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

Business Services Resilience and Restoration

Financial Services Sector Preparation for an Extreme Event

Draft as of March 13, 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. Customers rightfully expect these services to be secure, consistent, and accessible 24/7 with no disruption.

These growing 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 focusing beyond traditional **business continuity and disaster recovery** (BC/DR) to also include **operationally resilient business services.** This seeks to ensure that critical customer-facing business services are always accessible and functional, and limit – if not, eliminate – the disruption to the financial services sector in the event one or more financial services firms are incapacitated. Such proactive tactics instill consumer confidence in their financial firm(s) and the sector as a whole.

Being operationally resilient is supported by – and extends well 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 even when BC/DR plans fail or are rendered ineffective, such as might be the case in 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 resilience through a business restoration approach.

DRAFT

I. Operational Resilience

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

- **Prevent significant incidents** from occurring
- **Continue to provide** business services and functions to the firm's customers/clients and the financial sector in the event of an incident
- **Recover to normal** operations promptly when the incident is over
- **Learn from incidents** in order to limit the chances of them happening again in future

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.

Prevent Significant Incidents

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

Companies, government partners, and regulators have historically invested in people, process, and technology with a focus on prevention. However, the industry recognizes preventive controls alone are not sufficient for maximum preparation and protection against today's risks.

Continue to Provide

Consumers and firms expect their financial firms to transact for goods and services around the clock, and this increasing dependency of global business on financial firms is driving a foundational requirement for business services to always be available.

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

DRAFT

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

Recover to Normal

Disaster recovery focuses on returning physical systems in 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 business services by invoking standard contingency measures and disaster recovery plans, resulting in the need for a more significant recovery or reconstruction effort.

Restoring business services may require a complete rebuild of technology systems, including infrastructure and data stores. The identification and mapping of the most important activities would be essential in determining the approach and priority for each system rebuild. In these rebuilds, the efforts include more than reestablishing technology systems, but also the connecting of 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, the 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 Incidents

Firms have identified multiple opportunities to learn and 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. The key is identifying the

lessons learned from any exercise or incident and implementing appropriate controls. These 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") 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.

Sector-wide exercises are important for the sector overall as they help to identify potential operational resilience issues. The sector participates in a variety of exercises, including:

- Securities Industry and Financial Markets Association[3] ("SIFMA") Annual Test on the industry's ability to operate through a significant emergency using backup sites, recovery facilities and backup communications capabilities.
- Annual Quantum Dawn, hosted by SIFMA, tests the crisis response planning between critical firms and key government agencies.
- Hamilton Series, hosted by the U.S. Treasury, 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.

II. Resiliency of Business Services

In the realm of ever-more-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 a critical duty for financial firms to plan for plausible disruptions and evaluate systems and processes for sustaining the business

[2] https://www.fsisac.com/
[3] https://www.sifma.org/

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 re-established within a defined timeframe once disruption happens. DR focuses on re-establishing underlying technical capabilities, physical assets, and personnel to return the business services to normal operations. Such plans anticipate failure points and often rely on high availability designs to minimize business impact during a time of failure or other impact.

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 developed and matured strong BC/DR practices and generally have prevented or minimized wide-spread service interruptions. These practices must continue to mature in order to develop operationally resilient business services. To obtain this resilience requires establishing impact tolerances to provide 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 company 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 must also be designed and deployed for serviceability, meaning that changes can be implemented quickly and safely without fear of causing wide-spread, self-inflicted impacts to critical technology services. This would include logical or physical separation of critical capabilities designed to limit the impact and duration of incidents.

Operationally resilient business services require:

- Prioritizing the most important business services that, if not provided in the normal course of business, could:
    - 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 how those systems or processes could be substituted during a disruption
- Tested plans that ensure the shock of an event can be absorbed to minimize impact
- Internal communication plans, escalation paths, and identified decision-makers
- External communication plans for customers, other market participants and supervisory authorities, 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 rather than business services. 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 a catastrophic impact that cannot be resolved through established BC/DR plans. (See Figure 1 – Architecture of Resilience)

