2. What operational or cyber risks might be unavoidable?

Return to Question 13 | **Provide Feedback**

Overview

Return to Top

The biggest Risks to the CBDC is related to the Information Technology(IT) infrastructure for the CBDC and the need to ensure the CBDC meets the quality expectations of the U.S. Federal Reserve and the public. For example, the White Paper Desirements

- **B0020** is about establishing maintaining public confidence as a priority
- **B0027** and **B0050** are about establishing a priority on safe and trusted central bank money
- **R0011** is concerned about loss, theft, and fraud

These are unique problems for The Federal Reserve or to U.S. CBDC. These problems have been addressed by standards aimed at minimizing risk to projects heavily dependent on Software:

See the the OMG DIDO-RA section on:

- Quality
- Open Source Paradigm
- Assurance

Specification versus Standards

Return to Top

The difference between Specification and Standard is a specification is an explicit set of requirements to be satisfied by a material, product, or service. A Standard is a principle or example or measure used for comparison.

A Specification are statements detailing the requirements of a system or product that **should** or **must** be satisfied depending on the regulatory or contractual context. The Specification includes work products such as the definition of Protocols, Application Programming Interfaces (API), or the definition of processes. A Standard is a specification established by institutions such as Standards Developing Organization (SDO) or a Voluntary Standards Consensus Body (VSCB). Standards can be classified as Technical or *de facto* Standards.

ISO, IEC, IEEE Standards

Return to Top

The purpose of ISO/IEC 25000 is to provide a general overview of SQuaRE contents, common reference models, and definitions, as well as, the relationship among the documents, and allow users of the Guide to gain a good understanding of how to use this series of standards. It also contains an explanation of the transition process between the old ISO/IEC 9126 and the newer ISO/IEC 14598 series and SQuaRE.

Figure 1: Quality Characteristics and Measures Specifications

- ISO 9001:2015 Quality management
- ISO/IEC/IEEE 90003:2018 Software engineering – Guidelines for the application of ISO 9001:2015 to computer software
- ISO/IEC/IEEE 25000:2014 SQuaRE -- Guide to SQuaRE
- ISO/IEC 25001:2014 SQuaRE -- Planning and Management
- ISO/IEC 25010:2011 SQuaRE -- System and Software Quality Models
- ISO/IEC 25012:2008 SQuaRE -- Data Quality Model
- ISO/IEC 25020:2007 SQuaRE -- Measurement Reference Model and Guide
- ISO/IEC 25021:2012 SQuaRE -- Quality Measure Elements
- ISO/IEC 25022:2016 SQuaRE -- Measurement of Quality in Use
- ISO/IEC 25023:2016 SQuaRE -- Measurement of System and Software Product Quality
- ISO/IEC 25024:2015 SQuaRE -- Measurement of Data Quality
- ISO/IEC 25030:2007 SQuaRE -- Quality Requirements
- ISO/IEC 25040:2011 SQuaRE -- Evaluation Process
- ISO/IEC 25041:2012 SQuaRE -- Evaluation Guide for Developers, Acquirers and Independent Evaluators
- ISO/IEC 25045:2010 SQuaRE -- Evaluation Module for Recoverability
- ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes

Object Management Group (OMG) Standards and Consortium for Information & Software Quality (CISQ)

Return to Top

The Consortium for Information & Software Quality (CISQ) develops international standards to automate the measurement of software from source code. The industry needs standard, low-cost, automated measures for evaluating software size and structural quality that can be used to control the quality, cost, and risk of software produced internally or by third parties.

Automation is critical because the manual review is infeasible for large multi-layer, multi-language, multi-platform systems. Additionally, DevOps greatly speeds up the deployment of applications, some changing on a daily or even hourly basis, which may result in unintended vulnerabilities without review.

