BIS

Consultative Group on Risk Management

Central bank digital currency (CBDC) information security and operational risks to central banks

An operational lifecycle risk management framework

November 2023

BIS Representative Office for the Americas

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-717-7 (online)

Contents

Foreword

Introducing a central bank digital currency (CBDC) will have far-reaching implications for the operations of the issuing central bank and the risk it faces. Both will depend mainly on the particular design adopted and on a large range of factors internal and external to the central bank. This report analyses the operating, technology, third-party and business continuity risks for the issuing central bank. It therefore provides a useful complement to other work on CBDCs, which tends to focus on their implications for financial stability, monetary policy and the wider economy.

The report proposes an integrated risk-management framework that can be applied to the entire life cycle of a CBDC, from the research and design stages to implementation and operation. It discusses the implications of many of the design choices that a central bank needs to take and suggests tools and processes to identify and mitigate the risks that a CBDC poses to the issuing institution. For CBDCs to be a reliable means of payments, central banks also need to address, among others, the risks of interruptions or disruptions and ensure integrity and confidentiality. A key risk are the potential gaps in central banks' internal capabilities and skills. While many of the CBDC-related activities could in principle be outsourced, doing so requires adequate capacity to select and supervise vendors.

The report is the outcome of the work conducted by BIS member central banks in the Americas within the Consultative Group on Risk Management (CGRM), which brings together representatives of the central banks of Brazil, Canada, Chile, Colombia, Mexico, Peru and the United States. The task force was led by Diego Ballivián from the Central Bank of Chile; subgroups were led by Antonieta Campa from the Bank of Mexico, María Jesús Orellana from the Central Bank of Chile and David Whyte from the BIS. The BIS Americas Office acted as the secretariat.

Diego Ballivián
Chair of the Task Force
Central Bank of Chile

Alexandre Tombini
Chief Representative for the Americas
Bank for International Settlements

Executive summary

A central bank digital currency (CBDC) is digital money issued by a central bank. Just like physical money, a CBDC is a means of payment denominated in the national unit of account and is a liability of the central bank in a particular jurisdiction. The number of central banks across the globe that are working on CBDCs has tripled over the last three years – to 130 as of mid-2023.

CBDCs have the potential to drive innovation, promote financial inclusion and create an environment that enables the creation of the next generation of payment applications and digital businesses. At the same time, introducing a CBDC is likely to have major implications for the operation and stability of the financial and payment systems. Decisions relating to the available design choices will affect the nature and magnitude of risks facing a central bank issuing a CBDC. Therefore, it is important that these risks are carefully identified, assessed and addressed to meet the CBDC's use case and objectives, and to tackle the inevitable trade-offs between performance, interoperability, privacy and security. In particular, it is crucial that risk management is applied throughout the lifecycle of a CBDC, from the research and design stages to implementation and operations. The risks posed by a CBDC will be tied to design choices as well as external factors. Accordingly, adopting a risk management approach throughout its lifecycle can help to reduce undesirable outcomes, including governance issues, and support a more robust decision-making process for CBDC.

To explore the risks related to the introduction of a CBDC, the Consultative Group on Risk Management (CGRM) of central banks in the Americas set up a task force to explore the operational and information security risks related to the issuance of CBDCs – the CBDC Task Force. The Task Force addressed the topic from a broader, integrated risk management perspective.

Starting from the analysis of design choices and the factors affecting them, this report provides an integrated risk management framework that allows central banks to assess a variety of risk categories. This includes the operational and cyber security risks associated with CBDCs, but the complexity of CBDCs and the importance of their operational resilience means that an operational risk (OR) assessment alone would be insufficient. Accordingly, the integrated risk management approach proposed in this paper is a useful framework to inform design choices relating to a potential CBDC, to understand and manage associated risks, and to support central banks in developing tools and processes that mitigate the risks that a CBDC poses to the issuing institution.

The key findings are as follows.

1. Issuing a CBDC will have major implications for the business model of central banks and the risks they face, and it will modify their risk profiles.

To keep these risks within the limits of the institutions' risk appetite, central banks need to set up processes to identify, assess, monitor and report risks and their potential mitigants. Since risks change, this is not a one-off action but needs to take place on a recurrent basis. Given the major implications of issuing a CBDC, this should not be considered to be a technological project but rather a fundamental change in the way that the central bank operates.

2. Taxonomies and frameworks for integrated risk management analyses are essential.

Design choices will depend on the particular objectives and use cases for a CBDC as well as on country-specific ecosystem factors. This means that the design and risks posed by a CBDC will vary across countries. The multi-faceted nature of the risks calls for an integrated risk management framework to inform the design of a CBDC model and to manage risks throughout its lifecycle.

3. Central banks need to assess all risk categories as part of an integrated risk management framework and develop associated mitigation strategies.

The integrated risk management framework provides a list of CBDC-relevant risk categories. The literature highlights four categories for OR – operating, technology, third-party and business continuity risks. However, central banks should go beyond these categories and perform their own risk mapping exercises to identify additional risks. Mitigation strategies can be based on a wider variety of risk models, including information and communication technology (ICT) risk management (incorporating cyber security), project risk, and compliance risk management.

4. Central banks should evaluate potential gaps in their own internal capabilities and skills.

Potential gaps in the skills and capabilities needed at different stages of implementing a CBDC can be a key risk. Central banks should perform careful and realistic assessments about this, including with respect to their ability to develop the required skills internally. These assessments will help to determine whether CBDC-related activities could be performed internally or would, potentially, need to be outsourced to third parties. Therefore, the evaluation should also assess the risks of outsourcing (eg technology lock-in or vendor risks). Supervision capabilities should also be in place to ensure appropriate due diligence for CBDC processes.

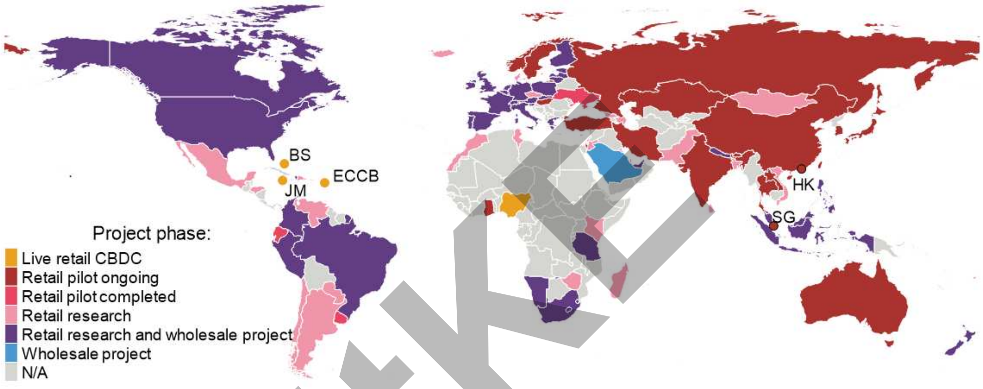
5. Operational and cyber security resilience is crucial.

For CBDCs to be a reliable means of payment, central banks should address the risks of interruptions or disruptions and ensure integrity and confidentiality. This requires the development of robust business continuity plans to ensure the reliability and continuity of services based on possible scenarios and threats, throughout the full (digital) currency cycle. CBDCs using novel technologies such as distributed ledger technology (DLT) will face unique cyber risks, as there is no widely accepted cyber security framework for DLT. Furthermore, there are limited real world data pertaining to threats to CBDCs, regardless of the type of technology they use. Accordingly, managing risks associated with CBDC issuance may require adapting existing cyber security assessment methodologies and frameworks to this unfamiliar landscape.

Introduction

The number of central banks exploring, developing or operating central bank digital currencies (CBDCs) has grown rapidly in recent years. In mid-2023, 130 countries, representing over 98% of global GDP, were undertaking work on CBDCs, up from only 35 in May 2020 (Graph 1).[1] This includes four live retail CBDCs – operated by the Central Bank of The Bahamas, the Eastern Caribbean Central Bank, the Central Bank of Nigeria and the Bank of Jamaica.[2]

CBDC research and pilots around the world Graph 1



BS = The Bahamas; ECCB = Eastern Caribbean Central Bank; HK = Hong Kong SAR; JM = Jamaica; SG = Singapore.

The designations used and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the BIS concerning the legal status of any country, area or territory or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Source: Auer, R, G Cornelli and J Frost (2023), "Rise of the Central Bank Digital Currencies", *International Journal of Central Banking*, forthcoming. Data updated July 2023.

The introduction of CBDCs will have major implications for the operation and stability of the financial system, and for the conduct of monetary policy and payment systems.[3] It could also create a variety of risks to the issuing central bank itself. The nature and importance of these risks depends on the precise design of the CBDC, the participation of third parties and the ecosystem in which the CBDC will operate.[4]

To explore these risks, the Consultative Group on Risk Management (CGRM) of central banks in the Americas set up a task force of risk management specialists to study operational and information security risks related to the issuance of CBDCs –ie, the CBDC Task Force. The Task Force did not address the financial stability risks of CBDCs or their impact on monetary policy operations or payment systems – these

[1] See www.atlanticcouncil.org/cbdctracker/. Last consulted in July 2023.

[2] Auer et al (2023). Data update as of July 2023.

[3] BIS, Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England and Board of Governors Federal Reserve System (2021).

[4] Bilotta and Botti (2021).

have been considered in a variety of international forums. Its remit also excluded direct financial risks. To the extent possible, the Task Force drew on existing work to avoid duplicating areas already covered in other forums. The work of the Task Force included literature reviews, internal discussions and meetings with private sector participants to identify risks to CBDC projects and initiatives. The Task Force was headed by Diego Ballivián, Chief Risk Officer at the Central Bank of Chile. Sub-groups were led by Antonieta Campa, Manager of Risk Strategy and the Project Management Division at the Bank of Mexico; María Jesús Orellana, Operational Risk Manager at the Central Bank of Chile; and David Whyte, Head of the Cyber Resilience Coordination Centre at the Bank for International Settlements. See the Annex for a complete list of members.

The aim of this report is to provide central banks with an integrated framework that allows them to assess the operational and cyber security risks associated with CBDCs. This could inform design choices relating to a potential CBDC and help central banks develop tools and processes that minimise the risks posed to issuing institutions.

The report is structured as follows. Section 1 provides background information on CBDCs, with an emphasis on the main design choices. This is important because different design choices could have significant implications for the risks faced by central banks. Section 2 provides a framework to perform an integrated risk management assessment (IRM) of CBDCs. Having an IRM is crucial since the complexity of CBDCs and the importance of their operational resilience means an operational risk (OR) assessment would be insufficient to deal with their risks. Section 3 tackles the key cyber security aspects of CBDCs, including the cyber threat landscape and associated risks, and offers insights about their prioritisation. Section 4 explores other important risks.

The four sections contribute to generating a comprehensive, panoramic view of why a CBDC may have a relevant impact on the central bank's risk profile, and therefore why issuing a CBDC should not be conceived solely as a technological project but as a fundamental change to the way in which the central bank operates. It is thus important to use taxonomies and frameworks for integrated risk management analyses. This will facilitate the identification and assessment of the external and internal factors involved in CBDC projects, although these may differ across jurisdictions. The approach outlined in this report will allow risks to be identified in a timely manner so that they can be managed effectively, including by the deployment of strategies for mitigating such risks.

1. Design choices

A retail CBDC can be seen as a sort of digital banknote that can be used by individuals and businesses (including merchants) to pay each other. A wholesale CBDC is restricted to use by financial institutions to settle trades in financial markets. In either case, it would have the full backing of the central bank. [5]

[5] CPMI-MC (2018).

The fact that CBDCs are a claim on the central bank clearly differentiates them from existing forms of cashless payment instruments for consumers, such as credit transfers, direct debits, card payments and e-money, which are liabilities of the issuing institution. They are also different from other types of digital money in the form of cryptoassets, stablecoins and other digital assets.[6]

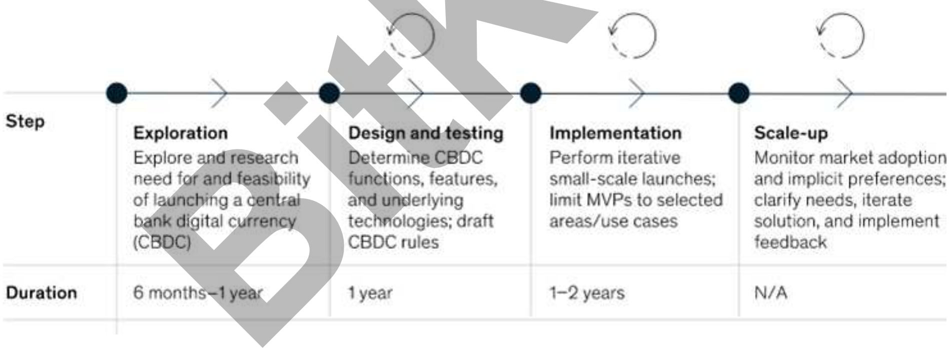
Considerations for selecting a particular CBDC model

While the reasons for issuing CBDCs and the risks they pose to the financial system are outside the scope of the Task Force's work – and hence this report – it is important to recognise that the various design choices will affect the risks posed to the central bank issuing that CBDC.

Introducing a CBDC involves significant preparatory and development work that can take several years.[7] As with any large-scale project, careful project management at the design, development, implementation and operating phases (see Graph 2) is essential to achieve project objectives on time, and to minimise scope creep. Graph 2 shows a possible route, along with development stages for a CBDC project, although timelines and procedures will vary in practice.

Development Stages for a CBDC Project

Graph 2



Step	**Exploration** Explore and research need for and feasibility of launching a central bank digital currency (CBDC)	**Design and testing** Determine CBDC functions, features, and underlying technologies; draft CBDC rules	**Implementation** Perform iterative small-scale launches; limit MVPs to selected areas/use cases	**Scale-up** Monitor market adoption and implicit preferences; clarify needs, iterate solution, and implement feedback
Duration	6 months–1 year	1 year	1–2 years	N/A

Source: Denecker et al (2022).

To successfully implement a CBDC, central banks must consider the objectives and use case for a CBDC (ie its core factors), engage with a wide range of internal and external stakeholders, and include a number of considerations of difference factors relating to a CBDC project. These considerations are visualised in Graph 3 and will be detailed in the following sections.

[6] Boar and Wehrli (2021).

[7] Several central banks have highlighted the importance of preparatory work for CBDC. See Auer, Frost, Gambacorta, Monnet, Rice and Shin (2021).

Core factors

1. Objective(s) for a CBDC. Countries may have a range of objectives for issuing CBDCs, including:[8]

- Increasing financial inclusion, or more generally, broadening access to the financial system to serve the unbanked and under-banked population.
- Extending public access to safe central bank money (as opposed to private digital currencies).
- Safely meeting future needs and demands for payment services, including ensuring competition, data privacy and the integrity of the payment system.
- Reducing costs and improving access to domestic and cross-border payments.[9]
- Contingency planning in case cash use suddenly declines or a private digital currency is widely adopted.
- Countering tax evasion and criminal uses of currency.
- Avoiding currency substitution and preparing for potential competition from other CBDCs.
- Creating a payment foundation to better support innovation (eg smart contracts, internet of things etc).
- Facilitating the distribution of central bank money and government benefits, particularly in remote areas.

Each jurisdiction will have its own objectives, which may differ from those of other jurisdictions. For example, promoting financial inclusion is an objective cited by more than 50% of emerging market economies (EMEs). This could be combined with the objective of developing payment systems cited by the central bank of Peru, or with the objective of increasing competition in payment systems cited by the central bank of Colombia.[10] This report does not assess CBDC objectives.

The implementation of a CBDC in a particular ecosystem may entail specific design choices and, therefore, risks. Accordingly, it is important to keep in mind the objective and use cases for CBDC when conducting risk assessments for all categories (see Section 2, Table 2) discussed in this document.

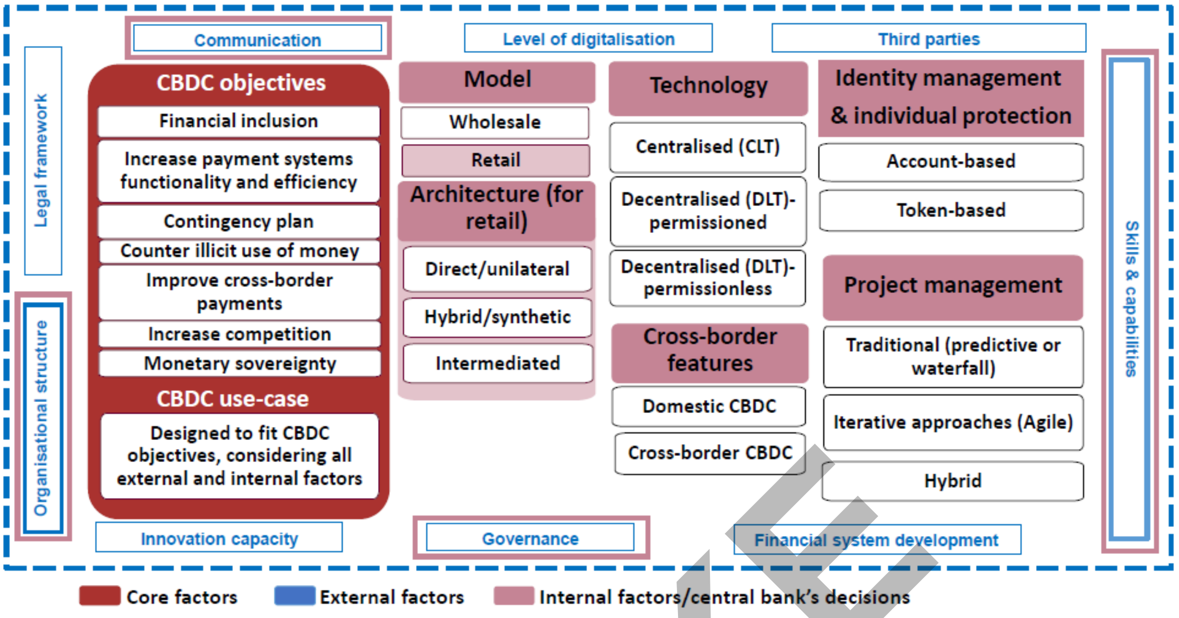
[8] Bank of Canada et al (2020) and Appendino et al (2023).

[9] Cross-border payments currently face challenges in terms of fees, accessibility and speed.

[10] BIS (2022).

Considerations for a CBDC project/model choice Graph 3

There is no "one model fits all" for CBDC projects. Different factors influence CBDC project design and implementation. These include the legal framework, the state of development of the financial system, relevant stakeholders, and skills and capabilities of the central bank.



Sources: CBDC Task Force.

