a) Operational Resiliency

Return to Question 13-1 | **Provide Feedback**

Overview

Return to Top

Within the context of CBDC, Operational Resilience needs to address things which can not be added on *post facto* or *"bolted on"* easily after the CBDC is deployed. In other words, it must be *"baked in"* so to speak. This means that for something new, like the CBDC, it starts with specifying both non-Functional and Functional Requirements. The specification of requirements needs to be done as soon as possible. Granted, the system must be agile and adapt to unforeseen changes in the deployment environment, threats, exploits, etc. However, there is a fine line between being "agile" and Scope Creep. Agile should not be defining or redefining major functional or non-function requirements, but rather defining or refining Software Requirements such as Business Requirements, User Requirements. Granted, some functional and non-functional can evolve over time, but usually as a result of a discovery process conducted during Research Development Test & Evaluation phases of a project, not during the production of a deployable system. Sometimes a Proof-of-Concept or Prototype Model[1)]. The Prototype model can work in areas such as Web Development, but not in the development of Mission Critical Systems. For Mission Critical Systems, the prototype is used as "throwaway" code used to capture and refine more formalized requirements.

Operational Resiliency also means once the CBDC is up and operational, it needs to respond to internal issues requiring continuous monitoring and adaptation of the CBDC in order to ensure it continues to have Operational Resiliency and that it can evolve and live beyond any existing software or hardware component that comprises the CBDC. In the U.S. Navy, this is referred to as "reboot the Navy" In other words, it is not possible to reboot all the systems on a ship or within a fleet at the same time and still maintain operational purpose. Likewise, in distributed systems, it is not possible to update all the parts at one time; sometimes older parts may take years to update. Also, see the OMG DIDO-RA sections on:

- Reboot the World Problem
- Software Interfaces
- Replaceability
- Extensible and Dynamic Topic Types for DDS (DDS-XTypes)

Operational Resiliency also means a system must continue to adapt to the threats (i.e., hostile cyber threats and physical threats like hurricanes, earthquakes, and fire), as well as, evolving national and geopolitical situations. The current Ukraine-Russian conflict is a prime example. This type of flexibility needs to be planned into the CBDC and not done as an *impromptu* reaction. See **Reboot the World Problem** above.

In other words, Operational Resiliency for the CBDC is not a *"done and dusted"* sort of problem, rather, it is a continuous process that covers the entire lifecycle of the CBDC or follow-on efforts.

Understanding the "What ifs"

Return to Top

A key aspect of obtaining **Operational Resiliency** is to develop *"what-if"* scenarios to validate the resilience of the system against functional and non-Functional requirements. Some possible scenarios might be:

- What if there is an upgrade to an Operating System?
- What if a key component of the CBDC system is obsolete and no longer available?
- What if there is a network outage in the NE U.S.?
- What if there is a network failure crossing the Atlantic?
- What if there is a breach of security from personnel?
- What if there is a compromise in the data access?
- What if there is a 10-fold demand for access to CBDC infrastructure?
- What if the value of the U.S. Dollar goes up or down against the rest of the world currencies?
- What happens if there is a war?

A well-defined Resilience Plan addressing the specific Functional and non-Functional requirements is essential. Trying to reverse engineer these requirements from an existing system adds a lot of risks and indicates the system is not designed but the result of Organic Development[2)]. While this makes sense for products with a short life span and is not Mission Critical, it is not going to:

- Instill confidence (i.e., **B0020**)
- Preserve the dominant role of the U.S. Dollar (i.e., **B0036**)
- Provide broad support from CBDC Stakeholders (i.e., **B0006**)
- Provide trusted central bank money (i.e., **B0027**).

Understanding the Requirements

Return to Top

The following is an outline from the OMG's DIDO-RA for non-Functional Requirements and should be reviewed and assessed for applicability to the CBDC. In essence, each of the **non-functional** requirements should be considered carefully and tailored to the needs of the Federal Reserve and the CBDC.

