Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Business Services Resilience and Restoration

Building Operationally Resilient Business Services in the Financial Sector

April 8, 2019

Overview

As the financial lives, interests, and concerns of customers have grown, so have the array of services offered by the financial services sector. These services increasingly rely on complex systems and a hyper-connected group of financial services companies. In addition to the expectation of security across all customers, retail and commercial banking customers rightfully expect these services to be consistent and accessible 24/7 with no disruption.

These expectations, paired with the current threat landscape, have resulted in once improbable scenarios now being considered extreme but plausible. As a result, the financial sector, government partners and regulatory bodies are focused on expanding existing **business continuity and disaster recovery** (BC/DR) planning assumptions and building **operationally resilient business services** and provisions for **business restoration** if recovery is not possible during an extreme event**.** This helps ensure that critical business services are always accessible and functional, and limits – if not, eliminates – the disruption to the financial services sector in the event one or more financial services firms are negatively impacted. Such proactive tactics instill consumer confidence in their financial firm(s) and the financial services sector.

Being operationally resilient is supported by – and extends beyond – having a strong BC/DR program and leveraging systems that are resilient through design. It is also supported by a comprehensive approach that addresses how business operational resilience is achieved should contingency plans fall short during an extreme event.

This white paper defines key terms used in discussions related to operational resilience, business continuity/disaster recovery, and business restoration. Additionally, it outlines an initial proposed approach to aligning and bridging these topics as well as developing a framework for operationally resilient business services, which firms can use to enhance or establish resiliency programs, build upon BC/DR capabilities, and support overall sector resilience through planning for business restoration.

I. Operational Resilience

As a result of an effective resilience program, firms should consider their ability to[1]:

- **Prevent significant incidents** from occurring
- **Continue to provide** critical business services, within defined impact tolerances in the event of an incident
- **Recover to normal** operations promptly
- **Learn from scenario-testing and incidents** in order to limit the impact of future, similar incidents

Operational resilience focuses on a firm's ability to absorb the shock of an event in order to minimize the impact to the firm, its customers and clients, and to the broader financial sector. This compliments and goes beyond PPD-21, which defines resilience as ""ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions."

Prevent Significant Incidents

In this context, significant incidents are those that directly impact the ability of a firm to deliver critical business services to its customers/clients.

Companies, government partners, and regulators have historically invested in people, process, and technology with a focus on prevention and mitigation. However, the industry recognizes preventive controls alone are not sufficient for maximum preparation and protection against today's risks. Planning should include assessments that identify the impact tolerance for the firm and for the customers.

[1] Based on the Bank of England June 2018 Financial Stability Report

Continue to Provide

Consumers and firms have come to expect a certain level of service from their financial firms to transact for goods and services, and this increasing dependency of global business on financial firms is driving a foundational requirement for business services to continue to meet these expectations.

See the section on Resilience of Business Services for additional information on this.

Recover to Normal

Disaster recovery focuses on returning systems to a normal operational state in the event of a failure or disruption.

In an extreme event, a firm may be unable to continue to deliver its complete business services by invoking standard contingency measures and disaster recovery plans, resulting in the need for a more significant recovery or reconstruction effort.

In extreme cases, restoring business services may require a complete rebuild of technology systems, including infrastructure and data stores. Prior identification and mapping of essential functions is key to determining the approach and priority for each system rebuild. In these rebuilds, the efforts include reestablishing technology systems, connecting those systems to business services, and reestablishing effective controls (e.g. access management and authentication) based on sequencing for both required functions and priority services.

Depending on the type of event and the effects on the technology systems, business services may require more than a direct recovery of the existing systems and technologies. It may also include the need for restoration if the

previous systems cannot be returned to their prior state within defined impact tolerances. See Restoration of Business Services below.