- OMG: Automated Source Code CISQ Maintainability Measure (ASCMM)
- OMG: Automated Source Code CISQ Measures (ASCQM)
- OMG: Automated Source Code CISQ Performance Efficiency Measure (ASCPEM)

- OMG: Automated Source Code CISQ Reliability Measure (ASCRM)
- OMG: Automated Source Code CISQ Security Measure (ASCSM)
- OMG: CISQ Automated Enhancement Points (AEP)
- OMG: CISQ Automated Function Points (AFP)
- OMG: CISQ Automated Technical Debt Measure (ATDM)

The Case Management Model and Notation (CMMN) specification defines a common meta-model and notation for modeling and graphically expressing a Case, as well as an interchange format for exchanging Case models among different tools. The specification is intended to capture the common elements that Case management products use, while also taking into account current research contributions to Case management. It is to case management products what the OMG Business Process Model and Notation (BPMN) specification is to business process management products. This specification is intended to be consistent with and complementary to BPMN.

- OMG: Case Management Model and Notation (CMMN)

The Structured Assurance Case Metamodel (SACM) specification defines a metamodel for representing structured assurance cases. An Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements. An Assurance Case is a document that facilitates information exchange between various system stakeholders such as suppliers and acquirers, and between the operator and regulator, where the knowledge related to the safety and security of the system is communicated in a clear and defendable way. Each assurance case should communicate the scope of the system, the operational context, the claims, the safety and/or security arguments, along with the corresponding evidence.

- OMG: Structured Assurance Case Metamodel (SACM)

The Test Information Interchange Format (TestIF) goal is to achieve a specification that defines the format for the exchange of test information among tools, applications, and systems that utilize it. The term “test information” is deliberately vague, because it includes the concepts of tests (test cases), test results, test scripts, test procedures, and other items that are normally documented as part of a software test effort. The long term goal is to standardize the exchange of all test-related artifacts produced or consumed as part of the testing process,

- OMG: Test Information Interchange Format (TestIF)

State of Data

Return to Top

Data can exist in many states depending on how it is being used. The risks and concerns about Data in each of its different states are also important. Often, the primary focus for understanding data is to concentrate on Data-at-Rest . Even though data tends to remain relatively static, it can change over time. In the past, there was little concern for Data-in-Motion , which can have serious effects on Reliability, Maintainability, and Availability (RAM), as well as, Securability and can leave a system vulnerable to breaches. With the advent of HTTPS, these vulnerabilities are mitigated. The latest issue has become the need to secure Data-in-Use. A recent WhatsApp data breach[1)] found that switching data

between image filters could cause memory corruption followed by a crash that left data exposed.

Figure 2 graphically represents the different Data States within a system. Most systems are now able to handle Data-in-Motion and Data-at-Rest issues but have traditionally relied on physical security to protect Data-in-Use.

Figure 2: The various States of Data

Table 1 provides a quick overview of the various data states. These data states are described in detail in the OMG DIDO-RA.

Table 1: Data can exist in the following different states

Data-at-Rest	Data-at-Rest refers to all data in computer storage. It excludes data while it is moving across or within a network, and it excludes data that is temporarily residing in computer memory.
Data-in-Motion	Data-in-Motion , also referred to as **Data in Transit** or **Data in Flight**, is a Digital Asset transmitted between locations (i.e., between computers or computer components). Data-In-Motion also describes data within Random Access Memory (RAM).
Data-in-Use	Data-in-Use covers data being processed (i.e., updated, processed, erased, accessed or read) by a system. Data-In-Use is not passively stored, but is actively moving through parts of a Computing Platform (i.e., Central Processing Unit (CPU), Dynamic Random Access Memory (DRAM),, Data Bus, etc.). **Data-In-Use** is one of three states of digital data – the other states are Data-at-Rest and Data-in-Motion.

Examples

Return to Top

Some “desirements” in the Money and Payments: The U.S. Dollar in the Age of Digital Transformation **White Paper** and relating to **Operational or Cyber Risks** are summarized in the White Paper Analysis done by the Object Management Group's CBDC WG and listed in Table 2.

