: https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-fall-2025.pdf

KEYS

49

KEYS



Incident Response Plan: Exercises & Tests

50

SESSION RECAP

1. Incident Response Foundations
2. Incident Response Compliance Update
3. Incident Response Scenarios

KEYS

51

KEYS

52

Fill out the survey to get your sticker!

KEYS

53

Thank You!

CONNECT WITH OUR SPEAKERS AT TANDEM.APP/AGENDA

KEYS

54