After-Action Report

2025 ICI Operational Resiliency Tabletop Exercise – Service Provider Disruption

November 2025

Table of Contents

"Our members' engagement in the Operational Resiliency Tabletop Exercise underscores what makes the asset management community so strong: a shared sense of responsibility to the investors we serve. By working through complex, fourth-party disruption scenarios together, firms not only identified potential vulnerabilities but also identified strategies, insights, and best practices that will help the entire industry respond more effectively to future challenges. ICI exists to enable that collaboration—to give members the space to prepare, learn, and lead together. The commitment and expertise on display in this exercise reaffirm our industry's resilience and our unwavering focus on protecting investors."

— Eric J. Pan, President and CEO, Investment Company Institute

Introduction

The asset management industry operates within a deeply interconnected ecosystem of service providers. While asset managers often implement governance processes to manage risk and strengthen operational resiliency, ICI members still face increasing risks due to ever more complex service provider ecosystems. Service providers themselves can expose firms to fourth-party providers—vendors that support the primary provider's operations. These fourth parties often deliver essential components but remain invisible until a disruption reveals their critical role.

This layered outsourcing model has proliferated , often due to perceived strategic advantages. Firms seek cost efficiencies, reduced internal technology burdens, and access to specialized capabilities, all made more accessible through cloud computing. While cloud computing has enabled scalable operations through expanded use of service providers with minimal internal infrastructure requirements, it has also introduced new dependencies and expanded the surface area for operational risk. A disruption at the fourth-party level, far removed from direct asset manager oversight, can cascade through the vendor chain and lead to widespread operational failures, both within and across asset management firms.

The 2025 ICI Operational Resiliency Tabletop Exercise, hosted by Charles Schwab in Denver, was designed to simulate a prolonged outage at AlphaPrime Trust Company (AlphaPrime), triggered by a failure at its fourth-party vendor CoreDataX.[1] The disruption impacted trade matching, corporate actions, settlement processing, and client reporting across multiple asset classes. By focusing on fourth-party risk, the exercise moved beyond traditional cybersecurity threats to examine the broader challenge of operational resilience in a deeply interconnected industry. Forty-two (42) firms and over 50 participants, including facilitators and observers, took part in the exercise, which was planned and led by ICI and volunteers from its Operational Resiliency Committee.[2]

The objectives of the tabletop exercise were as follows.

1. Provide a forum for collaboration and information sharing under simulated stressed conditions.
2. Raise participant awareness of operational risks stemming from vendor and fourth-party dependencies.
3. Allow firms to test and enhance their crisis management, communication, and recovery strategies in the face of a prolonged service provider disruption.

Participants were asked to assume AlphaPrime supported their own firm and that the disruption had ripple effects across the industry. Over a simulated three-day period, teams responded to evolving scenario injections that challenged their ability to maintain continuity, manage liquidity, coordinate communications, and protect client confidence.

---

1 Both AlphaPrime Trust Company and CoreDataX are fictitious firms for purposes of the simulation.

2 Members of ICI's Operational Resiliency committee from Lord, Abbett & Co LLC; Schwab Asset Management; Capital Group; Saturna Capital; Resolute Investment Managers; and Artisan Partners partnered with ICI in planning and leading the exercise.

Scenario and Methodology

The tabletop exercise followed a scenario in which a fourth-party technology failure at CoreDataX disrupted operations at AlphaPrime Trust Company, a key service provider in the asset management ecosystem. The outage impacted trade matching, corporate actions, settlement processing, and client reporting across multiple asset classes.

ICI organized exercise participants into groups of 6–8 individuals, led by facilitators. These groups reflected a mix of firm size and functional expertise. Teams responded to four scenario injections over a simulated three-day period, sharing insights and response strategies with the broader group as the exercise progressed.

Introduction

At 9:12 AM ET on a Tuesday, AlphaPrime Trust Company reported a critical outage caused by its fourth-party vendor, CoreDataX. Initially viewed as a localized issue, the disruption quickly escalated across trade matching, corporate actions, and settlement processing.

By mid-morning firms faced delayed settlements, inaccurate reporting, and rising client concerns. With no estimated time for resolution, participants activated crisis protocols and began assessing their exposure and their response options.