2. Use case for a CBDC. This is closely related to the objectives for introducing a CBDC and defines the decision to adopt. The associated design choices depend on external factors within the country such as the degree of financial literacy and inclusion, user characteristics (trust, knowledge etc), the availability of technological infrastructure and the level of digitalisation. This means that even when two central banks share the same objective, the decision about whether to adopt a CBDC or how to design it may vary considerably. For example, while two central banks might have "financial inclusion" as an objective for a CBDC project, their use cases could be very different – one may have digital infrastructure covering 45% of the population and another more than 85%. For some central banks, decisions may be reliant on securing technological coverage in remote areas, while another central bank's choices might be influenced by financial literacy and cultural factors.

External factors

External factors play a key role in shaping the scope and design of CBDC projects and may also impact strategy and project governance decisions. These vary by jurisdiction. Therefore, it is useful for central banks to identify those factors and dependencies that could affect the success of the project, in order to ensure that they are considered in the scoping and design stages of CBDC projects.[11] As an important step in risk management assessment and strategy, robust analysis should be undertaken by

[11] External dependencies mean that central banks which issue a CBDC must be able to license and operate any third-party technology that enables the operation of a CBDC.

central banks to provide a clear understanding of these factors.[12] Examples of external factors (ecosystem features) are listed in item 3 below.

3. Ecosystem features. These reflect the current financial, technological and legal environment in which the central bank operates. Relevant factors include the:

- **Legal framework** – the law governing financial services, payments and sovereign currency.[13]
- **Level of digitalisation** – the level of technological preparedness of the population and the availability of technological infrastructure.[14] This could be measured, for example, by mobile telephone usage and access to broadband internet, or trends in the proportion of cash vs digital payments.
- **Level of financial development** – including the technological and risk management skills of financial institutions, financial literacy among the population, financial inclusion, degree of development of the local economy, size of the informal economy and the use of cash for payments. This could be measured, for example, by access to different types of financial services and the types of digital financial products available.
- **Innovation capacity** – a jurisdiction's track record and potential for innovation that can support the development and implementation of a CBDC, which can impact the speed of the project and its effectiveness. This could be measured, for example, through the World Intellectual Property Organization Global Innovation Index.[15]
- **Geopolitical considerations** – includes technological/digital infrastructure availability based on geographical and/or political circumstances, regional settlement agreements and prioritisation to support the issuance of a CBDC.

4. Operational skills and capabilities**.** This includes the availability of human resources in a jurisdiction to (i) support existing and new technologies required for a CBDC; and (ii) develop or integrate existing technological infrastructure for use for a CBDC. It is helpful to perform a gap assessment of a central bank's internal skills and capabilities to determine whether it can recruit or acquire resources externally; this will in turn delineate the work that should be performed internally and the work to be outsourced to third parties. This factor can be categorised as both external and internal, and will influence the CBDC project environment. It will therefore be a source

[12] Auer et al (2023).

[13] In many jurisdictions the decision to issue a CBDC and significant policy decisions on design will be the responsibility of the executive and legislative branches. In such cases, the central bank would be primarily responsible for development and implementation.

[14] Some technologies might not be available in certain regions because their implementation is not cost effective for public or private actors. This factor can drastically limit the functionality of both the online and offline alternatives.

[15] WIPO (2018).

of operational risk that should be considered as part of the decision-making about project execution and operational risks of a CBDC in a jurisdiction (see Graph 3).[16]

Decision-makers at all levels should understand that external factors can materially impact not only the delivery schedule but also the viability of the CBDC project itself. For instance, poor internet accessibility may limit take-up in rural areas. The effective implementation of a CBDC thus requires evaluating the possibility of upgrading technical infrastructure.

Internal factors

Trade-offs exist when selecting a particular type of CBDC. In addition to the external factors mentioned above, central banks should consider a variety of internal factors. There is no "one model fits all" kind of choice for CBDC designs. Accordingly, we note the following key considerations for a CBDC project with a particular focus on OR.

5. CBDC models and architectures. CBDC models can take retail or wholesale forms. A retail CBDC is a claim on the central bank that is available to all households and firms in the economy. Regardless of whether a CBDC is account or token based, there are three general models or architectures available to central banks (see Graph 4):[17]

(i) **Direct:** single-tier retail CBDC in which the central bank directly handles all payments by the public and enterprises, and keeps all records of direct retail holdings by all participants in real time.

(ii) **Hybrid:** two-tiered retail CBDC model in which intermediaries onboard clients, perform know-your-customer (KYC) checks and handle consumers' payments in real time, and the central bank periodically records retail balances.

(iii) **Intermediated:** two-tiered retail CBDC model in which the main difference with the hybrid model is that the central bank only processes and records wholesale payments and balances, whereas intermediaries handle retail payments.[18]

On the other hand, a wholesale CBDC is a direct claim on the central bank that is only available to financial institutions or a subset thereof. These institutions could hold the CBDC to back their own issuance of "CBDC-related claims" to the public.[19]

[16] The gap assessment of capabilities and skills will guide a central bank on its needs and possibilities to: (i) recruit or train employees; (ii) invest in the required technology; and (iii) design, develop and implement a CBDC within a given time frame.

[17] Hybrid and intermediated models encompass a range of possible two-tiered operational arrangements for retail CBDC. Note that two-tiered models for CBDC avoid disintermediation, thus avoiding any sudden changes to the structure of the financial system that might jeopardise financial stability. As Auer and Böhme (2020) state: "In some, the central bank hosts a database of retail balances (even if anonymised), whereas in others it keeps track only of wholesale balances."

[18] See BIS (2021). Such designs could enhance security and privacy. At the same time, they require close supervision of intermediaries to ensure at all times that the wholesale holdings they communicate to the central bank accurately reflect the sum of their clients' retail accounts.

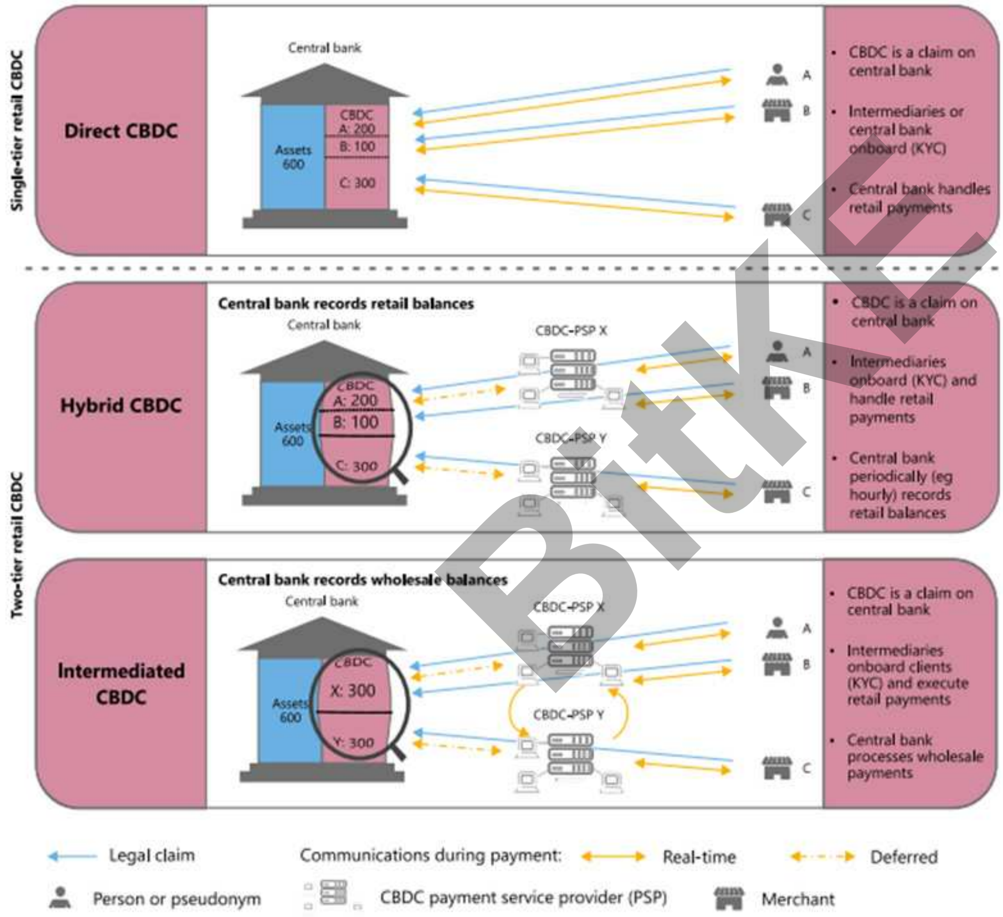
[19] This is not unlike the current reserve model for cash in which financial institutions hold cash reserves at central banks.

This could include so-called **synthetic** or **indirect** architectures. Wholesale CBDCs are intended for the settlement of interbank transfers and related wholesale transactions and could encompass digital assets or cross-border payments.

CBDCs could also provide additional automation and programmability features to enhance functionalities for central bank money such as conditional payment instructions whereby payments only settle after pre-defined conditions have been met. The central bank only operates the wholesale payment system and does not keep any record of the public's CBDC-related claims (see Table 1).[20]

Retail CBDC Architectures

Graph 4



Single-tier retail CBDC
Direct CBDC
Central bank
Assets 600
CBDC
A: 200
B: 100
C: 300
A
B
C
CBDC is a claim on central bank
Intermediaries or central bank onboard (KYC)
Central bank handles retail payments
Two-tier retail CBDC
Hybrid CBDC
Central bank records retail balances
Central bank
Assets 600
CBDC
A: 200
B: 100
C: 300
CBDC-PSP X
CBDC-PSP Y
A
B
C
CBDC is a claim on central bank
Intermediaries onboard (KYC) and handle retail payments
Central bank periodically (eg hourly) records retail balances
Intermediated CBDC
Central bank records wholesale balances
Central bank
Assets 600
CBDC
X: 300
Y: 300
CBDC-PSP X
CBDC-PSP Y
A
B
C
CBDC is a claim on central bank
Intermediaries onboard clients (KYC) and execute retail payments
Central bank processes wholesale payments
Legal claim
Communications during payment:
Real-time
Deferred
Person or pseudonym
CBDC payment service provider (PSP)
Merchant

Source: Auer and Böhme (2021).

[20] BIS (2021).

Summary of CBDC retail and wholesale architectures Table 1

Architecture name	Final audience (model)	Tiers	Onboarding, KYC of clients	Public holds claim on central bank	Real-time payment handling	Central bank balance register payments
Direct	Retail	One tier	Central bank, intermediaries	Yes	Central bank retail	Real-time retail
Hybrid	Retail	Two tiers	Intermediaries	Yes	Intermediaries retail	Periodically retail
Intermediated	Retail	Two tiers	Intermediaries	Yes	Intermediaries retail, central bank wholesale	Real-time wholesale
Indirect	Wholesale	Two tiers	Intermediaries	No – intermediary holds claim on central bank	Intermediaries retail, central bank wholesale	Real-time wholesale

Sources: CBDC Task Force

Different models and architectures for CBDC have specific implications in terms of OR for central banks, as they entail different levels of internal handling vs delegation to third parties of features such as record-keeping, security, integrity and availability.[21] Different levels of internal handling vs delegation to externals can be established for the various aspects of a CBDC, including the technological infrastructure and operating needs.

The following sections of the report will further explore OR categories for CBDCs.

6. CBDC technology. A CBDC could run on a conventional, centrally controlled database (centralised ledger technology (CLT)) or be fully or partly deployed on a system based on distributed ledger technology (DLT) in which the database is updated in a decentralised manner after different nodes have confirmed the transaction. Design options for DLT can include public and private ledgers, as well as permissioned or permissionless systems. CBDC can also use hybrid technology, in which DLT and CLT are used in different parts of the CBDC project. CLT and DLT infrastructures can and usually do store data in multiple, separate locations as a means of securing operational resilience.[22]

7. Availability (online/offline). A decision must also be made on whether a CBDC would be available to use in the absence of an internet connection. Offline transactions could ensure CBDC availability by making payments possible even if there is no connection to the internet. However, it also increases the possibility of digital counterfeiting and double spending.[23] As such, this decision needs to be assessed on the basis of preserving the confidentiality, integrity and availability (CIA)

[21] See BISIH, Hong Kong Centre, the Hong Kong Monetary Authority, and the Hong Kong Applied Science and Technology Research Institute (2022) for a graphical depiction of trade-offs between operational and supervisory burden for central banks, related to different models and architectures.

[22] See Auer and Böhme (2020) and Sultanik and Myers (2022).

[23] English (2021).

characteristics of a CBDC. Policy constraints, such as limits on transaction amounts and balances, could play a role in maintaining financial integrity and mitigating risks to the central bank.

8. Cross-border vs local features and capabilities. Cross-border payments are usually carried out through a network of correspondent banks. This tends to be inefficient given differing technologies and legal/regulatory frameworks, unaligned time zones and operating hours, and differences in technical/security standards that could contribute to critical OR. These factors may result in cross-border payments that are particularly difficult to effect in some EMEs, even though these jurisdictions may receive a large number of remittances.[24] The bulk of settlements in correspondent banking takes place for the purposes of commercial bank credit and these cross-border transactions imply credit, liquidity and settlement risks which could be reduced through cross-border CBDC arrangements.[25] Local features should be analysed, considering central bank capabilities to comply with the expected (regulatory) framework as well as operational standards for a secure cross-border CBDC.

9. Account vs token based. Account-based CBDC requires user identification for access. However, for token-based CBDC the access mechanism is via private/public keys and, while this allows for anonymity, it also implies risks related to the loss or theft of keys. Further, it could also enhance money laundering and terrorist financing risks.[26]

This decision can be used to support a number of objectives; it could be a means to reach unbanked or underbanked populations that have access to mobile telephones, or it could be a mitigation strategy to address risks related to the privacy and security of CBDC.[27]

10. Project implementation/management. Delivering a CBDC is a large-scale project that requires robust project management. Central banks have choices to make in terms of the project management methodology they will use (eg iterative approaches such as agile, or traditional/waterfall project methodologies, or a hybrid combination for different stages of the process).[28]

A multidisciplinary group of participants should be formed at the outset of the project and central banks should use this group, at all stages, to consider: [29]

[24] Bech et al (2022).

[25] BISIH et al (2022).

[26] As described in Section 4 on legal risk, legal frameworks can enhance privacy for individuals, for example, by allowing governments to access transaction information only with a court order.

[27] BIS (2022).

[28] See Section 4 on project management for a further description of these project management methodologies.

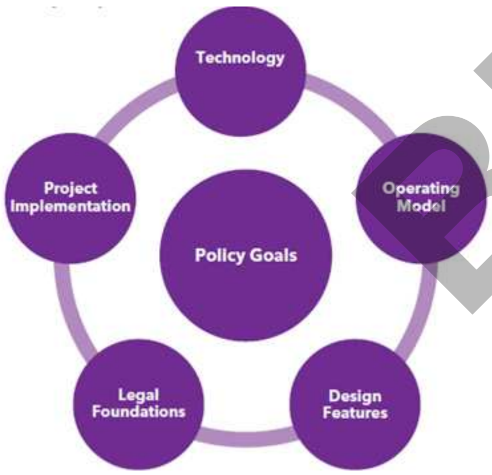
[29] The list provided is non-exhaustive and non-prescriptive. It was compiled by the CBDC Task Force through discussions in work sessions and is aligned with change management methodologies (involving in this case, both central bank internal operations and various external stakeholders and players in the new CBDC payment ecosystem). A discussion on the integration of change management and project management is provided by Parker et al (2013).

- The identification of relevant risks considering strategic, operational and legal risks (including enterprise and governance risks).
- Timely follow-up on strategic and operational challenges of the project at the appropriate level (eg strategic challenges by the board and operational aspects and risks by senior management).
- Communications strategies and partnerships, including involving the public and third parties (eg commercial banks and key government agencies).
- Continuous testing – including user experience testing – updated as new technologies are available, new conditions evolve and user feedback is received.
- Ongoing gap remediation through the identification of lessons learned and maintaining a registry of risks discovered, solved or reappearing.

As indicated in Graph 5, there are crucial choices and considerations for a CBDC that need to be managed. These include the operating model and its functions, design features, legal foundations and project implementation.[30] In this section, we have described a number of external and internal factors and provided a proposed basic taxonomy for central banks that can be considered when making design-related decisions for CBDC projects (see Graph 6).

Choices and considerations for CBDC

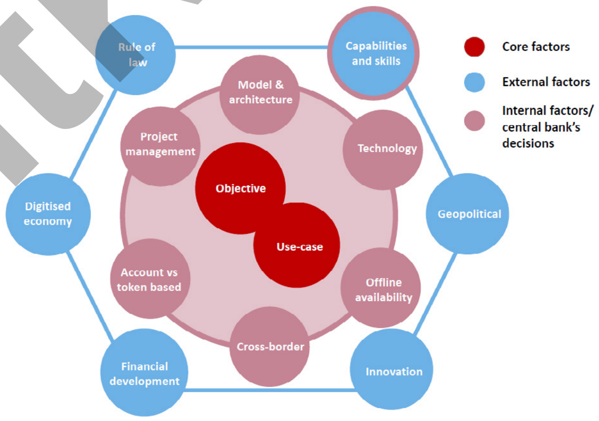
Graph 5



Source: Soderberg et al (2022)

Proposed taxonomy of design-related decisions for a CBDC

Graph 6



Source: CBDC Task Force.

Decisions made at the planning stage will influence the risks that central banks face during the development and deployment of a digital currency. This is extremely important as "the foundation of the monetary system is trust in the currency. As the central bank provides the ultimate unit of account, that trust is grounded on

[30] Soderberg et al (2022).

confidence in the central bank itself".[31] Any risk arising from the implementation and operation of a CBDC can have a reputational impact on the central bank.[32] To mitigate reputational impacts stemming from the materialisation of risks in a CBDC, central banks need to carefully gather the information to make necessary assessments. This includes the use of transversal and multidisciplinary teams from the very beginning of the evaluation phase as well as clear communication with senior management about available options, the implications of individual choices and the degree of their alignment with the risk appetite of the central bank. The following section will provide a methodological approach to evaluating key dimensions of OR for CBDC.

2. Operational risks of CBDCs – categorisation and analysis

The introduction of a CBDC exposes central banks to operational risks that need to be identified, analysed and managed.[33] Furthermore, it will change processes, technologies and external vendor relationships. Even central banks with robust risk management processes and a strong operational control environment for their regular activities may need to adapt policies and procedures, and procure additional staffing and other resources, in light of these new central bank operations. This will need to occur across the first, second and third lines of defence.

This section discusses some of the operational risks associated with the implementation of a CBDC.[34] To establish effective and efficient operational risk management (ORM), a set of principles is crucial for managing risks in CBDC.[35] An important step is the establishment of an **integrated risk management (IRM) framework**, that includes operational risks as well as other risk categories which might have a reputational impact on central banks (as described in Table 2).