1. Portability

- Adaptability
- Installability
- Replaceability

2. Reliability

- Maturity
- Availability
- Fault Tolerance
- Recoverability

3. Maintainability

- Modularity
- Reusability
- Analysability
- Modifiability
- https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:2_nonfunc:20_maintainability:testabilityTestability

4. Security

- Confidentiality
- Data Integrity
- Non-Repudiation
- Authenticity
- Accountability

5. Manageability

- Types of Manageability Functions
- Manageability Costs
- System Manageability Issues
- Software Manageability Issues

6. Usability

- Effectiveness Metrics
- Efficiency Metrics
- Attitude / Satisfaction Metrics

7. Performance

- Platform Performance
- Application Performance
- Network Performance

8. Interoperability

9. Elasticity

10. Scalability

The following is an outline from the OMG's DIDO-RA for Functional Requirements, and should be reviewed and assessed for applicability to the CBDC. In essence, each of the **functional** requirements should be

considered carefully and tailored to the needs of the Federal Reserve and the CBDC. For example, making a decision as to which **Hardware Platform(s)** or **Operating System Platform** to use has huge long range impacts on the CBDC and can ultimately negatively impact some non-Functional requirements such as **Portability**, **Replaceability**, **Manageability Costs** (See: Vendor Lock-In).

1. Platforms

   - Hardware Platform
   - Operating System Platform
   - Runtime Platforms
   - Network Platforms
   - Virtualized Nodes

2. Access Control

Steps to Achieving Operational Resilience

Return to Top

The following is an excerpt is from a blog from Matt Kunkel on *"What is Operational Resilience?"*[3)]

1. ***Take a holistic view of organizational risk.*** *Consider internal and external factors that impact your organization including business lines, assets, systems, processes, third parties, and people. Building a resilient operation means seeing the interconnection and interdependence of risk throughout the organization. Effective enterprise risk management systems must look across divisions and operations to holistically assess and account for potential threats.*
2. ***Design systems that take a comprehensive approach to risk assessment.*** *This starts with translating risk into a language that everyone at the firm understands. Having common vernacular permits a more comprehensive analysis and documentation of potential risks throughout the organization. It also allows for a more robust discussion around risk and returns as organizations consider how to adapt to changing conditions. Moreover, a shared language permits greater collaboration and cooperation, both critical to building a deeper understanding of the interdependence of risk in the organization and building operational resilience.*
3. ***Assess for critical points of failure to inform robust processes, ensure systems capabilities, and cultivate adaptable practices.*** *Although no market disruption or business interruption is the same, much can be learned from each. Knowing where the key risks lie across the organization and proactively implementing potential workarounds can help organizations better adapt to evolving conditions. The key is having robust systems and flexible processes, as well as cultivating a collaborative and resilient culture.*

Strengthing Operational Resilience

Return to Top

Another blog post from Dominick Campagna defines five ways to strengthen **Operational Resilience** in the Financial Services Sector[4)] and should include the CBDC.

> *For any financial services company, big or small, failure is not an option. Financial services play a critical, foundational role in almost every sector of the economy, and robust customer service is expected through technology failures, market disruption, systemic risk events, natural disasters, and even pandemics.*
>
> *Companies that can deliver robust services through unexpected disruptions are considered operationally resilient. The critical importance of operational resilience in financial services is evidenced by the flurry of guidance from global financial regulators detailing expectations and mandating best practices on how providers and supporting infrastructure can improve their operational resilience.*
>
> *Operational resilience, as **defined by the Federal Reserve Board (FRB)**, is the ability to deliver operations, including critical operations and core business lines, through disruption from any hazard. Last October, the FRB, in partnership with the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation, issued an interagency paper on Sound Practices to Strengthen Operational Resilience. This guidance, specifically written for banks and savings and loan companies with at least $100 billion in assets, can be adapted and applied to financial services companies of any size.*
>
> *In short, operational resilience is built through "effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions." More than business continuity, which is focused on uninterrupted operations, operational resilience considers how to best adapt a firm's operations to deliver services through any disruption.*

Table 1: 5 Ways to Strengthen Operational Resilience in the Financial Services Sector. [5)]

Step	**Description of Activities**
1. Establish Effective Governance	Effective governance at the board and senior management level are critical to strengthening operational resilience. A strong risk management culture—the foundation of operational resilience—can only happen when there is top-down, organizational commitment. Board and executive responsibilities lay the groundwork and accountability for an operationally resilient mindset and commitment to supporting practices throughout the organization.

