Question: 13. TBD How could a CBDC be designed to foster operational and cyber resiliency? What operational or cyber risks might be unavoidable?

Return to CBDC Benefits, Risks, and Policy Considerations

Question

Return to Top

1. How could a CBDC be designed to foster operational and cyber resiliency?
2. What operational or cyber risks might be unavoidable?

Answer

Return to Top

In order to answer this compound question, each part of the question is answered separately:

- 1. How could a CBDC be designed to foster operational and cyber resiliency?
- 2. What operational or cyber risks might be unavoidable?

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

Return to Top

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

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.[1)]. 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 1 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 1: Cyber Resiliency Constructs[2)]

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.

Construct	Definition, Purpose, and Application at the System Level
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.

2. What operational or cyber risks might be unavoidable?

Return to Top

References

Return to Top

Table 2: Guiding Document Specifics

Source	Money and Payments: The U.S. Dollar in the Age of Digital Transformation
Published Date:	January 2022
Requestor	Board of Governors, The Federal Reserve System
Area	Research and Analysis

[1)] [2)]

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