

# FS-ISAC Tabletop Exercise

Prepare Your Organization for Cybersecurity Incidents  
with Real-World Scenarios

## What is an FS-ISAC Tabletop Exercise?

The FS-ISAC (Financial Services Information Sharing and Analysis Center) Tabletop Exercise simulates a cyberattack scenario that challenges your organization's cybersecurity, fraud prevention, and incident response capabilities. It provides a realistic, high-pressure environment where participants from various departments must work together to mitigate a cyberattack on critical financial systems.

## Why Your Organization Needs This Exercise



### Strengthen Team Collaboration:

Foster relationships across departments and ensure all team members understand their roles in a cybersecurity crisis.



### Identify Vulnerabilities:

Gain a deeper understanding of your systems' weaknesses and refine your security protocols.



### Improve Response Plans:

Test your incident response and recovery strategies in a controlled, low-risk environment.



### Enhance Organizational Resilience:

Boost overall preparedness for a potential real-world attack and minimize downtime and losses.

## The Benefits of Participating in an FS-ISAC Tabletop Exercise

- **Minimal Time Investment:** FS-ISAC's confidential materials allow for an efficient, low-stress exercise with minimal resource allocation.
- **Cross-Functional Learning:** Engage stakeholders from multiple departments in a cohesive cybersecurity exercise.
- **Customized Scenarios:** Tailored scenarios challenge your organization to think critically and respond to emerging cyber threats, including AI exploitation, credential theft, and spear-phishing.



# FS-ISAC Tabletop Exercise

Prepare Your Organization for Cybersecurity Incidents  
with Real-World Scenarios

## Sample Exercise Scenario

In a recent FS-ISAC exercise, a multi-pronged cyberattack scenario unfolds:

➤ **Initial Breach:**

A threat actor impersonates an employee and exploits vulnerabilities in your IT helpdesk procedures.

➤ **Data Access:**

The attacker uses a vulnerability in AI-driven systems to access critical data and documents.

➤ **Credential Harvesting:**

Customers are targeted through spear-phishing emails and have their credentials stolen.

➤ **Fraudulent Transactions:**

The attackers initiate unauthorized transactions and alter communications to delay detection.

➤ **Covering Tracks:**

The attackers erase evidence and manipulate digital communications to obscure fraudulent activities.

## Key Topics Covered During the Exercise

- **AI Exploitation in Cybercrime:** Understanding how attackers leverage AI tools for criminal purposes.
- **Phishing and Credential Harvesting:** Identifying and mitigating advanced phishing schemes.
- **SIM Swap and Social Engineering:** Defending against sophisticated attack vectors.
- **Cybersecurity Resilience:** Enhancing your response and recovery capabilities for effective disaster recovery.

## Comprehensive Program Assessment

The tabletop exercise includes:

- **Procedural Observations:** Fraud prevention, security incident response, communication protocols, regulatory compliance, and business continuity.
- **Organizational Observations:** Vendor risk management, security enhancements, post-incident actions, and lessons learned.
- **Technical Observations:** IT help desk, monitoring tools, authentication protocols, and threat intelligence.



# FS-ISAC Tabletop Exercise

Prepare Your Organization for Cybersecurity Incidents  
with Real-World Scenarios

## Key Outcomes & Deliverables

### Incident Response Plan Evaluation:

Gain a detailed report on your team's readiness to respond to a cyberattack, along with actionable feedback on how to improve.

### Comprehensive Technical Report:

Receive a full report of procedural, organizational, and technical observations, complete with recommendations and priority levels.

### Security Incident Playbooks:

Access customized playbooks for ransomware, business email compromise (BEC), and other critical attack scenarios.

## Why Choose Sourcepass for Your Tabletop Exercise?

Sourcepass brings deep expertise in cybersecurity to guide you through realistic, FS-ISAC-designed tabletop exercises. Our team customizes each scenario to reflect your specific organization's risk profile and operational environment, ensuring that your team is well-prepared to manage and recover from a cybersecurity attack.

## Ready to Strengthen Your Cybersecurity Posture?

**Contact Sourcepass today** to schedule an FS-ISAC Tabletop Exercise and ensure your organization is prepared for the evolving cyber threat landscape. Together, we'll fortify your cybersecurity defenses and enhance your incident response readiness.