The organisation must define a variety of matters related to the CBDC project. These include significant processes and activities, the people involved and their functions, systems utilised and external service providers. Furthermore, all decisions related to a CBDC require integrated governance. This IRM framework should contemplate the "operational risk management process" for design, testing, user acceptance, implementation, monitoring and maintenance. It should also include the

[31] BIS (2021).

[32] All risks in any category (as mentioned in Table 2 with respect to OR) might have reputational impacts and thus, depending on the results of specific assessments and circumstances, could become strategic risks for a central bank. The assessment of particular strategic risks is out of scope for this document although we acknowledge that CBDC could be a strategic risk for central banks.

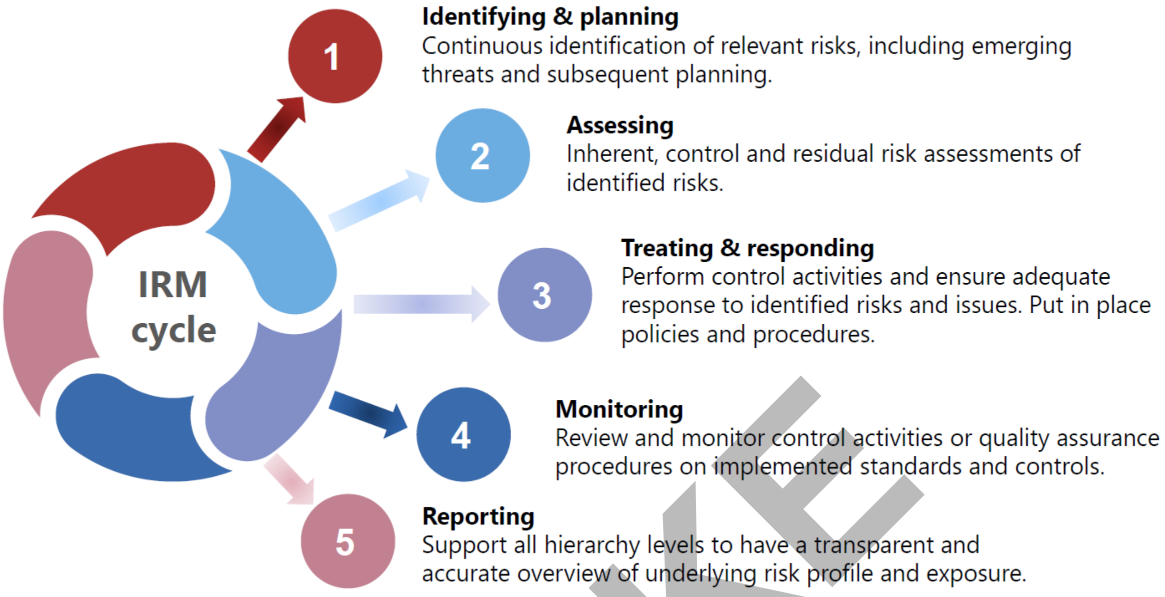
[33] ORM contributes directly to the effective management of central bank processes and activities, allowing for each institution to define its risk profile and adopt best practices and principles that, in a clear manner, establish the internal governance and mechanisms they should define and implement to mitigate operational risk. In the Basel III framework, operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (BCBS (2017)).

[34] FSI (2015).

[35] BCBS (2021b).

systematic use of measures to identify, assess, treat, monitor and report CBDC-related operational risk (see Graph 7).[36]

IRM lifecycle Graph 7



Identifying & planning
Continuous identification of relevant risks, including emerging threats and subsequent planning.

Assessing
Inherent, control and residual risk assessments of identified risks.

Treating & responding
Perform control activities and ensure adequate response to identified risks and issues. Put in place policies and procedures.

Monitoring
Review and monitor control activities or quality assurance procedures on implemented standards and controls.

Reporting
Support all hierarchy levels to have a transparent and accurate overview of underlying risk profile and exposure.

Source: CBDC Task Force.

Defining a risk profile before adopting a CBDC

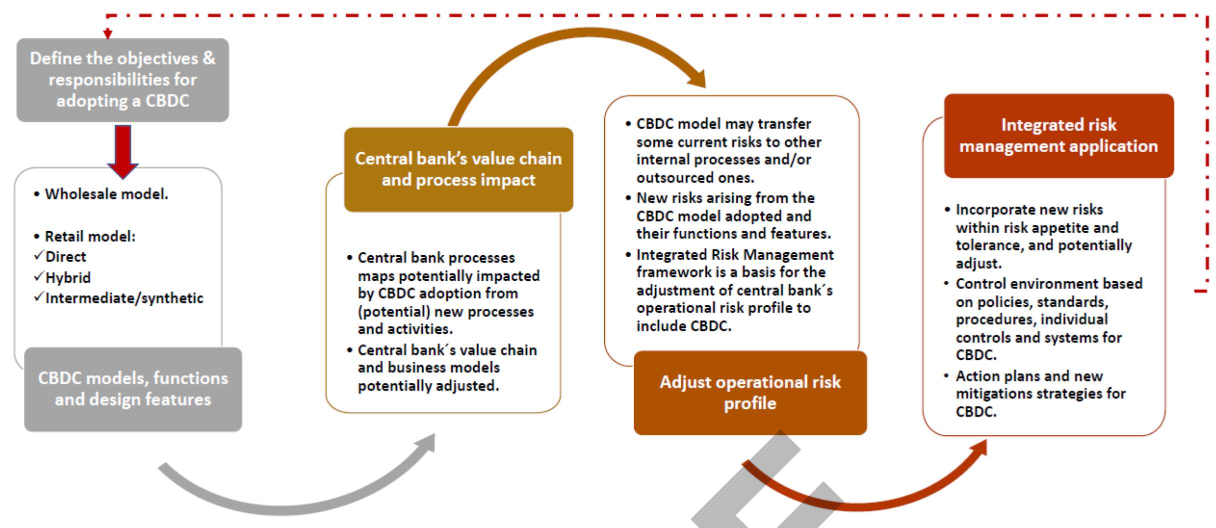
IRM begins a long time before the issuance of a CBDC, with an assessment of the business impact of different design options, the current risk profile, staffing levels and expertise, as well as existing and proposed processes.

[36] Soderberg et al (2022).

Integrated risk management cycle for adjusting risk profile when adopting a CBDC

Graph 8

Operational Risk Management establishes a control environment for CBDC



Define the objectives & responsibilities for adopting a CBDC

- Wholesale model.
- Retail model:
  - ✓Direct
  - ✓Hybrid
  - ✓Intermediate/synthetic

CBDC models, functions and design features

Central bank's value chain and process impact

- Central bank processes maps potentially impacted by CBDC adoption from (potential) new processes and activities.
- Central bank´s value chain and business models potentially adjusted.

- CBDC model may transfer some current risks to other internal processes and/or outsourced ones.
- New risks arising from the CBDC model adopted and their functions and features.
- Integrated Risk Management framework is a basis for the adjustment of central bank´s operational risk profile to include CBDC.

Adjust operational risk profile

Integrated risk management application

- Incorporate new risks within risk appetite and tolerance, and potentially adjust.
- Control environment based on policies, standards, procedures, individual controls and systems for CBDC.
- Action plans and new mitigations strategies for CBDC.

Source: CBDC Task Force.

Risk appetite and tolerance levels guide the CBDC risk profile

As a second step, a central bank should define key areas of operational performance, new risks, resilience objectives and metrics. It should also define thresholds beyond which the risk profile exceeds risk appetite. These may relate to business continuity, technology change management and information security, among others.[37] Additionally, processes and their related controls should be designed to achieve the expected risk profile and resilience objectives.

Once the appetite for different types of risk is defined, whenever the risk profile exceeds the defined thresholds there are essentially four ways to bring identified risks in line with risk appetite: avoid/resolve, mitigate, transfer or accept the risk. A decision in favour of one of the four options depends on the business model of each central bank because each decision may increase other key risks and should, accordingly, be aligned with the defined risk appetite.

[37] Information and communication technology (ICT) risk management incorporates cyber security risks as part of the framework, according to BCBS (2021a). This aims to manage all risks and impacts on information, technology and systems, which need to have a clear integrated control environment. Besides, the residual risk might be aligned with the risk appetite for information, depending on its levels of confidentiality, integrity and availability.

Categorising risks

As mentioned above, CBDCs may pose complex risks to central banks. To effectively manage operational risk and provide robust information to the board of directors and senior management, central banks may consider applying an **IRM cycle,** covering the most important risk categories relevant for CBDCs, that need to be analysed and managed in an integrated manner.

Table 2 shows proposed risk categories within the scope of an IRM related to CBDCs.[38] This table emphasises both risk categories and sources of risk, and the classification is: processes, people, systems and external events. These classifications allow for "root cause analysis" to be undertaken for any OR. All of these categories may potentially have reputational, financial and other impacts, depending on their environment, scope and the choices made relating to CBDC implementation.

Risk categories proposed for an integrated risk management framework

Table 2

Risk categories	Causes/sources				Risk descriptions (examples)	Example in CBDC context
	Processes	People	Systems	External event		
Operating or process-related	x	x	x	x	• Failures of processes or controls. • Inadequate processes or control design, implementation or ongoing management. • Lack of training or awareness. • Deviations or errors in transactional processes/ procedures. • Limited capacity (resources).	• Inability to produce accurate, timely and complete CBDC reports required to track issuance, distribution, account balance and reporting (audit and compliance).
Technology	x	x	x	x	• Technological failures. • Performance issues or capacity problems. • Incorrect implementation or maintenance. • Deviation from applicable standards. • Inadequate selection of technology. • Technology uncertainty. • No availability.	• Poor agility – risk of not being able to effectively and/or efficiently adapt the CBDC product offering to evolving to changes and needs. • Poor interoperability. • Poor integration.
Third party	x	x	x	x	• Failures in the due diligence process. • Operational risk related to third parties. • Exit strategy risk. • Financial ecosystem risk. • Facility risk.	• Poor selection of third parties and poor ongoing oversight and monitoring.
Business continuity	x	x	x	x	• Interruption/disruption. • Natural disasters or accidents. • Social disruption and biological threats. • Crime and terrorism. • Protection/recovery failures. • Crisis management.	• Unavailability of payment systems and/or technological integration with CBDC.

[38] This categorisation of risks for an IRM assessment can also be used for any other processes and projects.

Information & communication technology (ICT)	x	x	x	x	• Confidentiality, integrity and availability risks. • Information or data leakage. • Data corruption or inadequate treatment. • Cyber risk and threats. • Unauthorised disclosure of information/data. • Damage or theft of tech/non-tech assets which support critical information. • Failures of access control to information/data.	• Violations on CBDC-related data integrity, privacy, or availability. • Cyber-attacks on CBDC infrastructure.
Legal	x	x	x	x	• Faults or demands due to non-compliance with laws or policies. • Breach of contractual obligations. • Weak contracts.	• Disputes about intellectual property. • Disputes about CBDC holdings.
Compliance (regulatory) ethics & conduct	x	x		x	• Non–compliance with relevant external and internal rules. • Conduct and ethics risks. • Fraud and money laundering. • Corrupt practices. • Conflicts of interest. • Terrorism financing.	• Privacy (of end user data).
Enterprise	x	x		x	• Inadequate decision-making processes. • Duplication of functions and roles, or gaps. • Lack of commitment by senior management. • Unclear roles and responsibilities.	• Unclear communications internally within the central bank, to end users, to the general public and to stakeholders creating confusion about the CBDC product. • Unclear CBDC policy and value proposition. • Insufficient resources/expertise (ability to attract and retain experts in many fields).
Model	x	x	x		• Inadequate methodology, underlying assumptions or adoption of a standard model. • Inadequate inputs or model performance leads to adverse outcomes for decision-making or public disclosures.	• Inadequate adoption of security standards for hybrid DLT-CLT.
Environmental, social and governance (ESG)[39]	x	x	x	x	• Climate risks. • Health and safety issues. • Inappropriate working conditions. • Inappropriate board governance. • Inconsistency in the implementation of sustainability policies.	• Governance: unclear or absent independent supervision/ regulation/oversight of the CBDC payment product. • Social: CBDC product may fail to ensure inclusiveness/universal access.

Mapping CBDC risks

The remainder of this section discusses a range of risks associated with the adoption and operation of a CBDC. It is based on a systematic literature review undertaken by the Task Force. The Task Force did not assess the likelihood and impact of individual

[39] ESG risks are incorporated as a category for integrated risk management as CBDC projects will have a wider impact on their ecosystem, financial system (external risks) and on their organisations (internal risks). All aspects of their environmental, social and governance contexts should be considered.

risk factors, as these are likely to differ significantly across countries, depending on the external and internal factors discussed above.

To describe the main risks in a comprehensive manner, they are organised in the categories laid out in Table 3. The following analysis focuses on four key operational risk categories for CBDC projects that must be managed: operating (ie process-related), technology, third party and business continuity. In Section 3 we pay particular attention to a subset of ICT risks by describing cyber risks and threats in detail. This includes an overview of the cyber threat landscape as well as risks relevant to a CBDC implementation. Finally, in Section 4 we describe the remaining risk categories.

2.1. Operating risks

The level of operating (process-related) risk varies according to the CBDC model, design features and technologies defined or to be implemented by the central bank. Information Technology (IT) adoption and related security standards could imply significant changes to operational processes, which may increase risks and costs.[40]

The following table states some key operating risks identified in the literature on CBDCs, including the experiences of central banks during pilots and projects.

Some identified risks from central bank pilots and the CBDC literature

Table 3

Category	Identified risk	Causes/sources				Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
		Processes	People	Systems	External event			
Operating (process based)	Weak approach on acquiring, in a timely manner, internal capabilities and technical skills for new technologies.	x	x			Implementing immature/new/cutting-edge technologies such as DLT requires a high degree of expertise and could result in technical issues. Necessary to operate and maintain new technological activities under emerging standards and to expected service levels.	• Failures in processes and procedures. • Loss of reputation due to deficient operations. • Loss of efficiency. • Cost increases. • Information and technology security risks. • Difficulty in maintaining/evolving CBDC technology.	Technology, Third party, ICT/cyber
	Improper evaluation of internal capabilities and capacity for adopting a CBDC.	x	x	x	x	The real-time nature of CBDC will require adequately skilled resources and quick decision-making structures to respond in a timely manner and address urgent issues.	• Failures and quality loss of traditional (technological) activities and their security standards. • Negative impact on internal operational and maintenance planning. • Negative impact on resources allocated and daily activities. • Underestimation of complexity in key operational activities (payment systems/services).	Technology, Business continuity

[40] BIS (2022).

	Errors in operations and maintenance.	x	x	x	x	CBDC requires precise actions and infrastructure maintenance performance to ensure real-time operations and the expected results for all parties involved in the system. Any mistakes or lack of accuracy in operations could directly affect the whole system, security and services users.	• Technology risks associated with issuance process. • Serious impact on credibility. • Data exposure and its integrity. • Vulnerabilities/breaches of security. • Security exposure due to lack of knowledge of operating activities and resource planning.	Technology, Business continuity
	Rise in costs and burden (direct CBDC).	x		x		Insufficient involvement of private sector in operational architecture	• Increased costs for CBDC implementation and maintenance. • Overburden central banks operationally as a result of insufficient involvement of the private sector in the operational architecture. • Direct CBDC transfers of operational risks and costs from the private to the public sector.	
	Scalability challenges.	x	x	x		The design of a CBDC does not meet scalability needs, endangering the operational capacity of the system.	• Possible bank runs and high reputational costs, impacting the financial system directly, including customers and intermediaries.	Technology, Operating
	Errors in establishing thresholds, usability and capability features of the CBDC.	x	x	x		Errors and failures in defining features and components of a CBDC model vs how internal capabilities could operate and manage risk in an adequate manner.	• Inadequate security and performance standards. • Inadequate evaluation of capabilities to define and manage new features of the CBDC, impacting eg data security. • Inadequately established thresholds could cause prolonged processing times by impacting services and operations, account balances and systems capacity.	Technology, Legal

Sources: CBDC Task Force

CBDC adoption requires updated internal capabilities and skills. Gaps in skills and capabilities can introduce new broad risks to central banks that may impact processes and their outcomes, as well as systems and security standards, throughout the CBDC project, including its operations. If these gaps are not identified and treated promptly, there may be a direct impact on the success of the CBDC. During many CBDC research projects and pilots, gaps in IT (and security) capabilities were found to have been left unaddressed.[41] Acquiring new technologies for CBDC, such as DLT, could create operating risks with serious impacts on traditional payment and associated systems due to low internal capacity and skills.[42]

Operating risks of CBDCs often appear to be linked to IT risks that also impact ICT and cyber security. This is relevant for defining the correct risk evaluations and mitigation strategies – ensuring that IRM methods are utilised in CBDC operations. Unaddressed IT gaps which lead to system disruptions or failures could create major

[41] Auer et al (2020).

[42] Bank of England (2017).

risks for the credibility of CBDCs and central banks themselves. Skills and capabilities mapping is therefore crucial to successful CBDC implementation.

Mitigants

A number of operating risks for CBDC stem from human error, inadequate definitions or incomplete planning. A mitigant for these risks is ensuring that skills and capabilities available to the central bank meet the needs of CBDC. This aspect does not necessarily have to be handled internally by central banks: relying on third parties to acquire knowledge may be an option. At the same time, central banks could establish strategies for the development of internal **skills and capabilities** to reduce gaps.

Specific architecture models can contribute to the mitigation of operating risks. One option is a **two-tier architecture** in which private sector participants such as banks and non-banks (ie payment system providers (PSPs)) can manage end user services and thus reduce central bank costs and distribute risks.[43] This model can increase innovation in payment systems and can enhance CBDC usability on devices (eg prepaid CBDC, offline cards, smartphone wallets in standalone format or integrated with bank or big tech apps).[44] Similarly, to reduce the significant data management requirements for recording retail balances, an **intermediated architecture** can be used.[45]

However, regardless of the CBDC architecture that is implemented, operating risk may, in any case, change with respect to the previous risk assessment. Thus, central banks should aim to create a suitable control environment, the nature of which might depend on the central bank's risk appetite. Well-defined CBDC processes, systems maps and procedures aligned with the central bank's policies and standards should establish a clear control environment over key operating activities. This should contribute to the resilience of central banks and CBDCs.[46]

2.2. Technology risks related to CBDC

We have identified several technology risks that are worthy of further consideration: scalability, technological failure, maintenance issues, interoperability and integration issues.

Several central banks have found that technological constraints can present key operational IT risks. For example, the People's Bank of China (PBoC) found that the initial data storage requirements for its DLT pilot were much higher than had been expected.[47] Therefore, issues such as data privacy and service availability must be

[43] BIS (2022).

[44] Auer et al (2022).

[45] Auer and Böhme (2021).

[46] BCBS (2021b).

