BIS Innovation Hub

Project Polaris

Part 2: A security and resilience framework for CBDC systems

July 2023

In parternship with:

BIS Cyber Resilience Coordination Centre

Contents

This framework was quality assured by PA Consulting:

1. Executive summary

Cyber attacks on critical infrastructure are amongst the top five risks that could have the greatest impact on a global scale.[1] Central bank digital currency (CBDC) systems would be considered a critical national infrastructure, much like real-time gross settlement (RTGS) systems are today.

Cyber attacks typically occur across a spectrum of complexity, from simple and opportunistic (such as malware targeting personal data), to much more sophisticated (such as advanced persistent threats (APTs)).

Rapid growth in the digital environment and in the interconnectedness between parties and devices relying on the internet and telecommunications networks for various purposes has created a diverse and complex cyber threat landscape[2] which continues to evolve rapidly; for example, AI-assisted attacks are becoming more common.

In addition, with the increasing prevalence of cyber-physical systems (physical systems that are integrated with online systems), which are commonly known as devices that form the Internet of Things and which include consumer devices (for example smartphones, smart TVs, wearables, etc) or industrial components, cyber attacks can spill over from the digital to the physical space. The volume of connected cyber-physical devices is expected to be around 29.4 billion by 2030[3] and some of these may be used in retail scenarios, creating a large attack surface.

CBDCs could be used to provide functionality such as programmability, which could facilitate conditional and automated payments in potential use cases such as delivery vs payment, machine-to-machine payments between consumer devices, or for industrial automation. Any vulnerabilities could affect these transactions or cyber-physical devices and leave them open to breaches, criminal activity and physical manipulation.

CBDC systems could use new technologies, some of which are as yet unproven at the scale and critical operations demands that would be required, and therefore could introduce new security and operational risks.

Central banks and other actors in a CBDC ecosystem[4] will need to face up to this increasingly complex cyber threat landscape, comprised of unpredictable threat actors, new threats, a large attack surface and points of failure, supply chain risks and an environment where the potential upside for a threat actor could be high.

[1] See World Economic Forum (2023).

[2] See Doerr et al (2022) for survey results on cyber threats and central banking.

[3] See Statista (2022) for more details about the number of Internet of Things (IoT) connected devices worldwide.

[4] A CBDC ecosystem refers to the various public and private sector actors participating in a CBDC system.

A breach of a CBDC system due to cyber attacks or technical failures could erode confidence and trust in the CBDC system, the central bank, and potentially the financial system, in addition to generating a range of reputational, operational and potentially legal impacts.

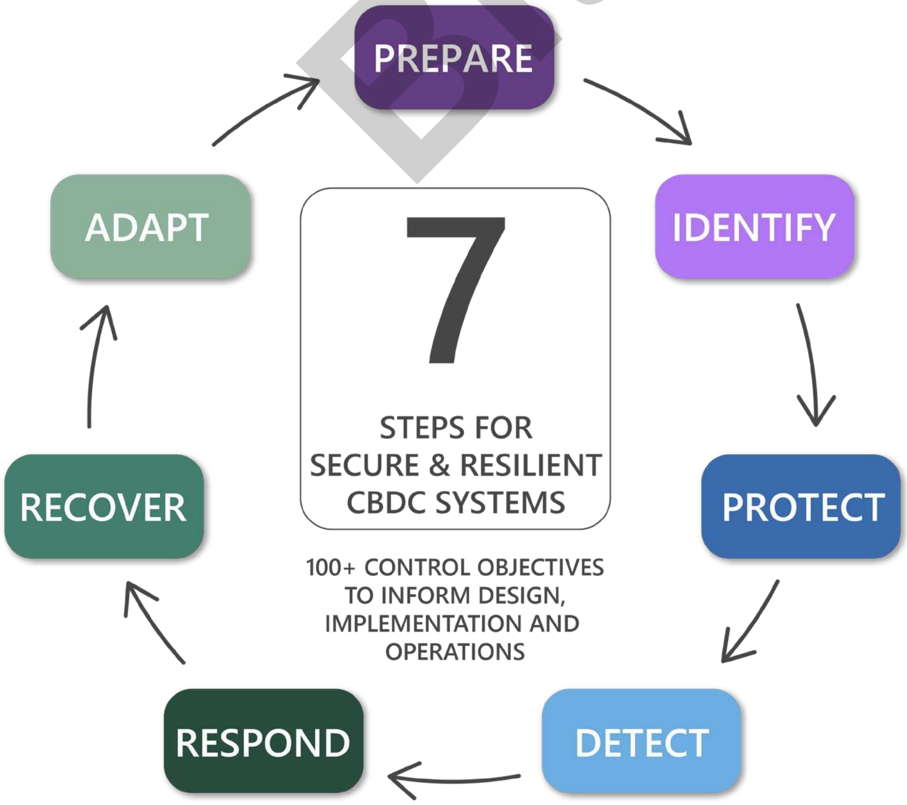
Retail CBDC systems must be highly secure and resilient. Central banks are at various stages of their work on retail CBDC, and as this progresses it is important that security and resilience be considered at the earliest possible stage.