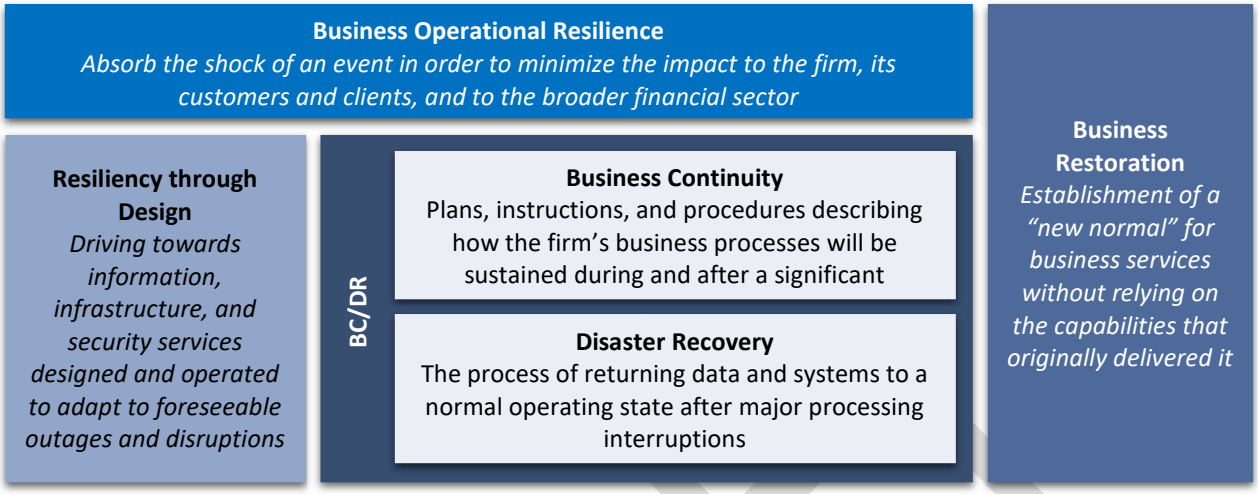

Figure 1 – Architecture of Resiliency

Restoration is the establishment of a "new normal" for business services without relying on the capabilities that originally delivered it. Instead of planning to re-establish previously normal operations, such restoration planning would consider alternative ways to deliver critical business services through different methods on a long-term, or even permanent, basis. This may include restoration to bare metal environments when recovery of current systems is not possible or practical.A business restoration plan or framework is invoked when expected business service resilience cannot be maintained within previously established tolerances. (See Figure 2 – Resiliency vs. Restoration of Business Services)

	Business Service Resilience		Business Service Restoration
Assumes	A business service norm will be disrupted	Business service norm can be re-established within tolerance range	Service unrecoverable with application-based plan
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, the financial sector has collectively undertaken efforts to begin to define and implement efforts to address it.

FS-ISAC

Formed in 1999 in response to a Presidential Decision Directive, 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 focused subsidiaries described below (FSARC and Sheltered Harbor) that conduct deeper analysis, and other forms of collaboration, and develop standards. FS-ISAC also maintains the financial services sector's "All Hazards Crisis Response Playbook", which outlines the processes and considerations for identifying and responding to significant threats or events. Taken together, FS-ISAC efforts provide situational awareness and raise awareness of the changing threat environment across all hazards including cyber, physical, and geo-political to its membership of over 7,000 financial firms.

DRAFT

FSARC

The Financial Systemic Analysis and Resilience Center[4] ("FSARC") was established in 2016 as an industry funded nonprofit entity that's mission is to increase the resiliency of the critical must run systems that underpin the US financial services sector. FSARC facilitates operational collaboration between participating financial institutions and market utilities, the US Government, and other key sector partners in a controlled 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. 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 in these systems does not have a broader systemic impact. The FSARC initiatives, and the outputs of them, for individual firms and the broader sector writ large all support the concept of operational resilience and will continue 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 U.S. Department of 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 market participants in order to facilitate the recovery of such information following an incident. Sheltered

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

Harbor coordinates the development of the data protection and portability standard, promotes 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

Overall, FSSCC encourages efforts to work collaboratively across firms to develop solutions to 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.

DRAFT

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. 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. Hyper-connectedness of financial firms requires planning for business operational resilience, not only individually but systemically. A single event is more likely to impact the entire value chain of a transaction, potentially including other financial and non-financial firms, than a single customer or entity. Therefore, it is a critical and shared duty for every financial firm 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 scenarios that may have originally been considered implausible and defining impact tolerances.
- Establishing a framework for assessing and preparing critical business services for restoration to identify the 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 across the sector.
- Supporting regulators in establishing standards that could be benefited by similar critical infrastructure sectors like healthcare, energy, utilities, and transportation.

Efforts to address business service resilience and restoration will require full sector engagement and numerous workstreams. Many of these efforts will be spear headed through SIFMA, whichis 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 will build upon past work conducted by the sector, such as the SIFMA Quantum Dawn exercises and the Hamilton Exercises led by the U.S. Department of Treasury.

DRAFT

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 is the plan, 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 new capabilities ("new normal") in the event previous capabilities cannot be recovered through established BC/DR processes.

Disaster Recovery is the process of recovering from major processing interruptions. Disaster Recovery is typically limited to one segment of the organization (region, data, center, etc.) and may include:

- 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.

Operational Resilience is the implementation of techniques to continue to provide services 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 foreseeable outages and disruptions.

DRAFT

About FSSCC

Formed in 2002 as a public/private partnership with the support of the U.S. Department of 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.

DRAFT