[47] Soderberg et al (2022).

carefully considered and addressed. These issues mainly impact large economies with a high flow of transactions.[48]

Problems with DLT scalability has emerged as a possible key risk in terms of the availability of CBDC, as identified in several CBDC pilots.[49] Hence, these technological limitations should be considered upon the initiation of any CBDC project. By doing so, central banks might experience fewer issues over the lifecycle of a specific technology.[50]

Meanwhile, technological failure may occur either at the hardware, software, network or consensus layers. At the hardware layer, storage could become corrupted, making it difficult or impossible to recover user balances. A failure of the software layer could, for example, be due to a bug in the implementation that induces errors in payments or user balance tracking. At the network level, disconnections or denial of service (DDOS) attacks (see Section 3) may result in **double spending** (see Section 4 on compliance risks) or create delays in transaction settlement. Potential impacts include economic losses and reputational harm. Further, **incorrect implementation, operation or maintenance of the CBDC platform** could lead to similar risks.

Finally, the incompatibility of technological standards applied on different CBDC platforms might hamper cross-border CBDC operations. For example, this may lead to frictions in international payments and may also affect compliance and AML/KYC initiatives (see Section 4).

[48] Sarmiento, A (2022).

[49] Bank of Canada et al (2020).

[50] Soderberg et al (2022).

Table 4 shows some IT risk descriptions and impacts, as discussed above.

Relevant technology risks (non-exhaustive list)

Table 4

Category	Identified risk	Causes/sources				Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
		Processes	People	Systems	External event			
Technology risk	Technology failures.	x	x	x	x	Failures at the hardware, software, network or consensus layers may affect the operation and availability of the CBDC, leading to legal and reputational impacts for central banks.	• Loss of reputation. • Economic losses. • Legal disputes. • Potential for fraud.	Operating, Business continuity, Legal, ICT/cyber, Financial, Compliance, Financial compliance
	Implementation, operation or maintenance mistakes.	x	x	x	x	May lead to incorrect balances or missed payments.	• Loss of reputation. • Economic losses. • Potential for fraud. • Missed payments.	
	Incompatibility across CBDCs.	x	x			Fragmentation of different CBDC platforms into different standards. The incompatibility of different standards may make cross-border payments and international trade more difficult as well as impeding interoperability with other financial infrastructures.	• Economic losses. • Friction in international payments. • Potential for fraud.	Model, Compliance, Financial,
	Problems integrating CBDC with other payment technology.	x	x	x	x	Inability to integrate CBDC with other payment technologies.	• Lack of adoption.	Operating, ICT/cyber

Source: CBDC Task Force.

IT mitigants

There is no single way to mitigate IT risk. Much depends on the IT model of the CBDC and on the ecosystem of the central bank, particularly with regard to internal/external capabilities.

In terms of CBDC models, some countries have ruled out the adoption of a direct model or single tier retail CBDC due to the IT risk concentration for central banks, and the associated high level of internal capabilities needed to ensure maintenance and operational continuity. Two-tiered models can thus be considered a mitigant for IT risk concentration. In the same way, central banks might contemplate outsourcing some IT processes where internal IT capabilities are not currently in place. This can take place while mitigating risks by continuing to develop and implement the internal knowledge that would eventually allow them to enhance risk management and controls for outsourced IT processes.

In terms of technology for CBDC, central banks could evaluate the use of different technologies as a mitigation strategy. This may involve the adoption of a single technology throughout the process or a combination of different technologies at various stages of the process (hybrid technology model). Requirements may evolve over time according to developments and the needs of particular CBDC ecosystems. The possibility of considering varying uses and combinations of technologies across time is aligned with a "long-term evaluation system" approach, in which different technologies are part of the same system, complementing the process workstream and its evolution.[51] Moreover, the use of an additional layer to enhance data security could serve as a mitigant, and it could help to deal with data risks related to particular technology choices.[52]

2.3. Third-party risk management associated with CBDCs

Third-party types and roles

In the CBDC ecosystem, third parties are participants outside the central bank. They include commercial banks, payment service providers, other government entities and technology companies, among others. Technology companies include system operators, traditional database and blockchain vendors, hardware and software providers, and expert developers. The implementation of CBDCs could become more complex when they involve the use of technologies or operating instances that were not previously part of the central bank's processes, potentially involving increased reliance on payment service providers and technology companies.

Third parties can perform a variety of roles in CBDCs, such as system management, account management and payment services.[53] In terms of CBDC system management, third parties may act as CBDC distributors and provide gateway access to connect end users to the CBDC system. They may also process and validate transactions. CBDC account management includes creating end user accounts, processing transactions, and maintaining account balances and transaction records. CBDC-based payment services refer to customer-facing services such as user interfaces, payment gateways and merchant services.

Third-party risk types

Guidance on third-party risk management is available.[54] The Task Force highlights the following third-party risks in the CBDC context:

[51] See Soderberg et al (2022). For example, pilots conducted by the People's Bank of China concluded that the capacity of DLT technology to process transactions and store data does not meet its requirements in respect of time periods in which there is greater demand (more transactions), such as during particular holidays. However, intermediaries can base their activities on any technology and still function in the e-CNY ecosystem.

[52] Auer et al (2022). An ICT risk management framework that pays sufficient attention to cyber security (see Section 3) could also address several operational, technological and security issues that emerge from IT infrastructure, hardware and software.

[53] AWS (2021) and Oliver Wyman and AWS (2022).

[54] BCBS (2005) and The Office of Comptroller of the Currency (OCC). (2021).

- **Operational risk** may arise if third parties face technology failures, cyber attacks, fraud, error, business disruptions or dependencies on a fourth party (ie a subcontractor of a third party). In addition, a third party and a central bank may have different operational risk standards. Any of these issues may disrupt the operation of a CBDC, which may lead to reputational damage and economic loss.
- **Exit strategy risk** refers to the risk that no appropriate exit strategy is in place, which could arise from an overdependency on one third party. This may also be called vendor lock-in risk. CBDC initiatives may require the implementation of new technologies, which may lead to a high level of dependency on technology vendors.[55]
- **People risk** may arise if there is not enough training and upskilling in place, or if there is fraud or the inappropriate disclosure of information. In the CBDC context, insufficient capabilities and skills at the central bank may be a key risk. Dependence on the knowledge of a third party may pose other types of OR, including the inappropriate use of data.
- **Strategic risks** may arise if a third party's strategy does not align with a central bank's and if a central bank does not have sufficient expertise to oversee the third party.
- **Financial ecosystem risks** may arise in integrating a CBDC system with existing financial infrastructure, such as real-time gross settlement (RTGS) systems, if the systems are insufficiently interoperable.[56]
- **Facility risks** refer to dependencies on power and telecommunications, which are part of business continuity risk discussed in section 2.4.

Third-party risks and infrastructures

Common third-party risks associated with both centralised databases and DLT-based CBDCs include dependencies on database and blockchain providers, servers and software. For example, payment services may be interrupted during the switch from one payment service provider (PSP) to another. Potential operational risk may arise if the servers of payment service providers are down due to natural disasters or power outages, or if the network is congested or down. On the software front, potential operational risk may arise if attacks disrupt the software of third parties, or if the software needs updates.

Some third-party risks unique to DLT-based CBDCs are discussed in Table 5.[57] For example, operational disruptions may arise in the event that key management custodians are attacked, private keys are lost, external servers are attacked or the data transmitted by servers are not reliable. In addition, disruptions to the operations of third parties that participate in the validation process pose operational risks to CBDCs.

[55] BCBS (2005).

[56] RTGS refers to funds transfer systems that transfer money or securities on a real-time basis.

[57] See also Hansen and Delak (2022).

Examples of third-party risk

Table 5

Identified risk	Causes/sources				Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
	Processes	People	Systems	External event			
Operational risk related to third parties.	x	x	x	x	Operational risk may arise if third parties face: technology failures, cyber-attacks, fraud or error, business disruptions, dependencies on a fourth party or different operational risk standards. Information may not be gathered from third parties on time.	• Operational disruption. • Reputational loss. • Economic loss. • Information oligopoly. • Extended time to recover CBDC operations.	Technology, Operating, Business continuity, Reputational
Exit strategy risk.	x		x	x	Over dependency on a single technology vendor may cause exit strategy risk (vendor lock-in risk).	• Operation disruption. • Reputational loss. • Economic loss. • Intellectual property disputes.	Operating, Business continuity, Reputational
Third-party risk related to a DLT-based CBDC.	x	x	x	x	Operational risk may arise if there are disruptions with key management custodians, external oracles or third parties participating in the validations.	• Operational disruption. • Reputational loss. • Economic loss.	Technology, Operating, Business continuity, Reputational

Source: CBDC Task Force.

Third-party risk and CBDC architecture

The level of third-party risk depends on the design choices related to CBDC architecture. For two-tier CBDCs (hybrid, intermediated or indirect), there is a clear reliance on third parties to handle payments. For example, if a third party has a power outage, then their customers' payments cannot be processed. Direct models can also rely on third parties, for activities such as implementing Know Your Customer (KYC) or account validation. Third parties can also be technology providers in both direct and two-tiered models. Therefore, third party risk will be linked to choices of the central bank in terms of the activities it decides to externalise.

Auer and Böhme (2021) state that the quantity of public information stored by the central bank depends on CBDC architectures. More information is held for a direct CBDC, while less information is shared for two-tier CBDCs. The balance of information held by central banks and by third parties could result in risks to data privacy, integrity and availability. These implications indicate that dependence on third parties could increase the organisational risk profile of the central bank, and thus become a strategic risk. Therefore, models of shared responsibility (particularly for data management) between central banks and third parties should be well defined.

Box 1

Example: outage of the DCash platform

An example of the materialisation of both technological and third-party risk is when the digital currency of the Eastern Caribbean Central Bank (ECCB), DCash, suffered an outage on 14 January 2022. This outage was due to an expired certificate in the version of Hyperledger Fabric used to implement the consensus algorithm underlying DCash.[58] This caused many failed transactions to occur but did not corrupt balances.[59] The outage was severe and was not resolved until March 2022

Mitigants to deal with third-party risks

A third-party risk management (TPRM) model can be helpful in this context. A TPRM model for CBDC begins by identifying external participants and assessing risks (see again Table 5). Addressing third-party risks from technology providers is especially important due to concerns related to data confidentiality, availability and integrity risks.

Board of Governors of the Federal Reserve System et al (2021) and The Office of the Superintendent of Financial Institutions (Canada) (2021), provide guidance on how to manage third-party risk. The *Principles for financial market infrastructures* (PFMI) provides international standards for payment systems, which can be applied to mitigate third-party risk such as financial ecosystem risks discussed before.[60] Auer and Böhme (2021) discuss enhanced monitoring and oversight of third parties that provide services to support CBDCs.

An effective TPRM model for CBDC follows the third-party risk management lifecycle.[61] Graph 9 shows the three stages of the TPRM lifecycle. In stage 1, the onboarding phase, a central bank develops a plan to manage the risks associated with third parties, performs due diligence to select a third party, and negotiates a contract that defines the rights and responsibilities of all parties. In stage 2, the monitoring phase, a central bank conducts ongoing monitoring and oversight of the third party’s activities. In stage 3, the offboarding phase, a central bank implements plans to terminate third-party relationships effectively.

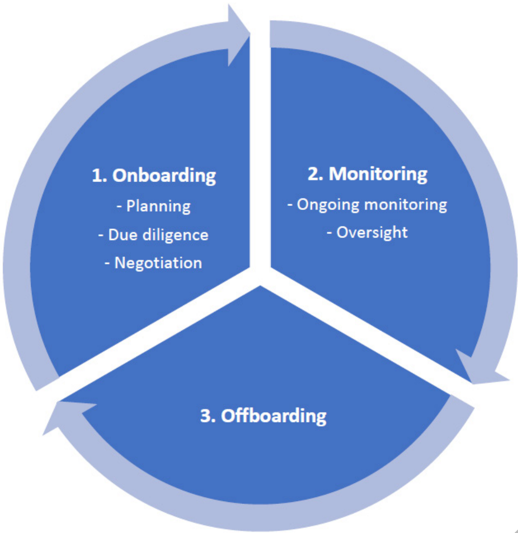
[58] Margulies (2022).

[59] ECCB (2022).

[60] CPSS-IOSCO (2012). See also ORIC International and McKinsey & Company (2017) and EBA (2019).

[61] Board of Governors of the Federal Reserve System et al (2021).

Third-party risk management lifecycle Graph 9



Source: CBDC Task Force.

2.4 Business continuity risk management: a critical component to strengthen CBDC resilience

Business continuity can be understood as “the process that allows organisations to continue operating during a disruption, ensuring the protection of their processes, assets and human resources.”[62] The IRM framework defines effective control mechanisms to prevent and mitigate disruption in operations which might be caused by failures or errors in process, people, systems, suppliers or external events.

An IRM framework for CBDC facilitates the identification of risk scenarios, threats and mitigants.

It should be an input for defining the base components for business continuity planning (BCP) and its decision-making process at the organisational level.

The following table describes some of the main business continuity risks that need to be addressed in relation to CBDCs. It shows examples of business continuity risks, which, were they to materialise, would result in a short or prolonged interruption or disruption to a CBDC platform and services.

[62] CGRM (2022).

Some key risks impacting business continuity of CBDC

Table 6

Category	Identified risk	Causes/ sources				Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
		Processes	People	Systems	External event			
Business continuity risks	Natural disasters affecting critical infrastructure.				x	Some countries have high exposures to natural disasters causing disruptions (weather, earthquakes etc).	• High impact on operational continuity of service. • Potential crisis management in case the critical infrastructure cannot be recovered, or the data are damaged, confidentiality is breached, or they are not backed-up.	Legal, Technology, ICT/cyber
	Business continuity capabilities are not ensured by third parties (supply chain disruption).			x	x	Some CBDC cycle stages could rely on suppliers (such as emission, validation, ledger, user services), which could suffer disruptions. Some countries rely on private sector infrastructure service providers which, in case of disruption, might have a significant impact on payment performance and on users.	• Depending on the level of suppliers' dependency, in case of interruption or disruption, it could impact operational performance, reputation, and loss of data or privacy. The impact might be severe depending on the assets compromised. • High impact on operational continuity of service.	Legal, Third party
	CBDC infrastructure with high dependence on the private sector may rely on their recovery capabilities.	X			x	Central banks may not be part of the business continuity and resilience plan and decisions thus relying on private sector capabilities and their recovery prioritisation.	• Central bank could outsource services on infrastructure operations and maintenance, without sufficient legal components to ensure that the central bank manages key decisions on the critical processes in case of a disruption or even a crisis.	ICT/cyber, Technology
	Offline systems could raise several ICT risks.	X	x	x	x	There is currently no technology to ensure authenticity in offline systems. There is a need to analyse the level of cyber security in the case of offline payments, which are out of the ledger.	• There is a high level of complexity in these technologies, and they use a mixed group of security elements that might complicate contingency plans in action. • Some security control cannot be replicated when a contingency plan is active, exposing the central bank to several threats.	

Source: CBDC Task Force.

During the Covid-19 pandemic some central banks faced operational constraints on maintaining continuity and dealing with challenges introduced by remote work. Information and cyber security were among the most complex risks faced and central banks worked hard to rapidly address them. Additionally, some central banks concluded that a CBDC project could enable them to reach users in remote locations or in communities affected by natural disasters.

Box 2

The ECCB's DCash from a business continuity perspective[*]

It is interesting to revisit the ECCB case from a BCP perspective. The ECCB accelerated the expansion of its DCash pilot to Saint Vincent and the Grenadines in 2021 due to a volcanic eruption (ie a natural disaster scenario). In this context, CBDC might be viewed as a mitigant by providing affected communities with the means to make and receive payments, thereby creating a resilient payment system.

Nevertheless, as previously described in the third-party risk part of this section, in January 2022 the DCash platform suffered an interruption caused by technical issues. Despite this, account balances and data security were not affected, and the pilot served as an opportunity to test systems resilience. This case serves to emphasise that mitigating business continuity risks is multifaceted and that BCP for numerous and sometimes conflicting scenarios should be considered by central banks.

* ECCB (2022).

From BCP towards a resilience framework

Implementing a strategic BCP supports the role of a central bank in safeguarding the financial system. It does this by incorporating the ICT risk framework (for protecting data and systems) and cyber security (as part of ICT risk framework) to form an overall **resilience framework**.

There are several steps central banks should take to apply their BCP process to a CBDC: (i) identify critical processes; (ii) identify and evaluate critical assets and resources; (iii) define risks, scenarios and threats to be evaluated; (iv) define mitigation strategies, and contingency and recovery plans; and (v) test plans to find improvements to the cycle.[63]

Some strategies can be managed by establishing a back-up system for critical infrastructure. In some countries, CBDCs themselves can be seen as part of a **payment system contingency plan.**[64] The central banks in these countries initiated pilot projects with the goal of creating an additional operational option for use in case of major disruption to digital payments.

Central banks may have to work in partnership with the private sector (suppliers, vendors or other intermediaries) and other government agencies to promote best practices and risk models to ensure resilience. They also need to establish the "right to audit" or "due diligence" processes to assess the operation of functions allocated to third parties. It is worth considering extending these rights to fourth parties as well.

Legally binding contracts and agreements are thus crucial to defining the relationship between central banks and third parties, and responsibilities in case of incidents. Another set of mitigants include applying security and technical standards to manage CBDC operations. Since there may not be specific standards for new technologies, these legal frameworks are essential for protecting assets (ie people,

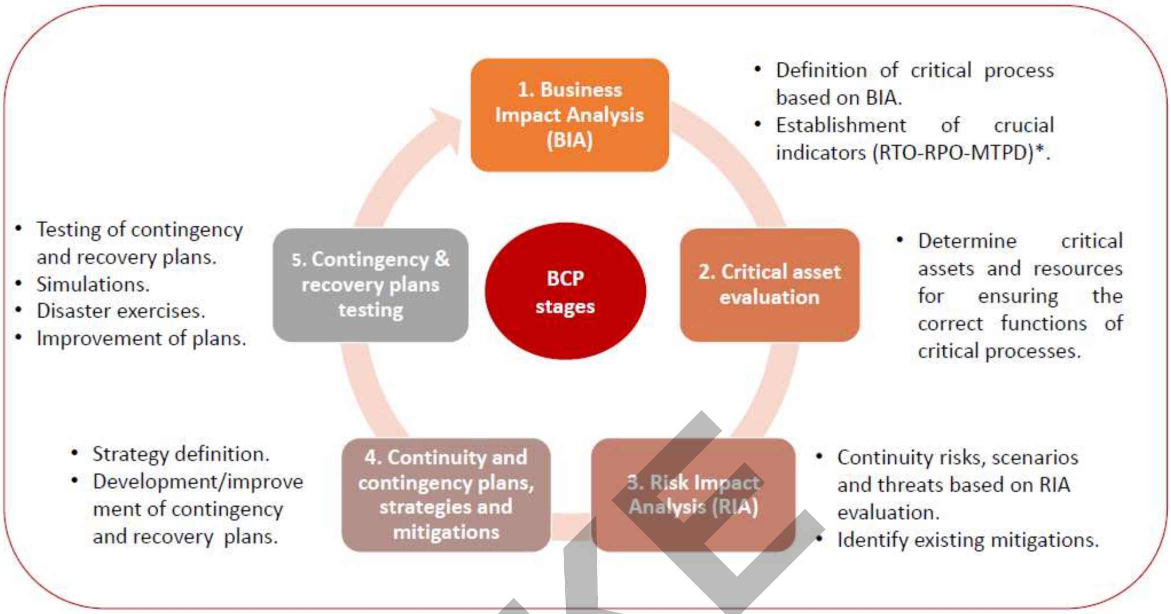
[63] ISO (2019).

