11 - 13 May 2026, Wolfsberg

23rd ISSA Symposium - Context Document

Breakout Session 2: Resilience, Recovery and Resolution

HYPOTHESIS

Resilience in Securities Services is critical for maintaining business continuity and ensuring client satisfaction, asset protection and market integrity. In its broadest sense, resiliency involves the ability to prevent disruption (resilience), rapidly recover when disruption occurs (recovery) and adapt when issues are found or recovery takes more time than is anticipated or acceptable (resolution).

The five top risks highlighted in 2026 are:

- Rising cyber threats
  Ongoing cyber threats continue to be a primary concern to resilience. Outdated legacy systems, particularly, are inherently a risk. Any issues cause regulatory scrutiny and can impact client confidence

- Increased dependence on digital and technology
  Rapid technology changes, including digital and AI adoption, are happening faster than the regulations can adapt. Embedding strong change management frameworks will therefore be key to maintaining resilience to prevent issues

- Geopolitical risk
  There are both geopolitical and geoeconomic uncertainties and these uncertainties, and their interconnectedness with Securities Services, pose significant challenges to the resiliency of operations

- Evolving regulation
  The regulatory landscape is complex, and changing, with different priorities across markets and regions. Whilst a strong regulatory framework is important, to ensure resilience it must also be able to adapt and not be too inflexible

- Third-Party risk
  Managing third-party counterparts (suppliers, clients, counterparties) - and their vulnerabilities - effectively is critical to the safety of Securities Services operations

Resiliency should therefore be embedded by Securities Services providers into their core operations to ensure that organizations can withstand any disruptions and recover quickly when something happens or - in the event that timely recovery is not possible - alternatives can be found.

Whilst each of these risks could impact the resiliency of an institution, there are two areas of particular concern. These are:

1. **Interconnectivity Risks and the Threat to Resiliency**

The risks of interconnectivity can amplify the impact of individual risks, potentially leading to larger, systemic crises. Whilst these individual risks are reviewed and resiliency frameworks have been implemented to mitigate them, additional factors need to be taken into consideration to cover the risks that could arise as result of the interconnectedness of the industry (e.g. concentration risk) and the threats these pose to resilience.

Situations where interconnectedness could be a threat to resilience include:

- The simultaneous materialization and correlation of threats of different natures (e.g. cyber security and physical security events)
- The transmission or propagation of impacts (e.g. cyber incidents) across interconnected participants within the same ecosystem
- The concentration of critical third-party counterparts (e.g. cloud providers) used by many firms may considerably amplify systemic vulnerabilities

To ensure that resiliency can be maintained, even where multiple and interconnected disruptions occur, organizations should therefore consider factors such as simultaneous disruptions or alternatively (or in addition) where there is a secondary impact and / or a cascade effect.

2. The Impact of Geopolitics on Resiliency

Recent geopolitical challenges have highlighted the fragility of current resiliency plans as well as exposed regional vulnerabilities. The implications of geopolitics can be wide-ranging as financial firms are dependent on redundancy and systems but the people element is also critical. It will be important to recognize the importance of both technology and people when considering ongoing resilience of assets and services in a region, as well as recovery and resolution plans.

OBJECTIVE OF THE BREAKOUT SESSION

The objective of the Breakout Session will be to review the overall theme of Resilience, Recovery and Resolution as well as debate the subgroup topics of:

1. Interconnectivity risks and the threat to resiliency
2. The impact of geopolitics on resiliency

The Breakout Session attendees should identify whether there are areas which impact the ISSA membership and broader Securities Services industry and assess what opportunities there are for ISSA to further develop its capabilities in this area.

PRE-READING

Breakout Session participants should read the following collateral to familiarize themselves with the hypothesis prior to the Symposium:

Emerging Risks & Global Financial Interconnectedness | DTCC

2025 Iberian Peninsula blackout - Wikipedia

The following information is on previous ISSA WG efforts and will also helpful pre-reading:

- Operational Resilience WG
  ISSA established the OR WG with the purpose of addressing the lack of a single "industry-wide" methodology for demonstrating operational resilience that catered for the Securities Services industry. There was also no means for responding in a consistent, efficient and sustainable manner to due diligence questions on the topic of operational resilience.
  The outcome was the ISSA Operational Resilience questionnaire (ISSA ORQ) which is designed to be used by the ISSA membership – and the broader Securities Services industry – both to request and to provide this information and to deal with current, and future, operational resilience requirements in a uniform way.
  ISSA-OR-Questionnaire-2024-v4.7-FINAL_protect.xlsx

- Recovery, Resolution and Resilience WG
  The WG was established in 2021 with the aim of developing a common understanding of critical functions and services among the market participants, i.e. Global Systemically Important Banks (GSIBs) and Financial Market Infrastructures (FMIs) who participated in the WG. Furthermore, the WG developed a set of stress scenarios and testing criteria in order to foster exchange of information between the FMIs and GSIBs and as such assess the impact on the industry which could potentially arise from those scenarios.
  ISSA-2021-Review-of-Critical-Functions-and-Stress-Scenarios-2022-02.pdf

QUESTIONS FOR CONSIDERATION

Below is a list of questions that the Breakout Session participants may wish to consider during their discussions:

Subgroup 1: Interconnectivity risks and the threat to resiliency

- What examples are there of interconnectivity risks for multiple events and / or industry players? Which of these areas should the Securities Services industry be focusing on?
- What steps can organizations, and the wider industry, take to prepare for a situation where multiple resiliency risk events occur simultaneously?
- How should existing frameworks be adjusted to deal with the risks associated with interconnectedness of different industry players?
- Can some of the resiliency risks identified also be enablers to enhance resiliency (e.g. advanced technology and AI-supported scenario testing can enhance preparedness, detection and recovery capabilities)?

Subgroup 2: The impact of geopolitics on resiliency

- How can Securities Services providers best adapt to ongoing geopolitical challenges?
- What needs to be put in place in the future when considering geopolitical risks to ensure a better level of resilience?
- Are there particular steps that need to be taken when considering the impact of geopolitics on employees in the workforce?
- Can some of the resiliency risks identified also be enablers to enhance resiliency (e.g. advanced technology and AI-supported scenario testing can enhance preparedness, detection and recovery capabilities)?