	Internal Events	External Events	Breakout Session
Injection 1: Day 1 (First 2 Hours)	A fourth-party failure at CoreDataX disrupts AlphaPrime's middle office systems, halting trade matching and corporate actions processing. Manual exception handling begins, and internal escalation paths are activated.	AlphaPrime issues a client notice citing a "data and reconciliation system outage." Custodians and CCPs flag delays. Clients report missing trade data and escalate concerns over NAV accuracy.	**Middle Office Response Team Focus** » Do you have a playbook for responding to a fourth-party outage? » How do you assess exposure across trade matching and settlement pipelines? » What internal coordination is required if systems are degraded but not offline?
Injection 2: Day 1 (3 to 8 Hours)	Corporate actions data feeds are corrupted or delayed. Settlement instructions and collateral movements are miscalculated. NAV and reporting processes are compromised.	Custodians and clearinghouses request revised settlement instructions. Clients escalate concerns about redemption timelines. Industry chatter intensifies.	**Back Office Response Team Focus** » What manual workflows can be activated to maintain continuity? » Can service providers support interim operations or data recovery? » How do you manage liquidity and client obligations under stress?
Injection 3: Day 1 (End of Day)	Crisis response teams coordinate across business, tech, and client service functions. Internal systems dependent on AlphaPrime data feeds are paused or degraded.	Regulators request updates on exposure and contingency plans. Clients demand direct updates. Media speculation grows.	**Communications, Legal, and Risk Team Focus** » Are messaging templates ready for vendor-driven disruptions? » What disclosures are required for regulators and clients? » How do you communicate risk exposure and mitigation steps?

	Situational Update	Breakout Session
Injection 4: Day 2 to Day 3+	AlphaPrime confirms CoreDataX remains offline with no ETA for restoration. Firms begin shifting flows to alternate providers. Liquidity management is strained.	**Strategic Response Team Focus** » What functions can be shifted to alternate providers? » How do you maintain transparency and client confidence? » What contingency plans are in place for prolonged outages?

Summary of Breakout Session Discussions

Following discussions during the tabletop exercise, each group provided ICI with notes summarizing their insights, observations, and conclusions from each scenario injection. ICI summarized the group responses, organizing information by internal versus external focus.

Identified Challenges and Impacted Capabilities

Client Communications: Firms emphasized the importance of proactive messaging and adaptable communication plans. With data feeds disrupted, clients experienced delays in trade confirmations and NAV updates. Call centers were overwhelmed, prompting the use of alternate channels such as IVR prompts, website notices, and scripted responses for advisors. Some firms considered activating dedicated lines for high-touch clients and coordinating messaging with custodians and fund administrators.

Client Obligations: Redemption timelines and liquidity needs became critical concerns. Firms discussed invoking overdraft facilities and fund credit lines, and considered delaying distributions or using in-kind transfers. Shadow NAVs and manual trade processing were revisited as fallback options. Prioritization of markets and client types (e.g., mutual funds vs. sub-advised accounts) was essential to managing risk.

Media Communications: With speculation growing, firms stressed the need to "own the narrative." Some considered engaging PR firms and preparing CEO-level messaging. Social media monitoring and press readiness were highlighted, along with the importance of consistent messaging across all external channels. Firms also discussed the timing of public disclosures and coordination with industry partners like ICI.

Regulatory Communications: Regulatory reporting grids were reviewed, and firms began preparing formal impact assessments. Coordination with the SEC and other regulators was initiated, with some firms considering requests for relief. Legal teams emphasized the importance of documenting actions and maintaining logs for future review. Firms also discussed the potential need for 8-K filings and litigation holds.

Operational Coordination: Firms activated war rooms and incident response teams, often under legal privilege. Coordination across legal, compliance, operations, and technology groups was essential. Manual workarounds were prioritized based on criticality, and staffing plans were adjusted to manage burnout and extended hours. Some firms repurposed non-critical staff and considered temporary hires.

Technology and Data Integrity: Internal systems dependent on AlphaPrime data feeds were paused or degraded. Firms assessed the viability of alternate data sources and began planning for potential vendor transitions. Golden copies of data were reviewed for integrity, and some firms considered internal tech builds to support continuity. Cybersecurity posture was elevated, and threat intelligence monitoring was initiated.

Liquidity and Risk Management: Liquidity stress emerged due to delayed settlements and collateral movements. Firms converted cash equivalents to real cash and reduced trading volumes. Risk assessments were conducted to evaluate exposure, and contingency plans were activated to sustain operations for 60–90 days. Some firms discussed the use of compliance hotlines for trade approvals and documentation.

Legal and Compliance: Contracts with AlphaPrime and related vendors were reviewed for SLAs and liability. Insurance coverage for third-party tech events was assessed. Legal teams prepared board communications and evaluated reputational risks. Firms emphasized the importance of understanding single points of failure and maintaining a compliance responsibility grid for regulatory engagement.

Lessons Learned and Key Takeaways for ICI Members

Based on small-group and all-participant discussions and related notes shared with ICI following each of the injections, the following lessons learned and key takeaways were identified.