Table 2: List of Operational or Cyber Risks Desirements identified in the White Paper

Category	**Desirements**
Benefits	B0020, B0027, B0048, B0050, B0053, B0054
Policy Considerations	P0012, P0017, P0020, P0021, P0025, P0027, P0028
Risks	R0011
Design	D0015, D0016, D0017

Discussion of Examples

Return to Top

Table 3 comments on those “desirements” identified by the White Paper and the OMG's CBDC WG White Paper Analysis relating to Central Bank Digital Currency (CBDC) Operational or Cyber Risks. See: Table 5 in Section 4.1 Stakeholders.

Table 3: List of *“desirements”* that allude to **stakeholders**

Desirement No.	Desirement Text	Comment
B0020	**Maintain public confidence by not requiring mechanisms, such as deposit insurance**	This is highly dependent on the Currency Model used for the CBDC. If it is Digital Cash Model then the need for deposit money is nil, since there are no deposits (i.s., just like there is no insurance on U.S. Dollars). However, if it is based on a Digital Account Model, then by definition there are accounts, and by experience, deposit insurance is required to stabilize (See: **R0012**) the assets stored in those accounts. Deposit insurance provides three important benefits to the economy:[2)] 1. It assures small depositors that their deposits are **safe** and will be immediately available to them if their bank fails.(See: **B0007**, **B0019**, **B0027**, **B0050**) 2. It maintains public **confidence** in the banking system, thus fostering economic stability. Without the confidence of the public, banks could not lend money but would have to keep depositors' money on hand in cash at all times. (See: **R0009**, **R0012**) 3. It **supports the banking structure**. Deposit insurance makes it possible for the United States to have a system of both large and small banks. If there were no deposit insurance, the banking industry would probably be concentrated in the hands of a very few enormous banks. (See: **R0001**, **R0003**, **R0018**)
B0027	**Maintain the centrality of safe and trusted central bank money**	Safety and trust are both about perceived risk. 1. Safety is defined as freedom from risk and risk is the possibility of suffering harm or loss. Both controllable and uncontrollable factors affect risk[3)]. 2. Risk and trust are inextricably intertwined and loss of trust is possibly the biggest risk an endeavor can encounter since trust is the basis of all interactions. Therefore, the key is to manage risk, which is the probability or threat of damage, injury, liability, loss, or any other negative occurrence caused by external or internal vulnerabilities, and that may be avoided through preemptive action. The goal of Systems Engineering is to manage the risk, including the risk of not delivering what the customer wants and needs, the risk of late delivery, the risk of excess cost, and the risk of negative unintended consequences. One measure of the utility of Systems Engineering activities is the degree to which such risk is reduced. Conversely, a measure of acceptability of the absence of a System Engineering activity is the level of excess risk incurred as a result.

Desirement No.	Desirement Text	Comment
B0048	**Provide a secure way for people to save**	In the U.S., savings accounts are a safe place since deposits (with limits) are guaranteed by Federal Deposit Insurance Corporation (FDIC) or the National Credit Union Administration (NCUA). Additionally, Certificates of Deposit (CDs) and U.S. government securities are also considered safe savings places. Both of these options offer some return on money. However, money safety is often associated with a high degree of liquidity, and relatively low fees.
B0050	**Extend Public Access to Safe Central Bank Money**	1. The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals See: **P0018** 2. Federal Reserve accounts for individuals represent a significant expansion of the Federal Reserve's role in the financial system and the economy. See: **P0019**
B0053	**Provide resiliency to threats to existing payment services—including: 1. operational disruptions 2. cybersecurity risks**	See the Overview of "What operational or cyber risks might be unavoidable?"
B0054	**Attract risk-averse users to CBDC**	The term **Risk-Averse** describes the investor who chooses the preservation of capital over the potential for a higher-than-average return. In investing, risk equals price volatility. A volatile investment can make you rich or devour your savings. A conservative investment will grow slowly and steadily over time. https://www.investopedia.com/terms/r/riskaverse.asp
P0012	**The firms that operate interbank payment services are subject to federal supervision**	See the detailed discussion in section 4.5 National Security Considerations.
P0017	**The PWG report recommends CBDC complement existing authorities regarding: 1. market integrity 2. investor protection 3. illicit finance**	See: 1. 4.1 Stakeholders 2. 4.4 National Privacy Considerations 3. 4.5 National Security Considerations