Learn From Scenario Testing and Incidents

Firms have identified multiple opportunities to learn from incidents and exercises to enhance existing processes and technologies. These may include firm only, sector-wide, or cross-sector exercises, as well as evaluation of incidents at their own firm, peer financial firms, or organizations in other sectors. Evaluating identified areas for improvement from an exercise or lessons learned from an incident allows firms to make an informed decision on what processes, procedures, and controls need to be updated or implemented in its environment. These action items and lessons learned may include the identification of the time taken to rebuild systems or make key decisions, so as to allow for alternative contingency plans. In the U.S., sector-wide and cross-sector exercises take place through several organizations, including the Financial Services Sector Coordinating Council ("FSSCC"), the U.S. Department of the Treasury, and the Financial Services Information Sharing and Analysis Center[2] ("FS-ISAC"). In addition, international activities take place, for example, through U.K. Finance and stakeholder organizations.

The financial services sector hosts many sector-wide exercises each year, which help to identify potential operational resilience issues. The sector participates in a variety of exercises, including:

- Hamilton Series, hosted by the U.S. Treasury as a joint collaboration with the FSSCC, operationally supported by the FS-ISAC, involves the private sector and various federal agencies to better prepare the financial sector in addressing the risks and challenges presented by a significant cyber security incident. Over 20 exercises have taken place in this series since 2014.

[2] https://www.fsisac.com/

- Cyber-Attack Against Payment Systems (CAPS) tabletop exercise in which over 2,000 financial institutions globally participate and the Cyber-Attack Against Insurance Systems (CAIS) exercise designed for North American insurance companies. These FS-ISAC organized exercises present a cyber attack scenario to challenge incident response teams and test incident response preparedness.

- Securities Industry and Financial Markets Association[3] ("SIFMA") and Futures Industry Association ("FIA") Annual Disaster Recovery Exercise, which focuses on the industry's ability to operate through a significant emergency using backup sites, recovery facilities and backup communications capabilities.

- Quantum Dawn, hosted annually by SIFMA, tests the crisis response planning between critical firms and key government agencies.

II. Resiliency of Business Services

In the realm of evermore complex business and technology integration, it is not a matter of "if" but "when" a disruption will be caused by anything from a natural disaster to an organized malicious threat actor. It is both good business practice and, in many cases, a regulatory requirement for firms to plan for plausible disruptions and evaluate systems and processes for sustaining business services during and after a disruption. A thorough Business Continuity plan will also consider scenarios that may have historically been considered implausible but are now quite possible due to various dynamic factors, such as increasing technical complexity and/or targeted malicious attacks.

Disaster Recovery is a subset of BC efforts and assumes "normal" functionality can be reestablished within a defined timeframe once disruption happens. DR focuses on reestablishing underlying capabilities, including data and data systems, physical assets, and personnel to return the business services to normal operations. Such plans anticipate failure points and can rely on a variety of system designs, including high

[3] https://www.sifma.org/

availability, hot/hot architectures or continuously available systems to minimize business disruption resulting from a system-impacting event.

Business continuity planning is a required investment for companies to avoid financial, regulatory, and reputational damage. Also, strong BC/DR plans enable the financial firm to deliver business services during an event outside the norm, instilling confidence in customers and partners in the reliability and resiliency of business services and the sector as a whole.

Financial firms continue to develop and mature BC/DR practices. These practices should continue to mature in order to develop operationally resilient business services, in light of the current risk landscape. Impact tolerance can aid firms in providing clear metrics indicating when an operational disruption would represent a threat to the viability of the firm, its customers and clients, and the sector. Ultimately, it is the business services that must be resilient through comprehensive design and implementation across of the various components that work together.

Virtually every business service provided by a financial services firm depends on technology to the extent that many of these services cannot be performed, even for a short period, by humans alone. This ubiquitous dependency requires that technology solutions be designed, or retrofitted, with fault-tolerance and rapid recoverability as a core requirement.

Systems also should be designed and deployed for serviceability, meaning that changes can be implemented as quickly and safely as possible, with minimal impact to critical technology services. One example of this is the logical or physical separation of critical capabilities designed to limit the impact and duration of incidents.