- **Vendor Dependency Mapping and Playbooks:** Firms must maintain clear documentation of critical third- and fourth-party dependencies. Playbooks should include protocols for severing system ties, switching providers, and activating manual workarounds. Understanding vendor SLAs and escalation paths is essential to rapid decision-making.
- **Manual Workaround Viability:** Shadow NAVs, spreadsheets, and fax-based approvals were revisited as fallback options. Firms emphasized the need to routinely test manual processes and ensure staff are trained to execute them under pressure. Prioritization frameworks for manual workflows should be established in advance.
- **Liquidity and Redemption Planning:** Liquidity stress emerged as a top concern. Firms discussed activating overdraft facilities, fund credit lines, and in-kind transfers. Redemption flexibility must be understood and documented, with contingency plans tailored to different fund types and jurisdictions.
- **Crisis Coordination and Role Clarity:** Establishing a privileged war room early was critical to centralizing decisions and communications. Firms highlighted the importance of clear roles across legal, compliance, operations, and communications, including external counsel and insurance providers.
- **Communication Strategy and Cadence:** Proactive messaging, adaptable templates, and consistent internal and external communications were key themes. Firms recommended scripting for advisors, call centers, and client-facing teams, and emphasized the need for coordinated updates across channels.
- **Staffing and Burnout Mitigation:** Sustained response over multiple days required flexible staffing plans. Firms considered temporary hires, cross-training, and HR support for extended hours, including food, travel, and wellness resources.
- **Regulatory Engagement and Documentation:** Regulatory grids and impact assessments were prepared early. Firms stressed the importance of documenting actions, maintaining logs, and coordinating disclosures with boards and regulators. Some discussed the potential need for 8-K filings and formal litigation holds.
- **Resilience Beyond Cybersecurity:** The exercise reinforced that operational resilience extends beyond cyber threats. Firms must be prepared for service provider outages, data integrity issues, and prolonged disruptions. Future tabletops should continue to explore non-cyber scenarios and include key partners.

Key Takeaways for ICI

The 2025 tabletop exercise and follow-up discussions yielded several strategic takeaways for ICI.

- To optimize the effectiveness of tabletop exercises that are focused on operational outages, ICI should continue to promote industry tabletop participation by member representatives with operational backgrounds.
- Continue hosting tabletop exercises that simulate complex, multi-party disruptions—including service provider outages and fourth-party failures—to strengthen member preparedness across legal, risk, compliance, operations, and technology functions.
- Continue to explore tabletop exercises that emphasize operational resiliency and cybersecurity, as both areas reflect an evolving risk landscape.
- Facilitate cross-firm collaboration and knowledge sharing, especially for resiliency-related manual workarounds, vendor contingency planning, regulatory coordination, and liquidity management strategies.
- Support members by developing industry-aligned playbooks, communication templates, and regulatory notification grids, and by convening real-time coordination calls during actual incidents, if warranted.
- Encourage firms to map critical vendor dependencies and test their ability to shift operations or data to alternate providers under stress, including evaluating the lift required for data migration and onboarding.

ICI remains committed to supporting its members in these efforts to enhance industry-wide resilience and safeguard investor confidence.

Conclusion

The 2025 ICI Operational Resiliency Tabletop Exercise highlighted the importance of preparation, coordination, and adaptability in managing service provider disruptions. Participants valued the opportunity to test response strategies, share insights, and identify gaps in their resiliency planning. The lessons learned will help strengthen the asset management industry's ability to respond to future operational crises with confidence and clarity.

Appendix A: Checklist of Resiliency Considerations

This checklist consolidates participant insights from the 2025 tabletop exercise and is organized by functional response teams that correspond to the four injections of this year's tabletop exercise. The resiliency considerations are recommendations only. Each ICI member should individually evaluate whether and to what extend to employ practices relating to service provider disruptions and fourth-party failures. No part of the resiliency considerations should be viewed as an endorsement or disparagement of any service provider, and each ICI member should individually evaluate which service providers to use and the terms and conditions of any such engagements.

Middle Office Response Team Considerations

Planning and Preparation

1. Maintain documented playbooks for vendor-driven disruptions, including fourth-party failures.
2. Establish protocols for trade matching and corporate actions when automated systems fail.
3. Map dependencies across trade lifecycle systems and assess exposure regularly.

Manual Workflows

4. Identify manual exception handling procedures and ensure staff are trained to execute them.
5. Reference and test manual workflows regularly (e.g., spreadsheets, fax approvals).

Coordination and Communication

6. Activate internal bridge lines and privileged war rooms for rapid coordination.
7. Ensure legal and compliance are engaged early for privileged discussions.