Many central banks already have robust cyber security and resilience measures in place and adhere to the highest of industry standards in controls and risk management. However, risks cannot be fully eliminated and it is critical that senior leadership be aware of the potential new and elevated level of threats and risks facing CBDC systems so an appropriate risk management and mitigation strategy can be established.

The Polaris security and resilience framework has been developed to guide central banks in designing, implementing and operating secure and resilient CBDC systems to mitigate the operational, legal and reputational risks facing central banks from cyber threats or operational failures.

This framework is CBDC-focused and leverages existing industry standards and guidelines, providing central banks with a seven-step model, as shown in Figure 1, for secure and resilient CBDC systems.

Figure 1: The seven steps for secure and resilient CBDC systems



Specifically, central banks could use the framework to:

- Recognise the complexity and new threat landscape brought by CBDC systems;
- Adopt modern enabling technologies supporting security and resilience where appropriate;
- Take stock of existing capabilities that could be leveraged for a CBDC system;
- Identify the capabilities that need to mature;
- Identify new capabilities that would need to be implemented.

The framework is a baseline and is intended to be updated periodically, keeping pace with any developments related to CBDC systems and the cyber threat landscape, in partnership with the central bank community as well as the public sector and private entities that could participate in a CBDC ecosystem.

2. Acronyms and abbreviations

AI	Artificial intelligence
AML	Anti-money laundering
API	Application programming interface
BCP	Business continuity plan
BIA	Business impact analysis
BIS	Bank for International Settlements
BIS CPMI	BIS Committee on Payments and Market Infrastructures
B2B	Business to business
CBDC	Central bank digital currency
CERT	Computer emergency response team
COTS	Commercial off-the-shelf software
DeFi	Decentralised finance
DLT	Distributed ledger technology
DNS	Domain name system
ENISA	European Union Agency for Cybersecurity
FI	Financial intermediary
FMI	Financial market infrastructure
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information technology
KYC	Know-your-customer
NIST	National Institute of Standards and Technology
PSP	Payment service provider
RPO	Recovery point objective
RTGS	Real-time gross settlement
RTO	Recovery time objective
SEI	Software Engineering Institute
SIEM	Security information and event management
SOC	Security operations centre

3. Introduction

A central bank's journey with central bank digital currency (CBDC) typically starts with research and proof of concept activities.[5] These typically focus on functional capabilities such as issuance and transfer of CBDCs. For a CBDC system to be truly production-ready, it will require robust understanding and implementation of both functional and non-functional capabilities.

Payment systems are a target of cyber attacks. For example, the attack on Bangladesh Bank in 2016 involved hackers compromising a user's workstation and sending fraudulent payment instructions via the SWIFT network.[6] The multiple large-value decentralised finance (DeFi) breaches in 2022 are an example of what could go wrong when new technologies are used without proper security safeguards.[7,8]

Threat actors against payment systems and central bank systems could include nation states, organised crime groups, cyber criminals, insiders and hacktivists, among others.

Design flaws, supply chain vulnerabilities and weakness in underlying operating infrastructure could be leveraged by threat actors to compromise systems for a range of reasons including economic disruption, financial gain, to sow distrust and fear or to damage the reputation of a central bank.