As an example, operationally resilient business services might feature the following qualities:

- Prioritizing the most important business services or essential functions that, if not provided in the normal course of business, might:

  - Undermine financial stability
  - Threaten the firm's ongoing viability
  - Cause harm to customers and clients

- Mapping the systems and processes that support these business services, including third party service providers and critical dependencies
- Knowledge of how the failure of an individual system or process could impact the provision of the business service and if those systems or processes could be substituted during a disruption
- Validated and tested plans to help minimize impact caused by adverse events
- Internal communication plans, escalation paths, and identified decision-makers
- External communication plans, which might consider customers, other market participants, and regulatory and other government partners

III. Restoration of Business Services

BC/DR plans identify how to deal with any potential impacting event but tend to be focused on underlying technology systems and data stores, rather than end-to-end business services. Expanding operational resilience focuses on the outcome of continuing to operate business services, within established tolerances, even during system-impacting events. Restoration then focuses on how to maintain or re-establish business services in event of an extreme event that cannot be resolved through established BC/DR plans. (See Figure 1 – Architecture of Resilience)

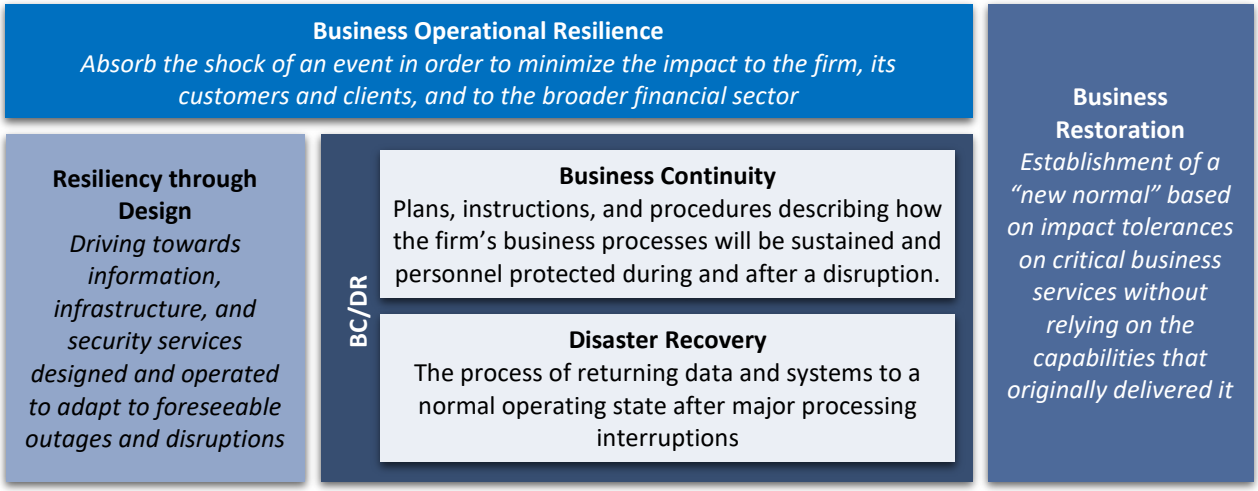

Figure 1 – Architecture of Resiliency

Expanding operational resilience to include establishment of a "new normal" for restoration of business services without relying on the capabilities that originally delivered is necessary in today's business recovery planning. In addition to planning to reestablish previously normal operations, such restoration planning might consider alternative ways to deliver critical business services via different methods on a long-term, or even permanent, basis. This may include restoration to alternative technology solutions (e.g., bare metal environments) when recovery of current systems is not possible or practical. (See Figure 2 – Resiliency vs. Restoration of Business Services)

	Business Service Resilience		Business Service Restoration
Assumes	A business service will be disrupted	Business service can be reestablished within tolerance range	Service recoverable to full working order
Delivers	Continuous business service	Minimized impact from disruptions	Rebuilding of business service

Figure 2 – Resiliency vs. Restoration of Business Services

IV. Financial Sector Efforts Underway

While "operational resilience" is a recent focus area, it is not a new concept. The financial sector is beginning to refine its thinking and evolve its approach to operational resilience. The financial services sector has been practicing the core tenets of resiliency for many years and has more recently begun to undertake efforts to look at new systemic risks and find alternative ways to mitigate or respond.