[64] Sveriges Riksbank (2022), Bank of Canada (2020) and Soderberg et al (2022).

technology, infrastructure and information) and therefore ensuring resilient CBDC operations.

Business continuity planning cycle

Graph 10


1. Business Impact Analysis (BIA)
• Definition of critical process based on BIA.
• Establishment of crucial indicators (RTO-RPO-MTPD)*.
BCP stages
2. Critical asset evaluation
• Determine critical assets and resources for ensuring the correct functions of critical processes.
3. Risk Impact Analysis (RIA)
• Continuity risks, scenarios and threats based on RIA evaluation.
• Identify existing mitigations.
4. Continuity and contingency plans, strategies and mitigations
• Strategy definition.
• Development/improvement of contingency and recovery plans.
5. Contingency & recovery plans testing
• Testing of contingency and recovery plans.
• Simulations.
• Disaster exercises.
• Improvement of plans.

RTO = Recovery Time Objective: the maximum time to restore operations after a failure.
RPO = Recovery Point Objective: the maximum time to restore data to avoid data loss.
MTPD = Maximum Tolerable Period of Disruption: the time-period that could be endured as a result of a disruption before being deemed unacceptable.

Source: CBDC Task Force (based on ISO 22301 (2019)).

To summarise, information security risk management can be linked to BCP to ensure an integrated risk perspective for CBDC based on principles for operational resilience.[65] Assessing scenarios and threats provides a holistic evaluation for critical processes and their assets. It also helps to secure information/data sensitivity, availability and integrity.[66] Finally, implementing resilience policies must promote private-public partnership innovation for CBDC technologies.[67]

Graph 11 emphasises the need to link BCP efforts with ICT risk management and third-party risk management to form a resilience framework which highlights that all critical processes should have contingency and recovery plans in place. The graph is based on the Digital Operational Resilience Act (DORA) which emphasises the interdependencies of ICT risk models, business continuity plans, third-party risks and ORM as part of a IRM framework.[68] DORA is a robust OR framework for mitigating “digital risks” on CBDC projects and it also considers connections with EU proposals related to DLT management. Similarly, the ISO has established standards by which to

[65] BCBS (2021c).

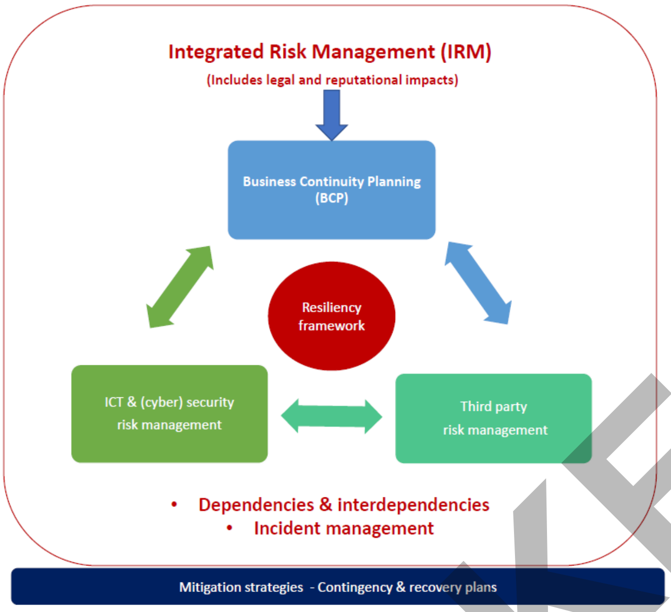
[66] Hansen and Delak (2022).

[67] EBA (2019).

[68] European Commission (2020).

manage security and resilience in organisations as a set of best practices on resilience.[69] In this way, resilience capabilities are essential to the delivery of desired outcomes associated with CBDCs in all types of environments.[70]

Proposed resilience framework Graph 11


Integrated Risk Management (IRM)
(Includes legal and reputational impacts)
Business Continuity Planning (BCP)
Resiliency framework
ICT & (cyber) security risk management
Third party risk management
• Dependencies & interdependencies
• Incident management
Mitigation strategies - Contingency & recovery plans

Source: CBDC Task Force.

Insights from the Task Force's analysis: towards integrated risk management and resilience

Central banks should consider any new CBDC projects from a risk management perspective. The Task Force undertook an analysis of relevant risk categories, although the lists of contemplated risks within each category are non-exhaustive. Insights from this review could be useful for risk managers and boards of directors in the context of a CBDC.

First, issuing a CBDC may considerably change a central bank's risk profile. This means that central banks should review their risk appetite in respect of some processes that have not traditionally dealt with the same level of complexity, such as legal, IT, security, digital, and availability of specific skills and capabilities, as well as identifying and planning for potential (external) scenarios that might cause disruptions (see Graph 8).

Second, identifying risks in an integrated manner is essential due to the potential generation by a single risk of multiple impacts across the entirety of the CBDC project.

[69] ISO (2022).

[70] BCBS (2021c).

In this respect, the operational perspective should start with Basel III framework and expand to consider other categories suggested by this work (see Table 2) for an integrated risk management framework. It is worth mentioning that all risk categories analysed could impact the reputation of a central bank.

Third, skills and capabilities, along with a high degree of flexibility to acquire new technologies and clear CBDC process maps may contribute to the mitigation of operating and IT risks. Regardless of the architecture or model defined for a CBDC, several risks mapped by the Task Force were identified as root cause of risks and require rapid adoption of knowledge and capabilities by central banks. These areas include new operations, technologies, security standard adoptions and integration with third parties. However, such rapid adoption would require high security standards to ensure confidentiality, integrity and availability. For this reason, cyber security is one of the key risks to be managed in a CBDC project (see the next section).

Finally, a strong resilience framework appears to be a requirement for the successful implementation of a CBDC and, in particular, to ensuring the effectiveness and efficiency of real-time operations. BCPs should be integrated with cyber security as part of ICT risk management and in the risk models of third parties (see Graph 9). Together, they produce an operational resilience model (see Graph 11), identifying risks and threats, and predicting and preventing serious events. It would also protect critical assets and CBDC processes, and, if necessary, enable their recovery. Being resilient also means that central banks should continuously work in an active partnership with strong coordination between all parties involved in CBDC operations to ensure the stability of the financial system.

This section focused on general risk management tactics, strategies and principles that central banks should consider as they embark on a CBDC project. We now turn to a detailed discussion on a major potential external risk facing central banks in the operation of a CBDC, namely cyber risk.

3. Cyber security is a key risk for CBDCs

The CBDC cyber security threat landscape

The financial industry is experiencing a notable increase in the frequency, sophistication and severity of cyber attacks against financial institutions and financial market infrastructures (FMIs).[71] As central banks actively explore and deploy CBDCs, three main insights need to be considered when defining the cyber threat landscape that they will be operating in.

First, it is well understood that CBDC projects will be high-value targets for a wide range of threat actors. In this environment, even if successful large-scale attacks do not jeopardise the integrity of a CBDC, any successful attack, even if minor, may erode public confidence in the system. It will be important to assess the cyber resilience of any proposed CBDC implementation relative to the cyber attack landscape to determine if there are any uniquely identified risks and their associated mitigants,

[71] IBM (2021).

particularly with respect to the risks mentioned in Table 2, ie ICT risks and business continuity risks.

To better understand cyber security risks, it is important to use threat models.[72] In particular, threat actors can be categorised as:

- Nation state-sponsored groups: these adversaries are part of or sponsored by a particular government and work to disrupt or compromise other governments, organisations or individuals to gain access to IT systems, information assets or create incidents towards some intended outcome.[73] These threat actors are highly skilled and motivated, with significant resources at their disposal. They can develop zero-day attacks on demand as well as influence or co-opt third-party software and hardware producers to introduce vulnerabilities into the supply chain.[74]
- Criminal organisations: individuals or groups of people that use technology to commit malicious incidents on IT systems to steal sensitive data, use computing resources without authorisation or to generate profit. Financial organisations are a particularly attractive target as a result of their large number of customers, their ever-expanding attack surface due to an increasing reliance on technology and the fact that they hold sensitive data on individuals. An attack on financial organisations also holds out the possibility of executing fraudulent transactions.
- System insiders: those individuals (with both privileged and non-privileged access) who have access to the internal operations of a CBDC (eg system administrators, developers and operators).
- Malicious users: malicious users of the CBDC will be able to access and exploit externally facing systems and applications, typically to manipulate the system and execute fraudulent transactions. This contrasts with system insiders who will have access to the internal operations, IT and processes of the CBDC system.
- Third parties: external entities including vendors, suppliers, partners, contractors or service providers that have access to CBDC systems, processes, data or privileged information. Third parties that were initially trusted and subject to enhanced due diligence, and that play a critical role in a CBDC business model/ecosystem, may eventually be subject to an acquisition or takeover by untrusted nations or organisations resulting in vulnerabilities.

Second, in certain reference architectures, the complexity and scale of a given CBDC technology stack may introduce unintended security vulnerabilities. Specifically, the digital transformations that many central banks are embarking on are resulting in accelerated system migrations to spark innovation and digital growth. This is also the case in respect of CBDC implementations. These transformations can cause operational challenges for both IT and security due to the pace and scale of

[72] "A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment" (NIST (2023)). Available at https://csrc.nist.gov/glossary/term/threat_modeling.

[73] Often referred to as advanced persistent threat (APT).

[74] A zero-day exploit is an attack against a software or hardware vulnerability that has been discovered but not publicly disclosed.

new technology adoption. Furthermore, although CBDC is not synonymous with DLT, several central banks are considering the use of this novel technology in the research, experimentation and implementation phases. The extent to which DLT will form a core part of a CBDC implementation in central banks is still uncertain.

This brings another set of challenges as both the technology and supporting processes regarding DLT are still evolving. Moreover, the associated vulnerabilities and threats are not as well understood as they are in respect of traditional IT.[75] In fact, some DLT-based schemes will make use of smart contracts that may utilise a Turing complete language (using conditional statements and loops). Although this allows for the development of complex near real-time logic on payment transactions, it would require a stringent security code review as there would be a requirement of near perfect logic and perfect coding in order to avoid introducing unintended vulnerabilities into the system. These characteristics pose both IT and ICT risks – particularly cyber security risks – for the CBDC project, as described in Table 2.

The implementation of a CBDC will require a high level of operational readiness, operational excellence (including risks relating to operations, IT, legal, third parties, compliance and business continuity), as well as cyber resilience. Accordingly, a focus on cyber security is required to assess the overall resilience of the system relative not only to the current payment system infrastructure but also to ensure that relevant interfaces and interactions do not pose vulnerabilities or diminish the current posture.

Third, several cross-border CBDC trials are underway, including projects Dunbar, Jura and mBridge, to test both wholesale and retail CBDCs.[76] For those jurisdictions that choose to use CBDC for cross-border payments, interoperability between payment systems will be a key consideration to achieve the necessary efficiency, innovation and ease of use required to promote wide-scale adoption. An IRM assessment of a cross-border feature for CBDC might involve IT, business continuity, legal, third-party and ICT risks, as previously mentioned (see Graph 2). However, on the latter, cyber security considerations need to be considered from the outset as they facilitate transactions that are inherently more complex than those that operate domestically. This highlights the need for international security standards to ensure that the overall payment system remains highly interoperable, secure and resilient by design.

An effective security analysis is one that is proactive. It requires that threats are considered first so that potential vulnerabilities can be identified during the system design phase. Identifying and remediating vulnerabilities at the design phase makes the system more resilient, reduces the attack surface and potentially reduces the cost of adding required (and unexpected) security features or compensating controls once the system has been implemented.

[75] HLEAC (2022) states that "a CBDC system, as a piece of critical national infrastructure, would be a target for attack from nation state or criminal actors. Such attacks would risk the exposure of sensitive payments data and the loss of national wealth. No design will guarantee absolute security. Any CBDC would need to be designed so that it was adaptable and could be updated rapidly in response to technological change and emerging security threats."

[76] Bech et al (2022).

Threat models are a useful way to understand security threats to a system, determine risks from those threats and establish appropriate mitigants, preferably during early implementation phases. Several methodologies exist that allow for a comprehensive review of the system design or architecture to discover and correct security flaws.

For example, the STRIDE threat model allows for the analysis of a broad range of methods that threat actors may use to exploit CBDCs.[77] It is used by decomposing the system to be secured into parts to analyse the vulnerability of each part to the identified threats. Each identified threat represents a violation of a desirable property for a system. STRIDE can be iteratively used for increasingly lower levels of system abstraction and compositions, to analyse each component for susceptibility and possible mitigants, for identified threats. Table 7 shows a sample (ie a non-exhaustive list) of a high-level STRIDE analysis for a CBDC system.

STRIDE cursory analysis of CBDC

Table 7

Threat	Property violated	Threat definition
Spoofing	Authentication	• A malicious entity pretends to be a legitimate user.
Tampering	Integrity	• Reliance on hardware and software vendors to enforce transaction integrity (in some designs).
Repudiation	Non-repudiation	• CBDC end users could try to spend the same funds from their wallets in multiple places. This double spending is a form of digital counterfeiting. • The CBDC portal/services may be spoofed by a malicious entity that a wallet connects to or is using as a relay to connect to a portal.
Information disclosure	Confidentiality	• If a system collects a huge amount of data and does not include privacy protections, then (i) it could be visible to system operators and (ii) if it is breached, sensitive data may be disclosed to the attacker.
Denial of service	Availability	• Malicious attackers could overwhelm the CBDC system with requests, preventing legitimate users from accessing CBDC services. • Damaged e-wallets could lead to the loss of funds. • Insiders at the central bank could accidentally impact the system or deliberately make fraudulent transactions.
Escalation of privileges	Authorisation	• Roles with privileged access, such as IT administrators or system operators, that are able to freeze or withdraw funds in CBDC accounts without users' consent, could lead to abuse of the CBDC system.

Source: CBDC Task Force.

[77] STRIDE is an acronym for spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege (Microsoft (2022)).

Cyber security risk categorisation

To properly categorise the cyber security risks associated with CBDCs, it is important to ensure a common understanding of the definitions of several critical terms (Box 3).

Box 3

Definitions

The term "cyber risk" is typically used to define a wide range of risks caused by either benign events or malicious incidents. Examples of benign events can include component or process failures, human error and accidental disclosure, while examples of malicious incidents could include phishing attacks and data breaches. FSB (2023) refers to cyber risk as "*the combination of the probability of cyber incidents occurring and their impact.*" [78] A cyber incident is defined as, "*a cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits, whether resulting from malicious activity or not.*"

While an information and technology risk can be defined as, "*The risk of deficiencies in the availability, performance, compatibility or capacity/efficiency of information technology systems caused by inadequate selection, implementation or operation. Additionally, the risk that data or information is incorrect, out of date, missing, irrelevant or incomplete when such data is required.*"[79]

Security measures must be put in place to protect the financial system and thus mitigate cyber risks at an acceptable threshold. This applies in respect of any event that could violate the security policies of the system and includes threats emanating from malicious actors who could exploit vulnerabilities for financial gain. Banks and other financial institutions must ensure that their systems are up to date with the latest software updates and security protocols whilst employing robust anti-fraud measures in order to protect their customers and keep their systems secure.

In fact, a cyber incident can be thought of as the realisation of a cyber risk (ie an event) that causes adverse consequences to the **confidentiality**, **integrity** or **availability (CIA)** of information systems and technology assets, or that violates policies on the acceptable use of information by insiders or external actors. Thus, "cyber security" can be defined as the "*preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.*"[80]

The CIA triad, shown in Graph 9, represents a model used to guide policies and define information security requirements for an organisation, it has three components:

- Confidentiality – preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability – ensuring timely and reliable access to, and use of, information by authorised users.[81]

[78] FSB (2023).

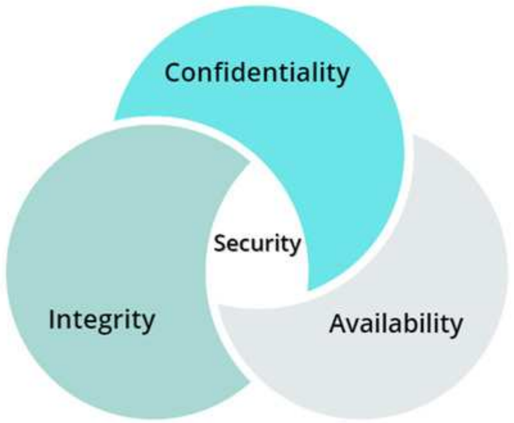
[79] BIS (2023), Internal policy document.

[80] FSB (2023).

[81] Cawthra et al (2020).

The CIA triad

Graph 12



Source: CBDC Task Force

Cyber and IT risks can be caused by either benign or malicious incidents. However, in both cases, the threat of misuse of information and communication technologies by insiders (malicious or careless) or external actors is challenging to address. Ultimately, a CBDC system is built upon IT systems and the baseline security requirements will be defined by considering how to satisfy the CIA triad.

A CBDC implementation project will be exposed to a wide range of risks, including cyber security risks. A cyber risk can be further refined as the intersection of assets, threats and vulnerabilities coupled with the probability of their occurrence and their respective impacts. Definitions are as follows:

- *Asset and asset processes* – a major application, general support system, high-impact program, physical plant, mission critical system, personnel, equipment, process or a logically related group of systems.[82]
- *Cyber threat* – any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image or reputation), organisational assets or individuals through an information system via unauthorised access, destruction, disclosure, modification of information and/or denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability.[83]
- *Vulnerability* – a weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.[84]

[82] NIST (2023), available at https://csrc.nist.gov/glossary/term/asset.

[83] Modified from NIST (2023), available at https://csrc.nist.gov/glossary/term/cyber_threat.

[84] Modified from NIST (2023), available at https://csrc.nist.gov/glossary/term/vulnerability.

The assessment of a risk requires an understanding of the threats to the organisation, the potential vulnerabilities within the organisation, and the likelihood and associated impacts of the successful exploitation of those vulnerabilities by the associated threats.[85] *Impact* refers to the level of disruption that may occur if an information system is jeopardised in the event that a particular cyber risk is realised. These levels include:

- *Very low* – loss of confidentiality, integrity or availability that could be expected to have a negligible adverse effect on organisational operations, organisational assets, individuals or other organisations.
- *Low* – loss of confidentiality, integrity or availability that could be expected to have a limited adverse effect on organisational operations, organisational assets, individuals or other organisations.
- *Moderate* – loss of confidentiality, integrity or availability that could be expected to have a serious adverse effect on organisational operations, organisational assets, individuals or other organisations.
- *High* – loss of confidentiality, integrity or availability that could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, individuals or other organisations.
- *Very high* – the loss of confidentiality, integrity or availability that could be expected to have multiple severe or catastrophic adverse effects on organisational operations, organisational assets, individuals or other organisations.[86]

Likelihood can be defined as a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.[87] Likelihood levels can be categorised as very high, high, medium, low, and very low, defined as:[88]

- *Very high* – an adversary is almost certain to initiate the threat event; or an error, accident or act of nature is almost certain to occur or occurs more than 100 times a year.
- *High* – an adversary is highly likely to initiate the threat event; or an error, accident, or act of nature is highly likely to occur or occurs between 10 and 100 times a year.
- *Medium* – an adversary is somewhat likely to initiate the threat event; or an error, accident, or act of nature is somewhat likely to occur or occurs between one and 10 times a year.
- *Low* – an adversary is unlikely to initiate the threat event; or an error, accident, or act of nature is unlikely to occur or occurs less than once a year but more than once every 10 years.

[85] NIST (2020).

[86] NIST (2012).

[87] NIST (2023) available at https://csrc.nist.gov/glossary/term/likelihood_of_occurrence.

[88] Adapted from NIST (2012).

- *Very low* – an adversary is highly unlikely to initiate the threat event; or an error, accident or act of nature is highly unlikely to occur or occurs less than once every 10 years.

Table 8 reveals the level of risk based on a combination of likelihood and impact.

Level of risk (combination of likelihood and impact) Table 8

Likelihood	Level of impact				
	VL	L	M	H	VH
VH	VL	L	M	H	VH
H	VL	L	M	H	VH
M	VL	L	M	M	H
L	VL	L	L	L	M
VL	VL	VL	VL	L	L

VL = very low, L = low, M = medium, H = high, VH = very high.

Source: CBDC Task Force.

Analysis methodology

Our methodology to assess the cyber risk of CBDCs is as follows: (i) an organised and systematic literature review was undertaken to identify a mixture of CBDC policy and technically focused papers (ii) each paper was analysed to identify cyber security-related threat events; (iii) the identified threat events were then notionally categorised into high-level cyber risk categories using a number of attributes; and (iv) duplicate threat events were removed and high-level cyber risk categories were determined.[89]

Thirty-seven cyber security threat events were identified as part of our analysis. Specifically, these threat events could, if realised, cause adverse consequences to the confidentiality, integrity or availability of the implementation of a CBDC. The attributes used to categorise threat events were based on several factors including: the threat event outcome; likelihood of the threat event occurring; whether DLT is potentially used as part of the technology stack, and the impact on the CIA triad. Of note, DLT is a novel and constantly evolving technology, thus CBDC implementations that make use of DLT will require additional analysis to properly assess the threat.

A total of eight cyber risks were identified. They included:

[89] "An event or situation that has the potential for causing undesirable consequences or impact" (NIST (2023)). Available at https://csrc.nist.gov/glossary/term/threat_event#:~:text=Definition(s)%3A,causing%20undesirable%20consequences%20or%20impact.

1. Breach of data privacy: occurs when the confidentiality of specified data is compromised.
2. Denial of service: occurs when legitimate users are unable to access information systems, devices or other network resources due to the actions of a malicious cyber threat actor.
3. Human error, negligence, malfeasance or lack of awareness: the threat that an insider will use her/his authorised access, wittingly or unwittingly, to do harm to the security of organisational operations and assets, individuals or other organisations.[90]
4. External dependency management: managing the risks that are associated with an organisation's dependence on external entities.
5. Complexity of the technology stack: the more complex a technology stack becomes the more it is prone to inefficiency and additional operational overheads, and this complexity also makes it more difficult to implement, monitor and operate a comprehensive and risk-based security control regime.
6. Complexity of the DLT technology stack: as this is new technology and has not yet been extensively studied, it may have a greater number of security vulnerabilities. Additionally, DLT technology is more complex from a security point of view than many traditional non-DLT IT options.
7. User credential theft and loss: a user cannot retrieve their login details (eg username and password) or a malicious actor steals login details to use them to gain unauthorised access to service applications or IT assets.
8. Disclosure of secret private keys or data leakage related to cryptographic vulnerabilities: the loss of private encryption keys or weak encryption methods/configurations (eg quantum cryptography) may result in the exposure of sensitive data or loss of the use of an asset through potential vulnerabilities.

Tables 9 to 16 below reveal the identified cyber risks and their associated threat events. The likelihood ratings given the specific threat events match the descriptions above and the DLT column is marked "Y" for threat events considered to be unique to DLT reference architectures and/or those threats requiring careful analysis when using a DLT implementation. This is to ensure that such risks are adequately understood and addressed.

[90] NIST (2023) available at https://csrc.nist.gov/glossary/term/insider_threat.

Data privacy risk

Table 9

Threat event	Description	Likelihood	DLT	C	I	A
Data breach.	Data collection and the potential for the aggregation of massive amounts of user data.	M	Y	✓		
Use of CBDC in illegal activities.	CBDC implementations must strike the right balance between user privacy and enhanced monitoring to meet (AML/CFT) requirements.	M	N	✓		
Misuse of technology limitations.	Cryptographic privacy protections are so computationally demanding that their use on system complements such as mobile devices may not be feasible.	M	N	✓		

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events.

Source: CBDC Task Force.

Denial of service risk

Table 10

Threat event	Description	Likelihood	DLT	C	I	A
Denial of service (online or offline).	An adversary could overwhelm the CBDC system with spurious requests (eg at the network or application layers), preventing legitimate users from accessing CBDC services.	M	N			✓
Denial of service (offline CBDC).	Wallets (eg hardware devices) damaged or lost offline could result in loss of funds.	M	Y			✓

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events.

Source: CBDC Task Force.

Human error, negligence, malfeasance or lack of awareness risk

Table 11

Threat event	Description	Likelihood	DLT	C	I	A
Social engineering attacks (phishing).	Phishing attacks are a type of social engineering attack often used to steal user data, including login credentials.	**VH**	**N**	✓		
Social engineering attacks (other).	Attacks that rely on tricking the user into bypassing security procedures eg pretexting, tailgating or vishing.	**H**	**N**	✓		
Insider threats.	Insiders, either normal users or admin users (ie privileged accounts) could accidentally or intentionally adversely impact the system (eg freeze or make fraudulent transactions).	**M**	**N**	✓	✓	✓
Unintentional configuration errors.	Configuration errors can leave organisations vulnerable to serious cyber-attacks and data breaches.	**M**	**N**	✓	✓	✓

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events.

Source: CBDC Task Force.

External dependency management

Table 12

Threat event	Description	Likelihood	DLT	C	I	A
Concentration risk.	The over-reliance on a single third party for critical system components or expertise (concentration risk) or as consensus validators. Specific expert skills required to deploy and operate specific components of the technology may only be available from third parties.	**H**	**N**		✓	✓
Attacks against supply chain providers.	Reliance on the security of software/hardware vendors to enforce secure production practices.	**M**	**Y**	✓	✓	
Third-party vendor risk.	The use of CBDC is a collaborative effort that requires the participation of a multitude of suppliers and third parties.	**M**	**N**	✓	✓	✓
Cloud technology threats.	The use of cloud technologies to deploy a CBDC can improve availability, however proper monitoring, auditing, polices, safeguards and governance need to be in place.	**M**	**N**	✓	✓	
Failure to use secure source code.	Secure application programming will be employed regardless of CBDC architecture.	**M**	**N**	✓	✓	
Selecting dedicated devices (eg hardware) that are not tamper-resistant.	Single-purpose dedicated, tamper-resistant CBDC hardware devices will be relied upon for secure transactions during normal operations and potentially during times of crisis where network connectivity may be sporadic or absent.	**L**	**Y**	✓	✓	✓

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events.

Source: CBDC Task Force.

Complexity of the technology stack

Table 13

Threat event	Description	Likelihood	DLT	C	I	A
Theft of payment credentials.	User/system credentials may have to be stored or replicated on more than one device, making them more susceptible to attacks	H	Y	✓	✓	✓
Disclosure of CBDC data in the cloud.	Suitable precautions need to be taken to isolate CBDC-specific resources from other clients.	M	N	✓	✓	
Interconnectivity (overdependent interaction with different CBDC designs).	Security standards for payment interface providers would ensure resilience, interoperability and consumer protection but also require extensive resources (time, cost, personnel) to integrate globally which can hinder local CBDC implementations and restrict it to operating in isolation.	L	Y	✓	✓	✓
Smartphone integration complexities.	Any CBDC store of value and supporting application running on a smartphone would have a complex, multi-factor threat surface. In addition, manufacturers exert control over the platform and can limit access to critical system components, including embedded secure enclaves and subscriber identity module (SIM) cards.	M	N	✓		
Protocol or programming errors.	Cloud integration and use of APIs coupled with programmable transactions can amplify the scale and scope of errors and vulnerabilities.	VH	N	✓	✓	

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events

Sources: CBDC Task Force

Complexity of the technology stack – DLT

Table 14

Threat event	Description	Likelihood	DLT	C	I	A
Malicious validators nodes.	If the CBDC operates on DLT, malicious validator nodes operated by non-central bank entities could present several threats. In addition, the central bank's monetary authority and independence may be undermined.	L	Y	✓	✓	
Double spending/ counterfeit.	CBDC end users could try to spend funds from their wallets in multiple places.	L	Y		✓	
Spoofing of CBDC protocol/services.	The CBDC portal/services may be spoofed by a malicious entity that a wallet connects to or is using as a relay to connect to a portal.	L	Y		✓	
Smart contract vulnerabilities/ code/logical fault.	Smart contracts are computer programmes and thus it is inevitable that they will have bugs that can lead to vulnerabilities. Programmable transactions can amplify the scale and scope of errors and thus vulnerabilities.	H	Y	✓	✓	✓
Misuse of multi-party consensus.	Multiple parties in the operation of the system increase the data theft targets for cyber attackers. However, the use of multi-party consensus also makes a system more secure as data cannot easily be manipulated, for example, to steal funds.	L	Y		✓	
Lack of security standards.	Existing security standards may have to be extended to accommodate some technology choices eg DLT and smart contracts.	M	Y	✓	✓	✓
Falsifying transactions (offline).	An offline system with poor non-repudiation controls could see an increase in fraudulent activity. It can attract those participating in illegal activity as a mechanism to disavow any knowledge of or connection to a potentially criminal act. At a systemic level, repudiation of transactions weakens traceability and forensic auditability. These are required for the prosecution of illegal activities.	M	Y		✓	
Lack of adequate privacy mechanisms.	When accessing sensitive information from individuals, adequate controls must be put in place for their protection. Including regulatory and legal compliance.	M	N	✓		

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events

Sources: CBDC Task Force

User credential theft and loss

Table 15

Threat event	Description	Likelihood	DLT	C	I	A
Access credentials could be stolen or lost.	The impact of credential theft and loss could be extremely damaging to an individual or entity's savings held in CBDC, and it could also damage the central bank’s reputation.	**VH**	**N**	✓	✓	✓
Attacks against user accounts with privileged roles.	Roles with privileged access, such as IT administrators or system operators, that are able to freeze or withdraw funds in CBDC accounts without users’ consent, could lead to abuse of the CBDC system. These accounts are prime targets for threat actors.	**H**	**N**	✓	✓	✓
Theft of biometric security data.	Biometric identifiers cannot be changed once leaked and malicious entities may try to exploit biometric stores to impersonate users or commit fraud.	**M**	**N**	✓	✓	✓

VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events

Sources: CBDC Task Force

Disclosure of secret private keys or data leakage related to cryptographic vulnerabilities

Table 16

Threats	Description	Likelihood	DLT	C	I	A
Quantum computing may render existing cryptographic primitives insecure.	Some cryptographic algorithms can weaken over time as technology advances, making them vulnerable to attackers. Any CBDC cryptographic functions should have the ability to change and upgrade the specific cryptographic techniques used by the system over time.	**M**	**N**	✓	✓	
Data compromise due to overreliance on cryptography (offline).	Cryptographic operations are mathematical algorithms that are executed to protect the confidentiality and integrity of sensitive assets. For offline use, cryptography techniques alone may not offer sufficient protection.	**M**	**N**			✓
Cryptographic weaknesses (operational).	For offline use, existing cryptography techniques alone may not offer sufficient protection.	**L**	**N**	✓	✓	
Loss of private keys.	Cryptography enhances security, but also has challenges. For example, losing the private key used to authenticate payment instructions would result in the funds being lost. Therefore, a combination of a high level of security around the storage of private keys and a mechanism to “freeze” and reissue CBDC for lost private keys would be required.	**M**	**N**	✓		✓
Use of weak cryptographic standards.	Cryptographic algorithms enable CBDC information to be secured so it must be robust and contemplate how long it will be safe in the medium and long term (eg quantum cryptography).	**L**	**N**	✓		

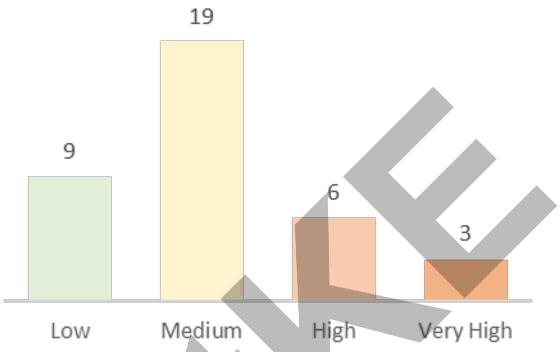
VL = very low, L = low, M = medium, H = high, VH = very high, Y = threat events considered to be unique to DLT reference architecture and/or those threats requiring careful analysis when using a DLT implementation, N = generic threat events.

Sources: CBDC Task Force

Eight cyber risks and 37 associated threat events that could realise those risks were considered in this analysis. Although not exhaustive, the list is representative and could be tailored and augmented to adequately capture the risks associated with a specific CBDC environment and reference architecture. Accordingly, this methodology could be used to prioritise mitigation formulations or for designing CBDC security control frameworks (ie through the use of likelihood ratings). Nine of the threat events have a likelihood rating of either high or very high (Graph 13). These threat events in particular should be carefully considered when a central bank designing a security control framework is adopting a risk-based approach to security.

The distribution of the likelihood levels that have been categorised

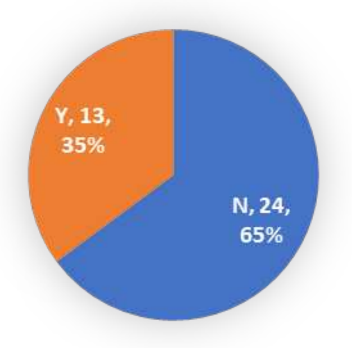
Graph 13



With respect to the effect of new technology on threat events, approximately one third of these threat events can be associated with the use of DLT (Graph 14). This further highlights that the use of novel technology will require careful analysis so that the right mitigants are institutionalised to address the risks to an acceptable threshold.

DLT-specific vs non-DLT-specific cyber risks

Graph 14



N = non-DLT-specific cyber risks; Y = DLT-specific cyber risks.

Source: CBDC Task Force.

The following table reveals key cyber security risks associated with a CBDC system.

Cyber security risks

Table 17

	Identified risk	Causes				Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
		Processes	People	Systems	External event			
Category	Data privacy.	x	x	x	x	The assurance that the confidentiality of, and access to, specified data is protected.	• Loss of reputation • Legal disputes • Potential for fraud • Data exposure	Compliance, Legal, ICT
	Denial of service.		x		x	Occurs when legitimate users are unable to access information systems, devices or other network resources due to the actions of a malicious cyber threat actor.	• Loss of reputation • Economic losses • Missed payments	Business continuity, ICT
	Human error, negligence, malfeasance or lack of awareness.	x	x			The threat that an insider will use her/his authorised access, wittingly or unwittingly, to do harm to the security of organisational operations and assets, individuals, or other organisations.	• Economic losses • Potential for fraud	Operating or process based, ICT
	External dependency management.	x			x	Managing the risks that are associated with an organisation's dependence on external entities.	• Operation disruption • Reputational loss • Economic loss	Third party, Technology, Operating or process based, Business Continuity ICT

Complexity of the technology stack.	x		x	x	The more complex a technology stack becomes the more it is prone to inefficiency and additional operational overhead as well as making it more difficult to implement, monitor and operate a comprehensive and risk-based security control regime.	• Technology • Operational • Business continuity • Reputational	Technology, Operating or process based, ICT
Complexity of the technology stack – DLT.	x		x	x	As DLT/blockchain/smart contracts are new technology, the associated technology stack can potentially have more security vulnerabilities. New technologies have not been studied as extensively and are more complex from a security point of view than many traditional non-DLT IT options.	• Technology • Operational • Business continuity • Reputational	Technology, Operating or process based, ICT
User credential theft and loss		x		x	When a user cannot retrieve their login details (eg username and password) or a malicious actor steals the login details to use them to gain unauthorised access to services applications or IT assets.	• Loss of reputation • Legal disputes • Potential for fraud • Data exposure	Business continuity, ICT
Disclosure of secret private keys or data leakage related to cryptographic vulnerabilities.	x		x		The loss of private encryption keys or weak encryption methods/ configurations (eg quantum cryptography) might result in the exposure of sensitive data or the loss of the use of an asset through potential vulnerabilities.	• Loss of reputation • Economic losses • Potential for fraud • Missed payments	

Source: CBDC Task Force.

Insights and observations

Given our cyber security analysis above, the deployment of a CBDC has several implications that may change the overall cyber risk profile of the central bank, as well as introduce new risks. Accordingly, we offer the following five insights.

First, CBDC implementations that make use of certain novel technologies (eg DLT) will have a different cyber risk profile to CBDC implementations that make use of conventional centrally controlled IT. For example, the underlying software that implements the DLT may not be fully vetted and there may be an over reliance on third-party expertise. Further, software developers implementing the software and security personnel assessing the security controls and mitigations may not have the required experience or training to identify and mitigate DLT-related vulnerabilities.

Second, although several cyber security frameworks exist that can be adapted to cover a CBDC implementation, there is no widely accepted cyber security framework for DLT. CBDCs will not only have a very diverse set of architectures but they will also make use of novel and still evolving technology as part of this implementation, eg DLT, digital identities, immutable data and smart contracts. Furthermore, since CBDC is relatively new compared with other payment systems, there are very limited historical data available to use to predict the likelihood and impacts of threats specific to CBDCs. Accordingly, to effectively manage these security risks, any security risk assessment or security framework must be adapted to evaluate the novel risks associated with a CBDC architecture in a threat landscape that is not well understood. This assessment can be undertaken under the IRM framework described in Section 2 and by considering the risk categories identified in Graph 2.

Third, our analysis has revealed eight cyber risks and 37 associated threat events that could realise those risks. While this is not an exhaustive list, likelihood ratings could be used to prioritise mitigation measures or the design of a CBDC security control framework for cyber risks. The impact on an organisation needs to be assessed using several organisation-specific factors that would influence the consequences of a risk if it were realised. It is assumed that cyber risk materialisation could have a high or very high impact across the organisation. Specifically, those threat events rated as very high or high in terms of likelihood, coupled with high or very high impact ratings, should be carefully considered if the organisation is adopting a risk-based security approach.

Fourth, cyber security needs to shift to cyber resilience, in the same way that Section 2 pointed to the need for business continuity to shift to operational resilience. CBDC is only one example of the level of bleeding edge innovation occurring in central banks today. Accordingly, the normally very conservative risk appetite of central banks is changing. The focus is shifting to the ability of an organisation to anticipate and withstand attacks, and to continue its critical operations during the response and recovery phases of a significant process/project. Hence the priority given to response and recovery processes, such as incident management.

Fifth, if a country's CBDC business model is closely reliant on the critical infrastructure (or third parties) of existing/alternative payment methods, a cyber security incident in relation to these common infrastructures (or third parties) may paralyse the entire payment system of the country. This would impact both CBDC and other payment methods at the same time. However, a CBDC business model that is distinct from the underlying infrastructure and processes of other payment methods may potentially provide heightened resilience, albeit at a non-trivial incremental cost.

4. Other relevant non-financial risks

Robust legal and compliance frameworks are crucial to facilitate the design, development, implementation and issuance of a CBDC. Early stakeholder engagement, together with ongoing communication, gap remediation and considered change management steps, will also increase the likelihood of success for a CBDC project.

Legal and compliance risks

As mentioned in Section 1, the national legal framework has important effects on how a CBDC can be set up.

Identified Legal Risks (non-exhaustive list) Table 18

Category	Identified risk	Processes	People	Systems	External event	Risk descriptions (based on a case or specific context)	Potential impacts	Other risks embedded
Legal risks	Limitations in legal frameworks		x		x	Incomplete legal frameworks can lead to a partial/ambiguous definition of legal responsibilities for stakeholders in CBDC; it can render prosecution of illicit activities or data privacy violations ineffective. Also, risks related to delays in required legislative amendments to operationalize CBDC.	• Certain design features of CBDC cannot be operated • Data privacy issues • Failures of processes • Legal costs • Reputational impact	Enterprise Operating Compliance
	Incompatibilities among different jurisdictions' legal frameworks for CBDC		x		x	Interlinkage between CBDC of different jurisdiction limited / constrained because of legal frameworks' incompatibilities.	• It could limit a CBDC's potential for cross border transactions and from acceptance by international platforms. • It could make CBDC less appealable /reliable, and therefore negatively affect its acceptance by the general public. • ICT and data protection issues	Enterprise Operating Compliance ICT/Cyber
	Inadequate definition of regulatory, supervisory and compliance frameworks for CBDC (considering third party participation)		x		x	Risks associated with local and non-domestic firms having a role within the CBDC ecosystem, while ensuring consistency with payments, financial regulation and trade agreements.	• Underperforming external dependencies • Non-compliance with financial regulations and trade agreements • Monetary sovereignty issues	Enterprise Operating Compliance ICT/Cyber Third-party

Source: CBDC Task Force

The two tables below highlight some important risks in the legal (Table 18) and compliance (Table 19) categories. Because of their close linkages, these categories will be discussed jointly.

Identified compliance risks (non-exhaustive list)

Table 19

Category	Identified risk	Processes	People	Systems	External event	Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
Compliance risks	Exploitation of existing vulnerabilities.		x	x	x	Gaps/weaknesses in legal or regulatory frameworks, financial and payment systems or the CBDC design could be exploited by threat actors to use CBDC for fraud, money laundering and other illicit activities, including CBDC double spending.	• Potential financial impact on central bank (cost of honoured claims for errors/frauds/illicit activities). • Reputational: diminished confidence in central bank by the public. • Problems related to financial system integrity. • Diminished CBDC adoption from public distrust or limitations on operationalising specific features.	Legal, Enterprise, ICT
	Potential data breaches of sensitive personal data.		x	x	x	Risk of large-scale breaches of data held by the system operator or intermediaries, regardless of the model chosen.	• Misuse of information causing reputational damage. • Breaches of data protection laws.	ICT, Legal, Enterprise

Source: CBDC Task Force.

From a risk management perspective, it is important to identify legal requirements and responsibilities for different stakeholders in a CBDC, since gaps could create legal and compliance risks (eg fraud, money laundering and other illicit activities), all of which can result in legal action. As many layers of domestic and international regulatory entities could be involved in a CBDC, it is relevant to recognise that changes to the law or regulatory environment could be lengthy and might affect projected timelines.

Further, data privacy violations could occur with respect to CBDC transactions and a proliferation of illicit actors. Enhanced data collection may create new data privacy and legal obligations for central banks, as transaction-level financial data may contain sensitive personal data. Whether the system is based on accounts or digital tokens, the design of a CBDC should consider the volume of personal information shared, and the risk of large-scale breaches of data held by the system operator or intermediaries. This may occur when the system is operating normally or in the event of disruptive scenarios.[91] In addition, in the absence of a robust legal framework, a central bank may face pressure from official sector actors to monitor individual data

[91] Auer and Böhme (2020).

transactions using CBDC.[92] To prevent abuse and ensure the accountability of authorities, central banks require legislation to protect institutional safeguards. For example, Jamaica's CBDC "JAM-DEX" requires a court order for information to be shared with other authorities.[93]

Gaps in CBDC legal frameworks may trigger financial and reputational risk. Processes and procedures to protect against duplicate or illicit transactions should be designed and potential liabilities allocated to specific owners. For example, offline use may diminish a central bank's real-time control of the validity or legitimacy of transactions (eg allowing transactions in remote areas with limited internet accessibility or during blackouts). Offline operations could thus expose central banks to fraudulent claims. Vulnerabilities may be related to the choice of technology (errors in DLT or CLT) or other design choices (which could be related to and/or impact specific features, such as anonymity, transaction volume, and data updates.

In terms of cross-border operations, the possible interoperability of CBDC systems would involve the interaction of local legal frameworks with foreign legal frameworks in areas such as the treatment of ICT, data and privacy, tax and payments, and capital flow management measures.

Potential mitigation strategies for legal and compliance risks

Any mitigation of legal and compliance risks needs to begin with an adequate analysis of the *legal framework to identify whether changes are necessary*. In parallel, project planning should involve consultations with third parties on the implementation of legal amendments related to the development of the CBDC project.

Another mitigation element is the *definition of standards* of compliance for the CBDC project, including those for third parties to avoid generating outsourced risks of fraud, money laundering and other illicit activities. Central banks should verify whether such standards are aligned with the central bank's existing standards or if current standards need to be adapted, in line with the central bank's risk appetite and to potentially coordinate with other jurisdictions to facilitate some degree of future interoperability. The standards should clearly define responsibilities for different participants and be accompanied by supervisory controls on activities such as customer due diligence, monitoring transactions and reporting suspicious transactions, amongst other obligations.[94] Of course, this relies on supervisory laws being designed to ensure that the central bank or another appropriate body has the authority to monitor/supervise, discipline and/or prosecute non-compliant actors.

Certain *design elements and choices* can also serve as mitigants for compliance risks. These include considering intermediated architectures to avoid keeping the data related to all transactions with the central bank, determining which data to keep private and from whom, using cryptographic techniques such as zero-knowledge proofs and operational arrangements such as operating limits for situations which

[92] Cecchetti and Schoenholtz (2022).

[93] Auer, Frost, Gambacorta, Monnet, Rice and Shin (2021)

[94] Auer, Haene and Holden (2021)".

could prove riskier to the central bank (offline connection, indirect models etc).[95] Some pilot CBDC projects, such as the PBoC's, are applying anonymity and transaction limits to accommodate different levels of user anonymity and access, by considering "there would be several grades of digital wallets based on the strength of the KYC levels, with stronger KYC requirements associated with higher transaction limits."[96]

Finally, *international cooperation* related to information from CBDC transactions is key, as it is with current financial transactions. Information flows contemplated in legal frameworks between countries could help authorities counter the illicit use of money, including tax evasion.[97]

Enterprise risk

Depending on the context faced by each central bank, enterprise risks can be considered strategic risks, as their impact can be substantial for a CBDC project, potentially even rendering the project unsuccessful.[98]

Central banks face enterprise risk as a result of having insufficient information about technologies and designs to adequately plan for a CBDC. Such risk also stems from an incomplete or inadequate assessment of its ecosystem features and their impacts on/relations to CBDC. As previously noted, the implementation of a CBDC requires design choices to be made and may involve the use of novel technologies. In this respect, a central bank should consider whether it has the skills and capacity necessary to develop, implement and operate a CBDC or whether and how it can acquire them. This includes allowing for future technological and governance changes at the enterprise level and considering the interactions between a CBDC and the current processes and operations of a central bank.

At the same time, much of the literature is focused on specific models and may not necessarily be applicable to a particular central bank's ecosystem. Accordingly, inaccurate or incomplete risk assessments based on dissimilar use cases and conditions from other – finished or ongoing – CBDC projects may lead to impaired adoption of a CBDC.[99] For example, in the absence of technological access and digitalisation, a society could not widely adopt CBDC.

[95] Auer and Böhme (2020) and Darbha and Arora (2020).

[96] Auer et al (2023).

[97] Soderberg et al (2022).

[98] In general, a CBDC that does not operate robustly may expose the central bank to reputational risks. It follows that risks in other categories, as described in Sections 2 to 4, can also become strategic/enterprise risks.

[99] Note that inadequate interpretation of ecosystem features and/or errors in the decision-making process can also be linked to model risk, as the chosen CBDC model might not be fit for the circumstances in which the central bank operates.

Identified enterprise risks (non-exhaustive list)

Table 20

Category	Identified risk	Processes	People	Systems	External event	Risk descriptions (based on a case or specific context)	Potential impacts	Other embedded risks
Enterprise risks	Incomplete or inadequate communication by the central bank with stakeholders.		x			Incomplete or inadequate communication with stakeholders (intermediaries, public, government etc) about the objective of the CBDC project and does not incorporate different perspectives in analysing a CBDC project or its potential impact on the payment and financial systems.	• An inappropriate communication plan is likely to result in instability for the stakeholders and financial actors. • Potential resistance from the banking sector to CBDC issuance, from the general public to adopting CBDC, from other authorities to make necessary legal changes etc. • Reputational and relational damage to the central bank. • Costs and delays to CBDC implementation/operations.	Operating, ICT/cyber, Legal, Third party
	Inappropriate CBDC design decision-making process.	x				Weak design of CBDC, as described in Section 1, such as offline, cross-border, direct/intermediated model etc.	• CBDC adoption impaired. • Failing to accomplish CBDC's objective. • Reputational. • Ineffective CBDC project governance. • Costs and delays to CBDC.	Operating, ICT/cyber, Legal, Third party
	Inadequate interpretation/erroneous consideration of external conditions' impact on CBDC projects.	X	x	x	x	Ecosystem features, as described in Section 1, such as level of maturity (financial, technological, digitalisation), financial literacy, natural conditions, rule of law etc, have a strong influence on a CBDC project's success.	• CBDC adoption impaired. • Failing to accomplish the goals of the CBDC project. Reputational.	Operating, ICT/cyber, Legal, Third party

Source: CBDC Task Force.

A strong commitment to the CBDC by the issuing central bank, including robust and timely communication with all stakeholders, will be critical to constructing and maintaining trust in the CBDC. In turn, this is critical to its broad acceptance. Thus, central banks need to enhance confidence in a CBDC through mitigation strategies based on effective ORM models and timely communications.[100]

[100] Errors related to understanding and/or implementing these ORM models can be a source of model risk for the CBDC project. Such errors may impact the inherent and residual risk profiles of a central bank.

ESG risk

From an IRM framework perspective for CBDC, the assessment of design features should incorporate environmental considerations, including physical and transition risks and opportunities related to CBDC. These can include considerations such as power consumption needs, the environmental impact of "use and discard" features and their linkage to carbon neutral initiatives. For example, certain technologies and schemes, such as DLT and particularly proof of work schemes, involve a high level of energy consumption "since every batch of transactions needs to be accompanied by a proof that a substantial quantum of otherwise useless computations has been performed."[101]

Further, a CBDC project will face social aspects, stemming from and impacting the ecosystem or external factors mentioned in Section 1, such as those relating to financial inclusion. In terms of governance risks, CBDC projects should consider those inherited from the central bank and those embedded in the CBDC project itself. Weak or less mature institutional governance frameworks might expose central banks to greater difficulties in respect of achieving their goals for a CBDC.

In this respect, key aspects for central banks wishing to implement a CBDC project are not just linked to technical issues, but also to cultural ones.[102] As organisational and cultural aspects may impact or even hamper a CBDC project, these aspects should be analysed and research on specific impacts on local culture and on the central bank should be conducted. The implementation of a proof of concept or a pilot may provide an opportunity to study the behaviour and cultural elements that will need to be managed.

Project risk

Once the design, operating model and its features are defined, the organisation and management of the *project lifecycle* is crucial for contributing to the success of CBDC implementation and deployment. Robust and resilient CBDC operations will be facilitated by the appropriate identification and management of risks throughout the stages of a CBDC project, as discussed in Sections 2 to 4.

[101] Auer, Frost, Gambacorta, Monnet, Rice and Shin (2021).

[102] Soderberg et al (2022).

Potential impacts on central banks of CBDC project risks Table 21

Potential impacts of project risks
• Stress on organisational culture.
• Business model scope and definition.
• Existing roles and responsibilities at value chain level, not just project level.
• Internal staff: modifying their current functions or responsibilities or incorporating new skills and team capabilities for CBDC.
• Budget prioritisation by the central bank.
• ICT and security framework.
• Cyber security standards.
• Third-party agreements, roles and responsibilities may change depending on the outcome of the project.
• Business continuity scope and capabilities.
• Current payment system and processes.
• Existing currency cycle.

Source: CBDC Task Force.

While project risks might be considered a second-order priority for CBDC projects, the *Principles for financial market infrastructures*[103] emphasises that the board of a central bank should closely monitor its risk profile to ensure a balance between risk appetite and tolerance. This means ensuring appropriate project management of financial infrastructure for all existing risks, as well as any risks arising from process changes, new products or new services that modify the risk profile.

Due to the complexity of operational risks, irrespective of whether they are mitigated internally or externally, it is important to highlight that CBDC projects use best practices to ensure the effective management of complex projects. For instance, The World Bank proposes several considerations for financial infrastructure projects.[104] It highlights practices such as establishing a specific, dedicated team for the project's end-to-end and daily management due to the number of decisions and the quantity of execution work needed. This team might manage the project as a separate business unit to ensure strong project management that is supported by well defined and monitored processes, procedures, an IRM framework, budgets and standards. Note that the definition and application of standards should be performed from the early stages of the project design in order to boost effectiveness and efficiency, and balance them with risk appetite.

The complexity of the CBDC project will increase when a cross-border scope is incorporated because different jurisdictional standards could directly impact the legacy payment systems. This should be considered during the project development stage to mitigate OR, as discussed in the sections above.[105]

[103] CPSS-IOSCO (2012).

[104] World Bank (2014).

[105] BIS, CPMI, BIS Innovation Hub, IMF and World Bank Group (2021).

The standards for a CBDC project could rely on organisational definitions, however, consideration of market best practices and project management methodologies is strongly recommended.[106]

Example of the practical application of an IRM framework to a CBDC assessment

Graph 15 provides an example of the application of the IRM framework proposed in this document to a CBDC assessment. The results are not based on real data. Rather, they are intended to show the steps to follow in practice and the potential results of an assessment of this type. While in this instance the framework is applied to just one risk category (ICT/cyber security) applications to other risk categories would follow the same path.

Graph 15 shows the assessment and mock results of a CBDC, considering:

1. **External factors:** these include ecosystem features and operational skills and capabilities, as mentioned in Section 1.

2. **Internal factors:** these include general design features that represent decisions of the central bank about a particular CBDC project, as mentioned in Section 1.

   Assessment of internal and external factors is the first step to an IRM assessment for CBDC, as these factors will impact all risk categories described in Table 2.

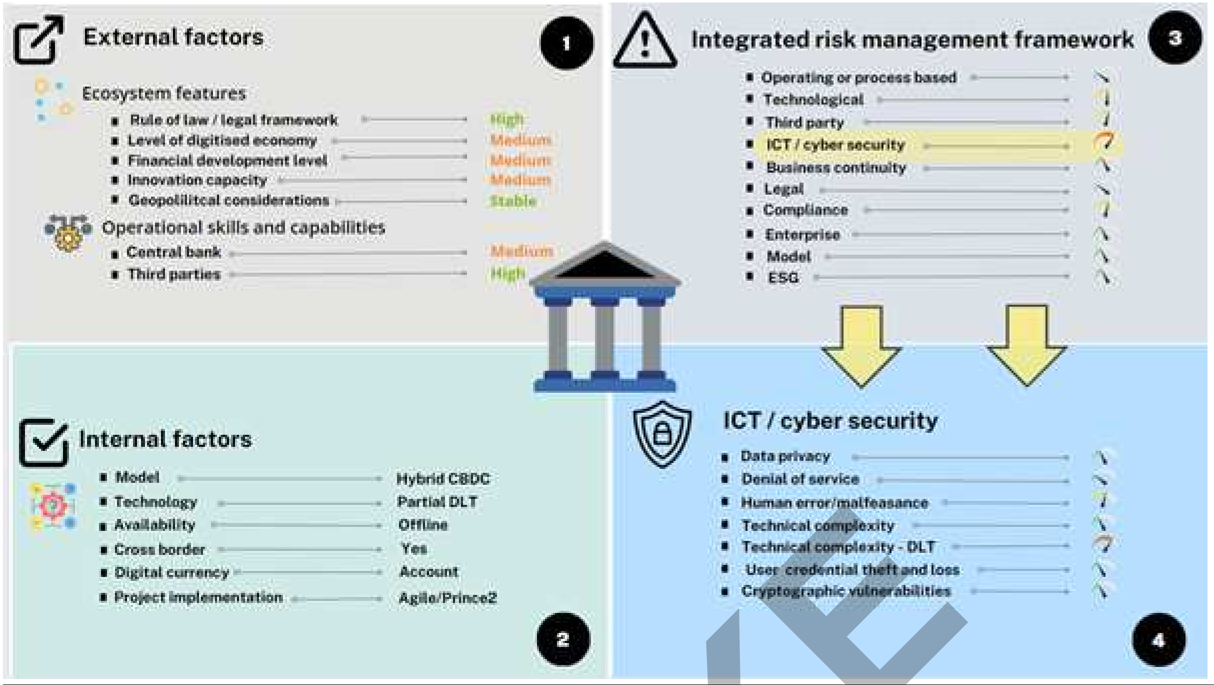
3. **Risk assessment (mock) results for the ICT/cyber risk category:** the assessment is based on the risk methodologies and relevant risks mentioned in this document are shown in the mock results. While not prescriptive or comprehensive, the risks outlined throughout the document and potential mitigation strategies for each risk category can help central banks to perform this assessment.