Technology and Risk

8. Scan for indicators of compromise and assess vendor transparency.
9. Establish sandbox environments or alternate connectivity protocols for compromised vendors.

Liquidity and Trading

10. Evaluate whether to continue trading or restrict to liquidity-only trades.
11. Prepare to raise cash and assess backup workforce availability.

Back Office Operations Response Team Considerations

NAV and Settlement

1. Maintain contingency plans for NAV calculation and settlement processing.
2. Test shadow NAV workflows and alternate NAV validation methods.
3. Coordinate with custodians for backup NAV support.

Liquidity Management

4. Prepare overdraft agreements and fund credit facilities for liquidity stress scenarios.
5. Prioritize markets and client types based on exposure and sensitivity.

Manual Processing

6. Establish prioritization frameworks for manual processing across asset classes.
7. Ensure staff are trained in legacy tools (e.g., Excel-based workflows).

Compliance and Reporting

8. Document escalation paths and decision-making protocols for suspensions.
9. Review fund documentation for jurisdictional settlement requirements (e.g., T+1).

Client Service

10. Equip client service teams with talking points and escalation protocols.
11. Monitor redemption activity and prepare for increased client inquiries.

Communications, Legal, and Risk Considerations

Communications

1. Develop adaptable messaging templates for clients, regulators, and media.
2. Coordinate messaging across public relations, client service, and government relations teams.
3. Activate alternate communication platforms (e.g., website, IVR, social media).

Legal

4. Review vendor contracts for SLAs, liability, and recourse options.
5. Prepare board communications and assess regulatory disclosure obligations.
6. Maintain logs of response actions for legal review and potential litigation holds.

Risk

7. Conduct regular tabletop exercises involving legal, compliance, and operations.
8. Map single points of failure and assess concentration risks across vendors.
9. Establish compliance responsibility grids for regulatory engagement.

Insurance and Governance

10. Evaluate insurance coverage for third-party tech disruptions.
11. Determine triggers for 8-K filings and materiality assessments.

Fraud and Reputation

12. Monitor for fraud and reputational risks during extended disruptions.
13. Coordinate with valuation committees and senior leadership on public messaging.

Firmwide Strategic Response Considerations

Leadership and Coordination

1. Define roles and responsibilities across legal, risk, operations, technology, and communications.
2. Activate staffing plans for sustained response, including temp hires and cross-training.
3. Establish cadence for crisis management team reconvening and decision tracking.

Vendor Management

4. Coordinate with alternate vendors for rapid onboarding and data migration.
5. Maintain golden copies of data and validate integrity for continuity.
6. Catalog fourth-party dependencies and assess onboarding lift.

Recovery Planning

7. Develop long-term recovery strategies and minimal viable product (MVP) plans.
8. Evaluate options for shifting functions to alternate providers.

Regulatory Engagement

9. Prepare formal impact assessments and exposure reports.
10. Coordinate with ICI and regulators for relief and guidance.

Sustainability and Resilience

11. Plan for multi-day disruptions including weekend staffing and HR support , as needed.
12. Ensure transparency and consistency in internal and external communications.

Appendix B: List of Participating Organizations

AllianceBernstein	Guggenheim Partners Investment Management	Neuberger Berman
Artisan Partners	GuideStone	PIMCO
Baron Capital	Heartland Advisors	Resolute Investment Managers
Brandes Investment Partners	Investment Company Institute	Saturna Capital Corporation
Brown Advisory	Jennison Associates	Schwartz Investment Counsel
Calamos Advisors	Jensen Investment Management	TD Asset Management
Capital Group	Lord, Abbett & Co.	U.S. Bancorp Asset Management
Charles Schwab	Matthews International Capital Management	Ultimus Fund Solutions
Diamond Hill Capital Management	Meketa Capital	UMB
Dimensional Fund Advisors	MFS Investment Management	VanEck Global
Dodge & Cox	Nationwide	William Blair Investment Management
DoubleLine Capital	Natixis Advisors	Morgan Stanley
Equitable		Janus Henderson
Federated Hermes		

[i] ICI Mutual Insurance Co., SIFMA and SS&C GIDS, Inc observed the tabletop as guests. ICI continues to seek meaningful partnerships in Operational Resiliency planning with relevant entities to the benefit of our members.

About ICI

The Investment Company Institute (ICI) is the leading association representing the global asset management industry in service of individual investors. ICI members are located in North America, Europe, and Asia and manage fund assets of US$50 trillion, including mutual funds, exchange-traded funds (ETFs), UCITS, closed-end funds, unit investment trusts (UITs) and similar funds in these different jurisdictions. ICI has offices in Washington DC, Brussels, and London.