FS-ISAC

Formed in 1999 in response to a U.S. Presidential Policy Directive 63 FS-ISAC's mission is to improve the security and resilience of the global financial services sector, including the public's financial life through collaboration across the public and private sectors. FS-ISAC empowers voluntary sharing, intelligence, crisis response, exercises, and best practices with the focused subsidiaries described below (FSARC and Sheltered Harbor) that conduct deeper analysis, other forms of collaboration, and develop standards. FS-ISAC also maintains the financial services sector's Financial Sector Crisis Response Framework (previously called the All Hazards Playbook), which outlines the processes and considerations for identifying and responding to significant threats or events. Taken together, FS-ISAC provides situational awareness and raises awareness of the changing threat environment across all hazards including cyber, physical, and geo-political to its membership of over 7,000 financial firms.

FSARC

The Financial Systemic Analysis and Resilience Center[4] ("FSARC") was established in 2016 as a membership-funded nonprofit entity whose mission is to increase the resiliency of critical systems that underpin the U.S. financial services sector. FSARC facilitates operational collaboration between participating financial institutions and market utilities, the U.S. Government, and other key sector partners in a controlled

[4] https://www.fsisac.com/article/fs-isac-announces-formation-financial-systemic-analysis-resilience-center-fsarc

environment where participants can securely collaborate. Together, they conduct analysis of critical financial sector systems and jointly monitor and warn against threats to those systems. The membership of FSARC is limited to the entities within the financial sector identified as "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

Key FSARC functions:

- Risk: Proactively identify and map systemic risks to critical infrastructure and coordinate sector resiliency planning to mitigate these risks.
- Intelligence: Provide an advanced warning capability for cyber related threats to systemically relevant critical infrastructure.

The goal of these initiatives is to ensure that an incident impacting a significant market participant does not have a broader systemic impact. The FSARC initiatives, and its outputs, for individual firms and the broader sector support the concept of operational resilience and will continue to do so as the risk initiatives are further undertaken and refined.

Sheltered Harbor

In 2015, several firms collectively established Sheltered Harbor[5] as an outcome of a sector-wide exercise with The U.S. Department of the Treasury focused on protecting critical account information of market participants in the event of a destructive cyber attack or major disaster. Sheltered Harbor was launched to promote the stability of the U.S. financial markets by protecting critical account information of participants in order to facilitate the recovery of such information following an incident. Sheltered Harbor coordinates the development of the data protection and portability standard, promotes

[5] https://shelteredharbor.org/

its adoption across the industry, supports participants in their implementation efforts, and ensures adherence through certification.

Sheltered Harbor members store data according to a common framework in immutable, air-gapped data vaults. Sheltered Harbor members can access specifications for common data formats, secure storage ("data vaults"), and operating processes to archive and restore data. Should a financial institution be unable to recover from a cyber attack in a timely fashion, firms that adhere to the Sheltered Harbor standard will provide customers access to their accounts and balances from a pre-designated alternate processing platform.

Off-Network Tools

Firms have undertaken individual efforts to increase their resiliency through the development of off-premise platforms that enable specific groups of employees to communicate and work during an incident impacting enterprise communications. These externally hosted platforms are designed to enable communication, collaboration, and coordinated responses during a widespread network unavailability incident.

Government and sector communication and incident response mechanisms may supplement firm-specific tools. These tools allow for priority communications via SMS messaging, conference calls, and direct phone calls.

Identification of Sector Critical Services

FSSCC encourages efforts to work collaboratively across firms to develop solutions that protect the ecosystem of sector critical functions and the critical business services that they support. The identification of these functions and services are based on the ability to pay for goods, services, and financial assets; intermediating between savers and borrowers; and insuring against and dispersing risk.

FSSCC has orchestrated conversations to identify and understand the overarching critical business functions and services (e.g. services and products) the financial sector

provides. Upon identifying those that are critical, the sector is able to focus on the underlying systems and processes and identify dependencies (e.g. people, data, systems, and assets).

