1. How could a CBDC be designed to foster operational and cyber resiliency?

Return to Question 13

Although Cyber Resiliency is affected by the Operational Resiliency of the system as a whole, the two topics need to be treated separately. Therefore, the question has been subdivided into two questions:

a) Operational Resiliency
b) Cyber Resiliency

a) Operational Resiliency

Return to Top

Within the context of CBDC, Operational Resilience needs to address a 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 that is new, like the CBDC, it starts with spcifying the requirements, both non-Functional and Functional Rerquirements. The specification of the requirements need to specifically call out the requirements as soon as possible. Granted, the system must be agile and adoapt to unforeseen changes in the deployment environment, threats, expoits, etc. However, if these are not specified as requirements, the impact of these changes can be extraordinary. For example, tying functionality to specific Operating System(OS) or a version of an OS rather than using standard, more portable altrnatives (i.e., Windows 7 or Windows 10 versus POSIX). Relying on Operating System sockets versus higher abstraction layers such as DDS.

Operational Resiliency also means once the CBDC is up and opertional, it needs to respond to internal issues requiring continuous monitoring and adaptation of the CBDC to ensure it continues to have Operational Resiliency and also that it able to evolve to live way beyond any existing software or harward 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. In distributed systems it is not possible to update all the parts at one time and sometimes older parts might 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 that it must continue to adapt to the surround situations (i.e., hostile cyber threats, physical threats like hurricanes, earthquakes, and fire) and evolving national and geopollitical situations. The current Ukraine-Russian conflict is a prime example. This type of flexibility needs to planned into the CBDC and not done as an *impromtu* reaction. See **Reboot the World**

Problem above.

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

A key aspect of Operational Resiliency is to develop *"what-if"* scenarios to validate the resilence of the system against the 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 personel breach of security?
- What if there is a compromise in the data access?
- What if there is a 10-fold demand for access to CBDC infrastructure?
- What id the 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 what these requirements are from an existing system adds a lot of risk and indicates that the system is not designed but is the result of Organic Development[1)]. While this make sense for products that have a short life span and are not Mission Critical, it is not going to:

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

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.

- 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_maintainabil

ity: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 Platforms** or **Operating System Platform** has huge long range impacts on the CBDC and ultimately can restrict some of the non-Functional requirements such as **Portability**, **Replaceability**, **Manageability Costs** (See: Vendor Lock-In).

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

2. Access Control

The following is an excerpt is from a blog from Matt Kunkel on *"What is Operational Resilience?"*[2)]

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 a 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 return 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.*

Another blog ppost from Dominick Campagna defines five ways to strength **Operational Resilience** in the Financial Services Sector[3], which 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.[4]

1. Establish Effective Governance	Effective governance at the board and senior management level is 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.
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, an operationally resilient firm will have the policies, procedures, and practices in place to guide them through any disruption. To do this in a systematic way, 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 buildout 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 is adopted, your plans should be revisited and tested. Any digital transformation efforts should include planning for and adoption of policies to address digital risk, 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 through a disruption.
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.

b) Cyber Resiliency

Return to Top

The first step in designing for Cyber Resiliency is to begin with a Systems Engineering approach and to survey CBDC Stakeholders to refine the definitions and expectations of Cyber Resiliency. See CBDC Stakeholders for a more detailed discussion.

An important first step needs to be to follow the NIST Special Publication SP 800-16 volume 2 guidelines for developing cyber-resilient systems.[5)]. Skipping this step and going right to design and implementation often ends with the problem space (i.e., CBDC) being defined by the product(s) it chooses to use rather than by the stakeholders requirements. A product based solution can work, but it often misses many key requirements important to the stakeholders. For example, the design must be Quantum Computing “safe” or resistent.

SP 800-16 provides a framework for conducting cyber resiliency engineering. It starts with defining and setting the goals, objectives, techniques, implementation approaches, design principles. Table 2 summarizes the definition and purpose of each construct, and how each construct is applied at the system level. **Note:** The framework is applicable to levels beyond the system level (e.g., mission or business function level, organizational level, or sector level).

Table 2: Cyber Resiliency Constructs[6)]

Construct	Definition, Purpose, and Application at the System Level
Goal	A high-level statement supporting (or focusing on) one aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyber resiliency. **Purpose:** Align the definition of cyber resiliency with definitions of other types of resilience. **Application:** Can be used to express high-level stakeholder concerns, goals, or priorities.
Objective	A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security. The objectives are more specific than goals and more relatable to threats. **Purpose:** Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate the definition of metrics or Measures of Effectiveness (MoEs). **Application:** Used in scoring methods or summaries of analyses (e.g., cyber resiliency posture assessments).
Sub-Objective	A statement, subsidiary to a cyber resiliency objective, that emphasizes different aspects of that objective or identifies methods to achieve that objective. **Purpose:** Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. **Application:** Used in scoring methods or analyses; may be reflected in system functional requirements.
Activity or Capability	A statement of a capability or action that supports the achievement of a sub-objective and, hence, an objective. **Purpose:** Facilitate the definition of metrics or MoE. While a representative set of activities or capabilities have been identified in [Bodeau18b], these are intended solely as a starting point for selection, tailoring, and prioritization. **Application:** Used in scoring methods or analyses; reflected in system functional requirements.
Strategic Design Principle	A high-level statement that reflects an aspect of the risk management strategy that informs systems security engineering practices for an organization, mission, or system. **Purpose:** Guide and inform engineering analyses and risk analyses throughout the system life cycle. Highlight different structural design principles, cyber resiliency techniques, and implementation approaches. **Application:** Included, cited, or restated in system non-functional requirements (e.g., requirements in a Statement of Work [SOW] for analyses or documentation).

Once the Systems Engineering is completed, a design can be made to foster cyber resiliency.

1)

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.

2)

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

3) 4)

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/

5) 6)

Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie McQuaid, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, National Institute for Standards and Technology (NIST), NIST Special Publication 800-160, Volume 2, Revision 1, December 2021, Accessed: 11 April 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf