
sifma
protiviti
Global Business Consulting
Third-Party Resilience:
Increasing Transparency

Table of Contents

Overview

The threats faced by financial institutions are vast, multi-faceted and constantly evolving. The industry has responded in kind, in part by investing in resilience capabilities that enhance their ability to recover from destructive attacks, including attacks that may lead to data loss or critical system unavailability. The resilience of an individual organisation or service often depends on the resilience of necessary upstream and downstream partners and suppliers. Many of these third parties are common to large financial institutions, creating potential systemic risk should the third party suffer a significant operational incident. Risks can emerge from, among other things, a lack of transparency from these third parties over their resilience and recovery capabilities. This lack of transparency impedes efforts to strengthen the resilience of global financial markets.

Third parties have historically been reluctant to divulge details of their resilience capabilities. When information in shared, it is often clear that the third party has not invested in appropriate cyber resilience measures necessary to address the modern threat environment. This paper identifies and examines the operational recovery capabilities that are increasingly becoming standard expectations for third parties providing services to financial institutions. Importantly, while financial institutions are primarily concerned about the resilience of the service they receive, the overall resilience of the third party's critical systems and infrastructure is no less important. By adopting these capabilities, institutions can ensure the continuity of their critical business services consistent with their regulatory obligations and in support of the overall resilience of the financial system.

The focus on these capabilities within third parties is a continuation of the financial sector's own consideration of data and system recovery risks. For additional information on related topics, please see Principles for Data Recovery From a Severe Cyber Scenario.

Resilience Capabilities

To assess the levels of resilience required to ensure continued operations in the event of an incident, financial institutions are increasingly approaching their third parties for more detailed evidence of recovery capabilities.[1]

An example of third parties needing to provide evidence of recovery capabilities is disaster recovery and business continuity planning. These firms need to demonstrate not just failover to an alternate location, but also capabilities to recover from severe scenarios. A data centre failover does not protect services from destruction of applications or data due to malware, ransomware, insider threats or extreme operational errors. In such circumstances, replicated data and secondary sites could be simultaneously impacted. Thus, both institutions and their third parties must implement robust recovery and backup technologies and processes, such as bare metal rebuilding and deployment of immutable data backups, to ensure that critical applications and their data can be reconstructed predictably. Reconstruction will also need to be adapted to impact tolerances and/or maximum tolerable disruption (MTD) metrics established by financial institutions.

In some extreme scenarios, technical recovery capabilities alone will not be sufficient. In these scenarios, third parties should be prepared to evidence how they have considered a combination of technical recovery capabilities alongside business resilience strategies to reduce impact and extend the time they can remain within tolerance. In scenarios where it is not possible to avoid breaching tolerances, third parties should be prepared to acknowledge that fact, and work proactively with their clients on workarounds and incident response strategies.

Even with the depth of due diligence performed on third parties prior to engagement, financial institutions' knowledge of these firms' resilience capabilities may be insufficient. When information sharing does take place, it may be incomplete, with crucial details omitted or redacted. As a result, a financial institution's ability to understand the overall resilience of its third parties may be limited.

For services deemed critical, insufficient information may result in ambiguities that can compromise a financial institution's ability to assure recovery.

1. Firms may want to consider consulting the Cyber Risk Institute, an organisation that SIFMA has collaborated with in the past, for its resources including the CRI Profile which includes third parties in its suggested framework.

An example of ambiguities that can affect a financial institution's ability to ensure recovery:

Detailed Documentation	Third parties often note they perform regular system recovery testing, but do not provide additional information on the frequency of testing or the requisite evidence.
Recovery Timeframe	Third parties may note they can recover within the client's business targets, but do not provide appropriate timeframes for recovery (i.e., their recovery time objectives).

Given increased regulatory requirements and scrutiny and the industry's dependence on, and investment in, third parties, financial institutions and the clients they serve increasingly need adequate access to more consistent and comprehensive resiliency data. This includes the specific services the third party supports, as well as their own systems and services' resilience capabilities.

An important element for third parties to consider as a way to increase resiliency is to fully comprehend the deterministic and nondeterministic recovery capabilities for critical systems and underlying data.