Step	Description of Activities
2. Identify Critical Assets	Disruption, by its nature, is unpredictable. Operational resilience is not about identifying and measuring risks and uncertainty, as the impact of evolving technology and market changes can rarely be predicted. It is instead a framework for protecting the core business. The identification of critical assets and functions and core business lines should be done with the intention of protecting those assets and operations regardless of the source of disruption. Whether impacted by an unexpected technology failure, pandemic, cybersecurity incident, or any other cause, and the operationally resilient firm will have the policies, procedures, and practices in place to guide them through any disruption. To do this systematically, the board must determine and approve the risk appetite and risk tolerance for operational disruption, both at the enterprise level and for critical operations and core business lines. These explicit board parameters for the firm's acceptable level of risk from operational disruption can guide effective decision-making, appropriate investment in resilient systems and controls, and a consistent firm-wide approach to operational risk management.
3. Consider Key Dependencies and Interconnections	After identifying the core business lines and critical assets and functions, consider the key personnel, technology, processes, data, and physical infrastructure facilities required to protect them. Understanding those inputs and mapping out the dependency and interconnection of those assets on other internal functions, external parameters, or third parties will support a robust plan for business continuity and operational resilience. Managing third-party risk is critical for operational resilience, given the growing dependence on third parties to maintain specific functions and services of core business lines. This risk must also be accounted for within the approved risk tolerance. An understanding of the entire picture is necessary for recovery planning and the build-out of appropriate redundancies and alternate availability of essential resources, personnel, technology capability, and, if necessary, physical infrastructure. Recovery planning should also be consistent with existing risk management practices to ensure that there are no gaps in providing service or meeting regulatory requirements.
4. Proactively Review and Audit Plans	Operational resilience is a dynamic process requiring periodic review, testing, and auditing. As systems and processes evolve, so should your plans. Regularly employing an internal or external audit function to assess the design and effectiveness of operational resilience efforts will help to keep your plans relevant, identify shortcomings due to process or policy changes, and support a firm-wide culture of risk management and operational resilience. As new infrastructure and technology are adopted, your plans should be revisited and tested. Any digital transformation efforts should include planning for and adopting policies to address digital risks, such as disruption due to an internal failure, cybersecurity incident, or processing error. Consistent testing of your operational resilience plans, including dependencies and interconnections, will prepare your firm to pivot and adapt quickly to a disruption.

Step	Description of Activities
5. Form a Collaborative Approach to Operational Risk Management	An operational risk management function is responsible for determining and managing exposure related to internal processes, people, and systems as well as external threats and third parties. However, they cannot do this in a silo. Effective operational risk management requires a collaborative approach between senior management, business units, the operational risk management function or designees, and the internal or external audit function. A cross-functional approach supports effective identification, mitigation, and resolution of operational risk, including technology and third-party risk, within the risk appetite and risk tolerance defined by the board while collaboration ensures a consistent, firm-wide approach and commitment to operational resilience.

1)

The prototyping model is a software development model in which a prototype is built, tested, and reworked until an acceptable prototype is achieved. It also creates a base to produce the final system or software. It works best in scenarios where the project's requirements are not known in detail. It is an iterative, trial and error method that takes place between developer and client. Matthew Martin, Prototyping Model in Software Engineering: Methodology, Process, Approach, Guru99, 5 March 2022, Accessed: 17 May 2022, https://www.guru99.com/software-engineering-prototyping-model.html

2)

Organic Development is the internal growth based on adjusting and adapting to the situations at hand. For example, new information systems might evolve incrementally based on user feedback rather than starting anew with a system from a third party.

3)

Matt Kunkel, What is Operational Resilience?, Logicgate, 17 September 2020, Accessed: 11 April 2022, What is Operational Resilience?

4) , 5)

Dominick Campagna, 5 Ways to Strengthen Operational Resilience in the Financial Services Sector, Logicgate, 22 January 2021, Accessed: 11 April 2022, https://www.logicgate.com/blog/5-ways-to-strengthen-operational-resilience-in-the-financial-services-sector/