4. **Results for the IRM assessment of a CBDC:** this provides an example of an IRM assessment for a CBDC, considering all risk categories described in the document.

[106] The standards should be managed in a clear project framework established by the central banks to facilitate the project organisation and management under a specific methodology – whether traditional waterfall methodologies, agile methodologies or a combination thereof.

Steps and potential results/output of IRM assessment for CBDC

Graph 15



Sources: CBDC Task Force

Box 4

Central bank profile – IRM assessment for CBDC issuance

In the following example the central bank of a country with a strong market economy, relatively high household income and per capita GDP for the region would like to issue a CBDC. The rule of law is strong and the country has made significant investments in digitisation as well as putting in place incentives to attract private sector investment in technology. Domestic levels of competitiveness, income per capita, and economic openness and freedom have been increasing steadily and consistently for years.

The IT and information skills within the central bank are adequate for maintaining legacy systems but the bank would need to rely on external vendors to assist with innovation opportunities, as well as the integration and operation of novel technology (eg DLT).

Conclusions

A large number of countries are currently conducting CBDC research, pilots or proofs of concept and a few have working implementations. CBDC models vary widely in terms of reference architectures, technologies, options for availability (online/offline), system scopes (local or cross-border) and security (token or account based). External factors, such as the level of digitalisation, financial development and innovation capacity, as well as the skills and capabilities within a jurisdiction, also play a key role in shaping the scope and design of CBDC projects. These factors may impact CBDC strategy and project governance decisions. Therefore, it is important that central banks consider internal and external factors, and perform robust risk analyses as part of the process of determining design choices that fit their respective risk appetites and deliver the required functionality. Such risk analyses are to be based on the objectives and defined use cases for a CBDC in the particular jurisdiction.

As described in this document, central banks should pay particular attention to adopting a timely and comprehensive risk management framework and plan related to all risk categories. This must enable the proper evaluation of CBDC-related design choices and associated features to be conducted.

Our main conclusions can be summarised in the following points.

1. Issuing a CBDC will have major implications for the business model of central banks and the risks they face, modifying their risk profiles.

The introduction of a CBDC will have major effects on a large range of central bank processes and policies. It also exposes the central bank to a variety of risks that are likely to change as the CBDC project moves through its various stages. Introducing a CBDC thus requires the regular identification, assessment, monitoring and reporting of risks and potential mitigants, as described in this report. This process helps to align the project with the risk appetite of the central bank. Moreover, due to the high impact on many central bank processes and standards, a CBDC project may be conceived as a new business model and not just a technological project.

2. Taxonomies and frameworks for integrated risk management analyses are essential.

Design choices will depend on the particular motivation and use cases for a CBDC as well as country-specific ecosystem factors. This means that the design and risks posed by a CBDC will vary across countries. The multifaceted nature of the risks call for an IRM framework to inform the design of a CBDC model and the management of risks throughout its lifecycle.

3. Central banks need to assess all risk categories as part of an integrated risk management framework and develop associated mitigation strategies.

The IRM framework provides a list of CBDC-relevant risk categories. The literature highlights four categories for OR – operating, technology, third-party and business continuity risks. However, central banks should go beyond these categories and perform their own risk mapping exercises to identify additional risks. Mitigation strategies can be based on a wider variety of risk models, including also information and communication technology (ICT) risk management (incorporating cyber security), project risk, and compliance risk management.

4. Central banks should evaluate potential gaps in their internal capabilities and skills.

Potential gaps in skills and capabilities for the implementation a CBDC, throughout the different project stages, is a key risk identified in this report. Central banks should perform careful and realistic assessments in this respect, including with regard to their ability to develop skills internally. These assessments will help determine whether CBDC-related activities could be performed internally or would potentially need to be outsourced to third parties. Therefore, the evaluation should also assess the risks of outsourcing, eg technological lock-in or vendor risks. Supervisory capabilities should also be in place to undertake appropriate due diligence related to CBDC processes.

5. Operational and cyber security resilience is crucial.

For CBDC to be a reliable means of payment, central banks need to address the risk of interruptions or disruptions, and ensure integrity and confidentiality. This requires the development of robust business continuity plans to ensure the reliability and continuity of services in the event of possible scenarios and threats throughout the full (digital) currency cycle. The approach should move to an operational resilience model due to the multiple scenarios that central banks are exposed to and the increased frequency of ICT threats. This would position cyber security as a vital consideration in a CBDC project. Thus, operational resilience requires the integration of BCP, ICT risk management and third-party risk management models (see Graph 11), to create a unique resilience framework for CBDCs. This should form a key part of central banks' integrated risk management frameworks.

In order to fulfil central banks' objectives and mandates, operational resilience should be preventative and predictive – incorporating processes to detect, withstand and recover all identified critical assets. It should also protect these assets in the event of a threat to the confidentiality, integrity and/or availability of CBDC. Should a major event occur, resilience models enable the central bank to recover and build-up capabilities and capacities to control and/or mitigate any undesirable impacts on financial stability.

Furthermore, the possible choice of novel technologies, the risks of which are not yet fully understood, is a particular focus of attention for central banks. Specifically, although several existing cyber security frameworks can be adapted to cover a CBDC, there is no widely accepted cyber security framework that addresses the integration of DLT, digital identities, immutable data and smart contracts. This is because reference architectures using these technologies are still evolving.

CBDCs pose both opportunities and challenges. On the one hand, they have the potential to drive innovation, promote financial inclusion and create an environment that enables the next generation of payment application and digital business models. On the other hand, the many design options available to central banks require careful identification of the inevitable trade-offs between adoption, performance, interoperability, privacy and security. Such trade-offs need to be addressed and this can only be accomplished in a meaningful way if the risks are well understood and managed. In our view, an approach that considers the application of an integrated risk management framework to the implementation of CBDC would be a useful tool to identify, measure, mitigate and monitor associated risks.

References

Aldasoro, I, L Gambacorta, P Giudici and T Leach (2020): "The drivers of cyber risk", *BIS Working Papers,* no 865, May.

Alonso V, Tombini A and Zampolli F (2020): "Retail payments in Latin America and the Caribbean: present and future", *BIS Quarterly Review,* December.

Appendino, M, O Bespalova, R Bhattacharya, J Clevy, N Geng, T Komatsuzaki, J Lesniak, W Lian, S Marcelino, M Villafuerte, Y Yakhshilikov (2023): "Crypto assets and CBDCs in Latin America and the Caribbean: opportunities and risks", *IMF Working Papers*, no 37, February.

Aquilina, M, J Frost, A Schrimpf (2023): "Addressing the risks in crypto: laying out the options", *BIS Bulletin*, no 66, January.

Arauz, A, R Garratt and D Ramos (2021): "Dinero Electrónico: the rise and fall of Ecuador's central bank digital currency", *Latin American Journal of Central Banking*, vol 2, no 2.

Auer R, H Banka, N Boakye-Adjei, A Faragallah, J Frost, H Natarajan and J Prenio (2022): "Central banks digital currencies: a new tool in the financial inclusion toolkit?", *FSI Insights*, no 41, April.

Auer, R and R Böhme (2020): "The technology of retail central bank digital currency", *BIS Quarterly Review*, March, pp 85–100, www.bis.org/publ/qtrpdf/r_qt2003j.htm.

——— (2021): "Central bank digital currency: the quest for minimally invasive technology", *BIS Working Papers*, no 948.

Auer, R, G Cornelli and J Frost (2023): "Rise of the central bank digital currencies: drivers, approaches and technologies", *International Journal of Central Banking*, forthcoming.

Auer, R, J Frost and L Gambacorta, C Monnet, T Rice and H S Shin (2021): "Central bank digital currencies: motives, economic implications and the research frontier", *BIS Working Papers*, no 976, November.

Auer, R, G Cornelli and J Frost (2023): "Rise of the Central Bank Digital Currencies", International Journal of Central Banking, forthcoming.

Auer, R, P Haene and H Holden (2021): "Multi-CBDC arrangements and the future of cross-border payments", *BIS Papers*, no 115, March.

Amazon Web Services (AWS) (2021): *Central bank digital currency (part 1): objectives and architectural considerations*.

Bank for International Settlements (BIS) (2021): "Central bank digital currencies: an opportunity for the monetary system", *Annual Economic Report 2021*, Chapter III, June.

——— (2022): "CBDCs in emerging market economies", *BIS Papers*, no 123, April.

——— (2023): *Information and Technology Risk Policy, Rule of Limited Application*, BIS internal policy, unpublished.

Bank of Canada (2020): *Contingency planning for a central bank digital currency*, February.

Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve System and BIS (2020): *Central bank digital currencies: foundational principles and core features*, October.

Bank of England (2017): *A blueprint for a new RTGS service for the United Kingdom*, May 2017.

——— (2018): "Building the UK financial sector's operational resilience", *Discussion Papers*, no 1, July.

——— (2020): "Central bank digital currency opportunities, challenges and design", *Discussion Paper*, March.

Basel Committee on Banking Supervision (BCBS) (2005): *Outsourcing in financial services*, February.

——— (2010): *Principles for enhancing corporate governance*, October.

——— (2017): *Basel III: finalising post-crisis reforms*, December, www.bis.org/bcbs/publ/d424.pdf.

——— (2021a): *Principles for the sound management of operational risk*, March.

——— (2021b): *Revisions to the principles for the sound management of operational risk*, March, www.bis.org/bcbs/publ/d515.pdf.

——— (2021c): *Principles for operational resilience*, March.

Bech, M, C Boar, D Eidan, P Haene, H Holden and W Toh (2022): *Using CBDCs across borders: lessons from practical experiments*, BIS Innovation Hub, June.

Bilotta, N and F Botti (2021): *The (near) future of central bank digital currencies*, Peter Lang International Academic Publishers.

Bindseil, U, P Fabio and I Terol (2021): "Central bank digital currency: functional scope, pricing and controls", *European Central Bank Occasional Paper Series*, no 286, December.

BIS, Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve System (2021): *Central bank digital currencies: financial stability implications*, September.

BIS, Committee on Payments and Market Infrastructure (CPMI), BIS Innovation Hub, International Monetary Fund and the World Bank Group (2021): *Central Bank digital currencies for cross-border payments*, July.

BIS Innovation Hub (BISIH) Hong Kong Centre, the Hong Kong Monetary Authority, and the Hong Kong Applied Science and Technology Research Institute (2022): *Project Aurum: a prototype for two-tier central bank digital currency (CBDC),* October.

BISIH, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates (2022): *Project mBridge: connecting economies through CBDC*, October.

——— (2021): *Inthanon-LionRock to mBridge: building a multi CBDC platform for international payments*, September.

Boar, C and A Wehrli, (2021): “Ready, steady, go? – Results of the third BIS survey on central bank digital currency”, *BIS Papers*, no 114, January.

Board of Governors of the Federal Reserve System (2022): *Money and payments: the US dollar in the age of digital transformation*, January.

Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (2021): “Proposed interagency guidance on third-party relationships: risk management”, *Federal Register*, vol 86, no 135, July.

Cawthra J, M Ekstrom, L Lusty, J Sexton, J Sweetnam, A Townsend and The MITRE Corporation (2020): “Data integrity: detecting and responding to ransomware and other destructive events, executive summary”, *NIST Special Publications*, no 1800-26A.

Cecchetti, S and K Schoenholtz (eds) (2021): “Central bank digital currency: considerations, projects, outlook”, *CEPR Press*, pp 57–63.

Cecchetti, S and K Schoenholtz (2022): *Central bank of digital currency: is it really worth the risk?*, January.

Central Bank of The Bahamas (2019): “Project Sand Dollar: a Bahamian payments system modernisation initiative”, December.

Chu, Y, J Lee, S Kim, H Kim, Y Yoon and H Chung (2022): “Review of offline payment function of CBDC considering security requirements”, *Applied Sciences*, vol 12, no 9.

Committee on Payments and Market Infrastructures and Markets Committee (CPMI-MC) (2018): *Central bank digital currencies*, March.

Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (CPSS-IOSCO) (2012): *Principles for financial market infrastructures*, April.

Consultative Group on Risk Management (CGRM) (2022): *Business continuity planning at central banks during and after pandemic*, April.

Darbha, S and R Arora (2020): “Privacy in CBDC technology”, *Bank of Canada Staff Analytical Notes*, no 9.

Denecker, O, A d’Estienne, P-M Gompertz and E Sasia (2022): *Central bank digital currencies: an active role for commercial banks*”, McKinsey & Company.

European Banking Authority (EBA) (2019): *Guidelines on ICT and security risk management,* November.

Eastern Caribbean Central Bank (ECCB) (2022): “Region-wide service interruption of Dcash platform”, 14 January, www.eccb-centralbank.org/news/view/region-wide-service-interruption-of-dcash-platform.

English, E (2021*): Finding a secure solution for offline use of central bank digital currencies (CBDCs)*, *Visa Economic Empowerment Institute*, March.

European Commission (2020): “Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014”
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

Fanti, G, K Kostiainen, W Howlett, J Lipsky, O Moehr, J Schnapper-Casteras and Josephine Wolff (2022): *Missing key: the challenge of cybersecurity and central bank digital currency*, Atlantic Council, June.

Fanti, G, J Lipsky and O Moehr (2022): "Central bankers' new cyber security challenge", *IMF Finance & Development*, September.

Financial Stability Board (FSB) (2023): *Cyber lexicon*, April.

Financial Stability Institute (FSI) (2015): "The 'four lines of defence model' for financial institutions", *FSI Occasional Papers*, no 11.

Hansen, T and K Delak (2022): "Security considerations for a central bank digital currency", *FEDS Notes*, February.

House of Lords Economic Affairs Committee (HLEAC) (2022): "Central bank digital currencies: a solution in search of a problem?", *HL Paper*, no 131, January.

IBM (2021): "IBM Security X-force threat intelligence index 2021".

International Standards Organization (ISO) (2018): *ISO 31000:2018 risk management – guidelines*.

——— (2019): *ISO 22301:2019 security and resilience – business continuity management systems – requirements*.

——— (2022): *ISO 22361:2022 security and resilience – crisis management – guidelines*.

Margulies, B (2022): "Pilot CBDC outage due to expired certificate, ECCB says", *Central Banking*, 3 February.

Microsoft (2022): *Microsoft threat modeling tool threats*, https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Minwalla, C (2020): "Security of a CBDC", *Bank of Canada Staff Analytical Notes*, no 11, June.

Minwalla, C, J Miedema, S Hernandez, A Lalani-Sutton (2023): "A central bank digital currency for offline payments", *Bank of Canada Staff Analytical Notes*, no 2, February.

National Institute of Standards and Technology (NIST) (2012): "Guide for conducting risk assessments: information security", *NIST Special Publications*, no 800-30, revision 1.

——— (2020): "Security and privacy controls for information systems and organizations", *NIST Special Publications*, no 800-53 revision 5.

——— (2023): *Glossary*, last updated 13 April, https://csrc.nist.gov/glossary.

Office of the Superintendent of Financial Institutions (Canada) (2021): "Third-party risk management guidelines", no B–10, www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx.

Oliver Wyman and AWS (2022): *Retail central bank digital currency: from vision to design: a framework to align policy objectives and technology design choices*, March.

Operational Risk Consortium (ORIC) International and McKinsey & Company (2017): *Improving third-party risk management*, October.

Organisation for Economic Co-operation and Development (OECD) (2022): "Lessons from the crypto winter: DeFi versus CeFi", *OECD Business and Finance Policy Papers*.

Parker, D, J Charlton, A Ribeiro and R Pathak (2013): "Integration of project-based management and change management: Intervention methodology", *International Journal of Productivity and Performance Management*, vol 62, no 5, pp 534–44.

Sarmiento, A (2022): "Seven lessons from the e-peso pilot plan: the possibility of a central bank digital currency", *Latin American Journal of Central Banking*, vol 3, no 2.

Soderberg, G, M Bechara, W Bossu, N Che, S Davidovic, J Kiff, I Lukonga, T Mancini-Griffoli, T Sun and A Yoshinaga (2022): "Behind the scenes of central bank digital currency: emerging trends, insights, and policy lessons", *IMF Fintech Notes*, February.

Sultanik, E and M Myers (2022): "Do you really need a blockchain? An operational risk assessment", *Trail of Bits*.

Sveriges Riksbank (2022): *E-krona pilot phase 2*, April.

World Bank (2014): *Guidelines for the successful regional integration of financial infrastructures*, January.

World Bank Group (2021): *Central bank digital currencies for cross-border payments: a review of current experiments and ideas*, November.

World Economic Forum (WEF) (2021): "CBDC technology considerations", *Digital Currency Governance Consortium White Papers*, no 8, November.

World Intellectual Property Organization (WIPO) (2018): *Global innovation index 2018: energizing the world with innovation*, July.

Annex – Members of the CBDC Task Force set up by the Consultative Group on Risk Management of central banks in the Americas

Central Bank of Brazil	Luiz Antonio Valente Deputy Head of Corporate Risk Division
Bank of Canada	Luc Demers Senior Compliance Specialist, ITS
	Karim McDaniels Senior Analyst, Enterprise Risk Office
	Cyrus Minwalla Security Lead
Central Bank of Chile	Diego Ballivián (Task Force leader) Chief Risk Officer
	María Jesús Orellana (Workstream leader) Operational Risk Manager
Central Bank of Colombia	Julio Álvarez Head of Information and Cyber Security
	Erika Herrera Head of Risk and Processes Department
Bank of Mexico	Antonieta Campa (Workstream leader) Manager, Risk Strategy and Project Management Division César Ortega Manager, Monitoring Division Carlos Arias Deputy Manager, Specialised Risks and Business Continuity Subdivision
Federal Reserve Bank of New York	Li He Portfolio Risk and Valuation Team in the Risk Group
	Pablo Azar Research Economist in Money and Payments Studies Function
Bank for International Settlements	Steffen Grosse Senior Operational Risk Manager
	David Whyte (Workstream leader) Head of Cyber Resilience Coordination Centre

	Christian Upper (Secretariat) Senior Adviser
	Jesse Johal (Secretariat) Visiting Economist