CBDC systems will need to remain highly resilient in a broad range of scenarios, including short-term (such as temporary system outages), ongoing situations (such as in areas without reliable internet, telecommunications connectivity or power), or civil contingency conditions (such as natural disasters or war),[9] besides being highly responsive in normal operations.

Digital transformation trends have brought new opportunities for security and resilience, but also come with their own challenges which would need to be understood and assessed. For example, cloud computing platforms can provide more computing resources and data centre locations and therefore potentially better resilience, but could also increase the risk of data exposure if not managed properly.

As technology and the cyber security threat landscape continue to evolve, CBDC systems as well as all the actors in a CBDC ecosystem will need to adapt to new and emerging threats and implement and apply robust risk, change and operational management processes.

[5] See Kosse and Mattei (2022) for results from a recent BIS survey.

[6] World Informatix Cyber Security (2021) contains a detailed description of this incident and how SWIFT has since worked with its user community to strengthen cyber security.

[7] See BISIH (2023c).

[8] The lack of proper safeguards or understanding of systems using current technologies is also a challenge.

[9] These resilience scenario categorisations are set out in the handbook for offline payments also developed as part of Project Polaris (BISIH (2023a)).

The Polaris framework has been developed to enable central banks to manage CBDC-related security and resilience risks, considering the threat landscape, the challenges and opportunities presented by new and emerging technologies, and an evolving technical and business environment.

The framework could also help central banks assess their cyber security and resilience maturity level as it stands today as compared with what could be required when operating a CBDC system, by assessing and ranking how the organisation adheres to the practices outlined in this framework.[10] This could help inform requirements and planning for implementing or improving capabilities at each phase of a CBDC system implementation or in live operations.

The Polaris framework makes several assumptions about a future CBDC ecosystem, including the potential complexities, challenges and risks this could bring. The criteria and threat landscape considered when developing this framework and its building blocks are also described. These assumptions are discussed in detail in Section 4.

Each of the seven steps in the framework is discussed in Section 5, with guidance for how central banks can use the framework provided in Section 6.

Over one hundred control objectives, detailed in Appendix A, could be used as a guide to aid the implementation of the necessary security and resilience capabilities for developing and operating CBDC systems. Central banks could choose to adopt some of the enabling technologies and techniques for security and resilience, as described in Appendix B. They may also identify additional capabilities that could be required that are not currently detailed in this framework.

The seven-step framework is an iterative process, by which central banks should periodically review their preparedness for moving to the next phase of their CBDC journey, identify new threats and requirements, ensure their prevention, detection and response controls are still effective, and adapt their security and resilience measures accordingly.

[10] The NIST cyber security framework (NIST (2018)) outlines four tiers for assessment and ranking, which could also be used.