Desirement No.	Desirement Text	Comment
P0020	**The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments**	Although the private sector is more than willing to take on this role, without some assurance that the wallets cannot be hacked and any losses will be covered by insurance, achievement of this desirement will probably have limited success. Hacks and data breaches happen almost daily. Cryptocurrency exchange hacks are particularly damaging because it affects thousands of users and involves the loss of funds. [4)]. *Cryptocurrency exchanges come and go, and it's almost inevitable that an exchange will get hacked at one point or another. While cryptocurrencies themselves are very secure, exchanges can be affected by a variety of vulnerabilities, making them a prime target for malicious actors.* *State of the industry – February 2020: As it stands, 2019 saw a record number of twelve crypto exchanges being hacked. That being said, across the board the amounts of crypto stolen were worthless. In total,* ***\$292,665,886 worth of cryptocurrency and 510,000 user logins were stolen from crypto exchanges in 2019****.* *One would hope that as time goes on cryptocurrency exchanges would become more secure. The unfortunate reality is that more exchanges are hacked every year. As cryptocurrency and exchanges remain largely unregulated, it is unclear who has jurisdiction over cryptocurrency markets.* in 2019, there was a hack of a South Korean exchange that suffered a \$51 million dollar breach. The stolen crypto has been on the move. It is moving between wallets, although it is unclear what purpose this will serve. At the current time, it is easy for exchanges or wallets to make lots of claims about security, but until there is a detailed assurance claim model to substantiate the claims, the promises are hollow. See: 1. OMG: Structured Assurance Case Metamodel (SACM) 2. OMG: Test Information Interchange Format (TestIF) 3. OMG: Case Management Model and Notation (CMMN)

Desirement No.	Desirement Text	Comment
P0021	**The intermediaries would operate in an open market for CBDC services**	The lion's share of U.S. CBDC intermediaries will be building, delivering, and offering the services of software applications. This is not unlike the current situation in the smartphone world. However, the intermediary's applications will have to run not just on smartphones, but also on personal computers, servers, and mainframes. The Federal Reserve and a U.S. CBDC must be able to achieve and retain the confidence of consumers that these applications are sufficiently robust and provide reliable security to hold their vital assets. Therefore, there is a need for a U.S. CBDC “application store” to act as a web portal through which end users can access, download and install U.S. CBDC-approved software applications that rigorous Assurance Case Models with which the quality and security of these applications are validated. See: 1. OMG: Structured Assurance Case Metamodel (SACM) 2. OMG: Test Information Interchange Format (TestIF) 3. OMG: Case Management Model and Notation (CMMN)
P0025	**CBDC intermediary would need to verify the identity of a person accessing CBDC**	1. If the Digital Cash Model is used, then just like physical cash, there should be no IDs required. 2. If the Digital Account Model is used, it might depend on the rules placed on the intermediaries, Here are the rules for cashing checks in the U.S.: a. When cashing a check, people use an ID to complete the transaction. Banks are required to have an identity verification policy by the Federal Deposit Insurance Corporation, which is why an ID is necessary[5)] i. Ways of not showing an ID for cashing checks are: 1. *Signing it over to another individual* 2. *Using ATM check to cash if it’s offered by your bank* 3. *Depositing it into your own account using a bank ATM* b. When using Credit Cards, the major Credit Cards (i.e., Visa and Mastercard) do not require an ID to complete a transaction. *They both have rules that limit stores from requiring you to show your ID as a condition of purpose. These rules also make them accept your card even if you refuse to show your ID.*[6)]
P0027	**CBDC a risk-free asset**	The risk-free rate of return is the theoretical rate of return of an investment with zero risk. The risk-free rate represents the interest an investor would expect from an absolutely risk-free investment over a specified period of time. The so-called “real” risk-free rate can be calculated by subtracting the current inflation rate from the yield of the Treasury bond matching your investment duration. https://www.investopedia.com/terms/r/risk-freerate.asp