Deterministic vs Nondeterministic Recovery[2]

Recovery from a significant operational incident, particularly one that impacts data confidentiality, integrity or availability, can vary significantly given that the recovery process typically includes both deterministic (i.e., fixed) and nondeterministic (i.e., variable and event-driven) dependencies. While some elements of recovery can be predetermined, tested and improved (e.g., restoring from bare metal/system rebuild – see diagram below), other elements are determined by the incident (e.g., the time needed to identify and remove a malicious actor from an institution's environment). Moreover, the time needed to restore data following a destructive event will always vary based on the extent of data loss and unknowable details about the environment where data is being restored.

Recovery Types

	Deterministic	Nondeterministic
Definition	Recovery time fixed and not dependent on event type and/or event severity	Recovery time variable and dependent on event type and severity
Example	System rebuild	Ensuring that systems are clear from a cyber event
Testing Needs	Effective understanding of recovery time	Relative understanding of recovery time
Recovery Time Impact	Tested recovery times essential	Tested recovery times aspirational

In a scenario that involves deterministic and nondeterministic elements, a generic recovery time mandate cannot effectively be proven as the breadth of impact can vary greatly. The appropriate emphasis on recovery therefore needs to be on capabilities that continuously mature, effectively accelerating recovery against a variety of scenarios. Arbitrary and prescriptive goals could result in a rush to premature recovery and inflict even greater market damage.

Firms can partly account for the nondeterministic elements of recovery by improving and shortening the time required for the deterministic elements. The objective is to create an ever-larger buffer between the impact tolerance/MTD and the time required for the deterministic elements of recovery. In addition, institutions can use scenario-based (i.e., tabletop simulation) testing to exercise the skills and capabilities needed for recovery. This approach enables them to validate assumptions, develop 'muscle memory' and identify areas for improvement.

Financial institutions need to understand the approaches taken by their third parties to address these scenarios. Financial institutions should receive the required data and information that assures them that their third parties are building the necessary technology recovery capabilities, and equally that the third parties are preparing for and practicing the nondeterministic elements of recovery. This can include business resilience strategies to extend the point before a tolerance is breached or to enable faster recovery to a minimum service level.

2. Also noted in Principals for Data Recovery From a Severe Cyber Scenario.

Third Parties' Resilience Capabilities

The financial services industry's resiliency standards are relatively advanced, driven by the critical importance of the sector in the economy, the sensitivity of the data held and regulatory expectations. As the criticality and concentration between third parties increases, the expectations that financial institutions have on those firms to demonstrate resilience capabilities equivalent to their clients is also increasing.

We have outlined those capabilities and expectations in the following four phases: Planning, Recovery, Testing (including data recovery) and Evidence. The phases and their elements are consistent with good practices established by financial sector institutions.

Planning

Third parties should have well-documented recovery plans that demonstrate they are in position to meet their clients' business recovery objectives. The business recovery plan should be supported by an information technology recovery plan composed of a set of strategies, procedures and protocols designed to allow for recovery of IT infrastructure systems and data after a disruptive event in line with the needs of the business. The plan's purpose is to restore critical IT services, recover data and resume normal business operations. Third parties should develop a complete picture of dependencies and potential vulnerabilities by considering their own supply chains, and in particular key service providers or contractors used in connection with services provided to financial institutions.

Recovery plans may, for example, include the following elements:

Bare Metal Restore	Ability to bring the operating systems, applications, configuration files and data back to the state they were in before failure, and within an impact tolerance that aligns to the needs of the institutions dependent on the third party's services. This typically requires the ability to recover both the infrastructure and/or operating system (known as a bare metal restore), including any applicable data to support the recovery of the business operation.
Data Recovery Point	Ability to account for client risk tolerances, as defined through service level agreements, when reconciling data to a recovery point. Third parties should consider whether their plan has a formal data backup procedure and schedule that will meet the client's recovery point objective for information needed by the client.
Data Backup	Identification of the last known good backup from which the restore can be conducted. To ensure the data backup has not been modified in the attack and is therefore able to deploy on production servers, immutable data backups should be used.
New Policies	Policies for redeployment of applications to the new environment.
Data Verification and Validations	Processes for system and application verification and validations, including the business steps to validate the data or transaction information.
Communication	Procedures to notify customers, including communications about any potential data loss as a result of the incident, are in place and tested.