Financial Services Sector Cybersecurity Profile

Through the FSSCC, members developed a Financial Services Sector Cybersecurity Profile[6] ("Profile") – a cyber security assessment tool that extends the NIST Cybersecurity Framework to include cyber security regulatory expectations specific to the financial sector. This includes key aspects of operational resilience, such as business continuity and disaster recovery governance, evaluation of internal and external dependencies, and planning for significant events. The Profile created a set of assessment questions for financial firms and government partners to use to understand cyber security and those key aspects of operational resilience at financial firms.

V. Sector Next Steps

There is a shared responsibility for business services resiliency. Inter-connectedness of financial firms requires planning for business operational resilience and benefits from sector-wide coordination. A single event could potentially impact the entire value chain of a transaction and might affect firms. Therefore, it is incumbent upon financial firms to design, build, and deliver resilient business services supported through prevention, response, recovery, and learning from business operational disruptions, while also being prepared to execute business restoration in cases of extreme impact.

[6] https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile

Working with government and sector partners, the FSSCC and its members plan to continue to focus on business services resiliency through:

- Creating a framework or enhancing an existing framework to expand concepts from BC/DR to capture a wide range of plausible events, including those that may have originally been considered implausible, and defining impact tolerances.
- Engaging business lines in the discussion of resilience and impact tolerance to encourage investment and sustainability.
- Establishing a framework for assessing essential functions for restoration and identification of minimum requirements to deliver critical business services.
- Prioritizing sector-wide critical services, as well as cross-sector dependencies, to determine the needs and approach for mutual assurance and potentially sector-wide metrics for specific business services.
- Supporting government partners in establishing standards that could be benefited by similar critical infrastructure sectors like telecommunications, healthcare, energy, utilities, and transportation.

Efforts to address business service resilience and restoration will benefit from full sector engagement. Many of these efforts will be led by SIFMA, which is partnering with global affiliate organizations the Association for Financial Markets in Europe, the Asia Securities Industry & Financial Markets Association (“ASIFMA”), and the Global Financial Markets Association (“GFMA”). This effort will build upon past sector efforts, including the SIFMA Quantum Dawn exercises and the Hamilton Exercises led by the U.S. Department of the Treasury.

Key Definitions

Bare Metal restoration is a process whereby new technology environments ("new normal") need to be created. This would typically take place when the infrastructure and operating data required to deliver business services have been destroyed or rendered unusable.

Business Continuity Plan[7] is the instructions and procedures that describe how a firm's business processes will sustain during and after a significant disruption.

Business Restoration is the process of reestablishing business operational services through to normal operating capabilities ("new normal") in the event previous capabilities cannot be recovered.

Continuity is the ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an incident that disrupts normal operations.

Disaster Recovery is the process of recovering from major processing interruptions. Disaster Recovery includes:

- Restoring an information system to full operation after an interruption in service, including equipment repair or replacement, file recovery or restoration, and resumption of service to users.
- Restoring an application and infrastructure to operation in order to support a business function in the designated disaster recovery site after an interruption in service.

Impact Tolerances quantify the amount of disruption that could be tolerated in the event of an incident prior to having a detrimental effect on a firm, its clients or the sector.

[7] Based on NIST definition available at https://csrc.nist.gov/glossary/term/business-continuity-plan.

Operational Resilience is the implementation of techniques to absorb the shock of an event in order to minimize the impact to the firm, its customers, and the sector during an incident.

Resiliency through Design is the information, infrastructure, and security services designed and operated to adapt to outages and disruptions.

About FSSCC

Formed in 2002 as a public/private partnership with the support of the U.S. Department of the Treasury, FSSCC collaborates with the Treasury and the financial regulatory agencies at the federal and state levels through the Financial and Banking Information Infrastructure Committee, which also formed in 2002 under the Treasury's leadership. FSSCC members include 72 of the largest financial firms and their industry associations representing banking, insurance, credit card networks, credit unions, exchanges, and financial utilities in payments, clearing, and settlement.

For additional information, visit https://www.fsscc.org.