Desirement No.	Desirement Text	Comment
P0028	**Require significant international coordination to address issues such as: 1. common standards 2. infrastructure, 3. the types of intermediaries able to access any new infrastructure, 4. legal frameworks 5. preventing illicit transactions 6. the cost and timing of implementation**	See: 4.6 International Considerations
R0011	**Increased Risk to consumer's vulnerability to: 1. loss 2. theft 3. fraud**	If the U.S. CBDC avoids most of the safeguards built into the current U.S. financial system, then there is an increased risk of **loss**, **theft**, and **fraud**. Most of the laws and regulations outlined in section 4.5 National Security Considerations have evolved over time in response to consumer demand for protection. Although it seems appealing, more efficient, and even "modern", consumers should demand the same level of protection from a U.S.-based CBDC. According to Ryan Browne of CNBC[7)] • *Overall losses caused by Decentralized Finance (DeFi) exploits have totaled \$12 billion so far in 2021, according to a report from Elliptic.* • *Fraud and theft accounted for \$10.5 billion of that sum — a sevenfold increase from last year.*

Desirement No.	Desirement Text	Comment
D0015	**Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks**	In order to protect data during all aspects of data handling and processing, there will most likely need to be new network hardware, computer processors, and even new encryption algorithms based on Quantum Computing's ability to crack encryption. See: 1. State of Data 2. OMG DIDO-RA Network Devices 3. Data in Use 4. Access Control List (ACL) 5. Zero Trust Security Model 6. Zero Trust Architecture (ZTA) 7. The Onion Router (Tor) 8. Secure Memory Encryption (SME) 9. Full Memory Encryption (FME) 10. Total Memory Encryption (TME) 11. Software Guard Extensions (SGX) 12. Multi-Party Computation (MPC) 13. TRESOR 14. Homomorphic Encryption (HE)
D0016	**Design should include offline capabilities to help with the operational resilience of the payment system**	See: Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?
D0017	**Design should include digital payments in areas suffering from large disruption, such as natural disasters**	See: Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?
B = Benefit Considerations		
P = Policy Considerations		
R = Risk Considerations		
D = Design Considerations		

1)

Czarina Grace, WhatsApp Data Breach 2021 Could Expose 2 Billion Users: Update Now on Android, iOS to Fix Security Risk, iTechPpost, 6 September 2021, Accessed 6 October 2021, https://www.itechpost.com/articles/106929/20210906/whatsapp-data-breach-2021-expose-2-billion-users-update-now.htm

2)

State of Connecticut, Department of Banking, ABC's of Banking, Accessed: 13 April 2022, https://portal.ct.gov/DOB/Consumer/Consumer-Education/ABCs-of-Banking---Deposit-Insurance

3)

Derek Lann, What is the Relationship Between Safety and Risk? Accessed: 13 April 2022, https://avatarms.com/safety-risk/

4)

Selfkey Blog, A Comprehensive List of Cryptocurrency Exchange Hacks, 13 February 2020, Accessed: 13 April 2020, https://selfkey.org/list-of-cryptocurrency-exchange-hacks/
5)

Frank Gogol, Stilt, How to Cash a Check Without an ID, 18 March 2022, Accessed: 13 April 2022, https://www.stilt.com/blog/2021/05/how-to-cash-a-check-without-an-id/#3_Ways_to_Cash_a_Check_Without_an_ID
6)

Privacy Rights Clearing House, Do I have to show my ID when I buy something with a credit card?, 15 July 2019, Accessed: 13 April 2022, https://privacyrights.org/resources/do-i-have-show-my-id-when-i-buy-something-credit-card
7)

Ryan Browne, CNBC, 19 November 2021, Accessed: 13 April 2022, https://www.cnbc.com/2021/11/19/over-10-billion-lost-to-defi-scams-and-thefts-in-2021.html