Third parties should establish appropriate schedules to regularly review and update their recovery plans and conduct tests at defined intervals. This process should occur at least annually and whenever there are significant changes that could affect the stated business recovery objectives.

Client communications are another consideration. A communications plan should cover the protocols during disruption, as well as the reporting of incidents consistent with client agreements and incident reporting requirements imposed by regulators.

Recovery Testing

Third parties may test in a similar manner to their financial firm clients, but we recognise that each business is unique and therefore may test differently. The rigour, frequency and type of testing performed should align with the financial sector firm it supports. Parity of testing supersedes the importance of identical testing regimes.

Financial institutions expect that tests will 1) stress the organisation to provide meaningful, actionable feedback, 2) provide a benchmark against the third party's impact tolerance or Service Level Agreements (SLAs) (whichever requires a shorter recovery time) and 3) incorporate extreme but plausible scenarios.

Examples include traditional disaster recovery testing, which involves testing locations; sustained resiliency where operations are failed over to secondary locations where they continue processing business loads for an extended period (typically at least five business days); and cyber recovery, where primary and secondary processing capabilities have been compromised, necessitating a bare metal rebuild and data restoration. Third parties should also be familiar with and test SIFMA's Reconnection Framework – Guidelines for Remediating Cyber Events Impacting the Financial Ecosystem.

A third party's testing program should consider the following:

Test Outcomes	Testing is not a pass or fail effort, but a manner through which to verify resilience capabilities and determine how to reduce recovery time. Financial institutions seek mostly to understand how a firm will strive to enhance their own recoverability based on the outcomes of a test.
Number of Tests	There is no set number of tests a third party should undertake. The number should be a product of the firm's importance to the industry and the outcomes of previous testing. However, where outages exceed defined tolerance, additional testing should be undertaken to evidence that the deficiency has been addressed.
Joint Testing	The financial sector welcomes testing capabilities jointly to increase the ability for personnel to learn from each other and to collaborate more effectively in a recovery scenario. However, joint testing should be left to those institutions and third parties that represent the most critical components of the financial sector ecosystem. SIFMA's annual industry-wide business continuity test is an example of these types of tests.
End-to-End Testing	While in theory such testing is ideal, in practice it is not possible. Instead, a combination of different testing types such as technology recovery, simulation, and business strategies, among others, lead to an end-to-end examination of risk. No single test can be comprehensively end-to-end. Utilisation of testing outcomes to serve as a proxy for end-to-end tests is also an acceptable method to manage and expedite testing.
Rebuild Testing	• Third parties should undertake rebuild testing, which should include bare metal recovery and data restoration of infrastructure/OS/configuration files. This may be demonstrated through a mock rebuild in a non-production environment or through advanced capabilities that demonstrate an ability to rebuild on demand. • Rebuild testing should include restoration of data and considerations for data loss during the interval from the last immutable backup and the point of failure; while permutations are many, an approach to reconstruction within data loss tolerance should be documented and, to the extent practical, tested. • Validation of the application's recovery to a level that can meet the needs of the business services it supports (i.e. its impact tolerance/MTD is also required). Use of proxy testing or extrapolation from partial to full scale are accepted practices to evidence this capability, given sufficient documentation of processes.

Data Recovery Testing

Data recovery testing may not cover end-to-end transaction processing or system performance. Tests may not be continuous in nature and may be carried out in distinct phases (i.e., infrastructure/OS recovery, configuration files, core data restoration and applications). Regular testing of recovery plans should occur at a minimum on an annual basis and cover the rebuild of the infrastructure/OS, the restoration of data from an immutable backup, and the redeployment of the application.

Tests should meet the following minimum expectations:

Data Restoration	Immutable data is stored and encrypted at rest.
Backups	• Backup procedures and oversight should ensure that routine backup operations are frequent enough to ensure usability commensurate with business needs. Business data backups (file system and database) should be carried out to ensure they meet expected business data loss tolerance levels. A minimum immutable backup frequency should align with the business resilience requirements of the institution supported by the third party's service. • Backup retention should be enforced. A period of 35 days is advised to ensure coverage over the full length of a month, including possible weekends and holidays. • Third parties should confirm offline backup files reside on storage media that is logically or physically segregated (i.e., air gapped) from both the primary and other failover environment(s). Access to these backups should be restricted and only possible with unique credentials. • Immutability of backup and appropriate access controls must be demonstrated to ensure viability of backup from tampering or deletion. Third parties should validate that the credentials used to create offline backups (i.e., to include applications and databases) are separate and distinct from the credentials used to replicate production data and offline backups. • Immutability may be demonstrated through configuration or use of Write-Once-Read-Many (WORM) storage. Common methods to achieve online and/or offline backup immutability include software only, software + media, media only, or hardware based. • Backups should be tested (e.g., database restore tests) at least annually to ensure the functionality of backup appliances and commensurate processes that specify and recover targeted data.

Evidence

Third parties should be prepared to demonstrate that adequate levels of planning and testing have been conducted, and that the overall recovery times align with the business recovery objectives of the financial institution.

The following outlines the types of evidence that financial institutions may expect to receive:

Documented Recovery Plans	Detailed documentation of recovery plans that outline the strategies and procedures for restoring operations in the event of disruption.
Test Results and Reports	Detailed records of testing activities should be provided, demonstrating adherence to the documented recovery plan. These records should include evidence that recovery operations were successfully executed using immutable backups, particularly in the event of a destructive cyber incident. In the case of a sustained resiliency test, the documentation should confirm that production workloads were maintained at the alternate site for an extended period (typically a minimum of five business days). The records should outline the scope, methodology and outcomes of each test, thereby verifying the effectiveness and reliability of the recovery plans.
Disclosure of Concerns	Communication of discrepancies between current capabilities and the required recovery objectives, along with plans to address these gaps.
Continuous Improvement Processes	Information on formal governance to manage resilience capabilities, including on mechanisms for regularly updating and enhancing recovery plans based on test results, real incidents, and evolving threats.

By providing this evidence, third parties can demonstrate their commitment to meeting critical business resiliency objectives and ensuring robust recovery capabilities.

These firms should also evaluate methods for presenting this evidence to their financial institution customers.

The following options may be considered:

Full Disclosure	Reasonable access to all relevant evidence, allowing the financial institution to thoroughly review details of testing activities and outcomes.
Risk-Based Redaction	Redact certain sensitive information. This approach balances transparency with the need to protect proprietary or sensitive data.
On-Site Review in Isolation	Allow financial institutions to review evidence in a controlled and secure environment, typically on-site. This method ensures confidentiality while enabling the institution to verify evidence firsthand.

Conclusion

The financial sector's interconnectedness to and reliance on critical third parties continues to create significant dependencies as risks evolve. As part of their risk mitigation efforts, financial institutions will need third parties to demonstrate advanced resiliency capabilities. The standards identified in this paper represent what these firms should consider meeting to serve financial institutions effectively. By increasing transparency, the broader financial services ecosystem can decrease the resiliency knowledge gaps between key partners. These efforts will not only enhance the resilience of the sector and decrease risks to financial institutions, but will also contribute to maintaining broader financial stability in an increasingly interconnected world.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit sifma.org.

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through our network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, visit protiviti.com.

Contacts

Thomas Wagner
Managing Director
Financial Services Operations
SIFMA
+1.212.313.1161
twagner@sifma.org

Steve Byron
Managing Director
Technology, Operations and Business Continuity
SIFMA
+1.212.313.1260
sbyron@sifma.org

Douglas Wilbert
Managing Director
Protiviti
+1.917.697.1572
douglas.wilbert@protiviti.com

Brian Kostek
Managing Director
Protiviti
+1.813.348.3375
brian.kostek@protiviti.com