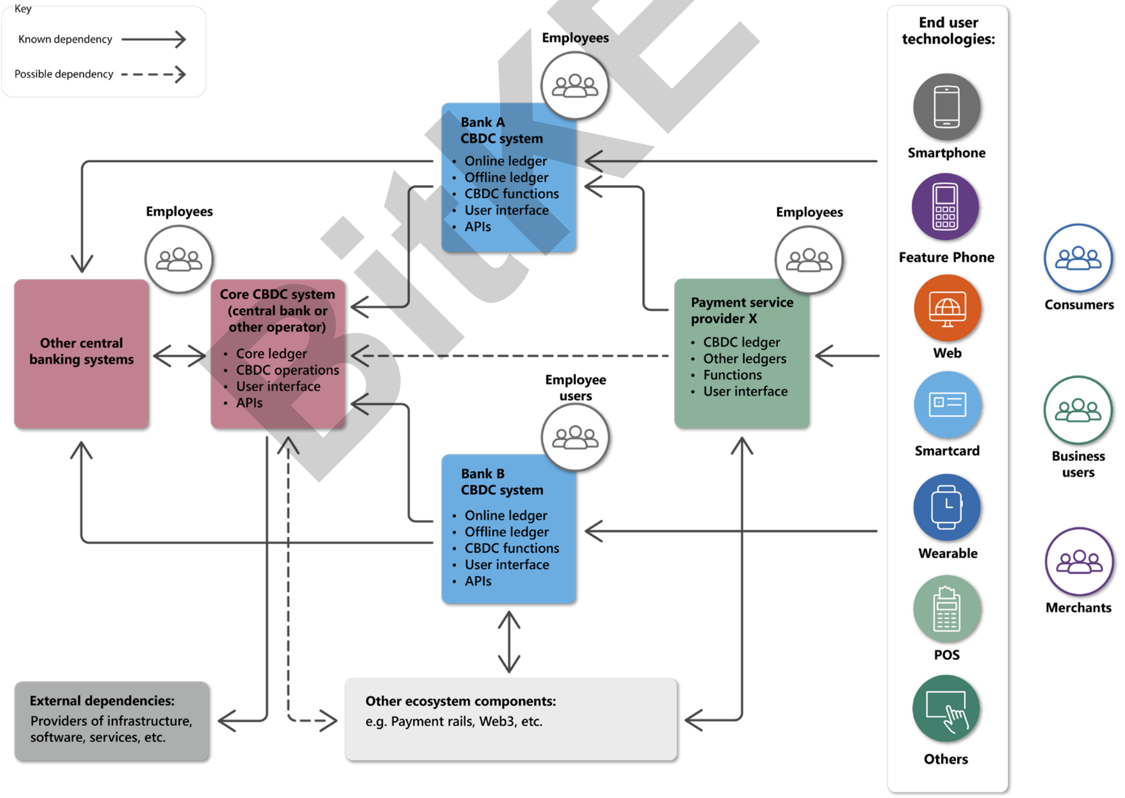
4. Assumptions about a CBDC ecosystem

This section sets out the assumptions used in developing this framework.

4.1 A two-tier CBDC model

A two-tier CBDC model is assumed.[11] In this model the central bank issues CBDC and manages the supply. It maintains the CBDC account balances of financial institutions such as banks and payment service providers (PSPs), which in turn would be responsible for distributing CBDCs to end users (individuals and businesses) and supporting CBDC payments. Such financial institutions will typically be responsible for know-your-customer (KYC) and anti-money laundering (AML) compliance and due diligence. They are collectively referred to as financial intermediaries (FIs) for the rest of this report.

Figure 2: A simplified CBDC ecosystem



This diagram aims to show key sources of threats and risks, and therefore does not necessarily cover all actors in the CBDC ecosystem. A central bank would bear overall responsibility for the CBDC system, but could outsource or commission its operation to another entity. There could be other financial entities between the central bank and the end user layers.

[11] See Auer and Böhme (2020) for a discussion on the various technical designs of CBDC systems. This framework focuses on retail CBDCs as they tend to have more components than wholesale ones.

It is assumed that the CBDC ecosystem needs to support a range of end users who would use various payment instruments as depicted in Figure 2, and therefore such payment functions would need to be available 24/7.

It is assumed that CBDC systems need to integrate with existing and future payment systems. These could include real-time gross settlement (RTGS) systems, instant payment systems, e-money and mobile money solutions, point of sale solutions, embedded payments and various end user solutions as well as other innovations in the future.

In addition, cross-border transactions using CBDC may require support for one or more of the interconnection models such as a hub and spoke[12] or multi-CBDC bridge[13] approach, which may bring additional security and resilience requirements.

4.2 Participants' security and resilience capabilities

This section sets out various assumptions about the security and resilience capabilities and expectations of different participants in a retail CBDC ecosystem.

Central banks

It is assumed that central banks have robust capabilities and practices for physical and cyber security, resilience, external dependency management and enterprise risk management, leveraging industry standard risk management and security frameworks.

It is also assumed that central banks (or other public authorities) would be involved in assessing and verifying the security and operational resilience measures of participants in the retail CBDC ecosystem, perhaps as part of oversight activities.

Participating financial institutions

It is assumed that participants in a retail CBDC ecosystem such as commercial banks, PSPs, and other FIs have robust capabilities and practices for physical and cyber security, resilience, external dependency management and enterprise risk management, leveraging industry standard risk management and security frameworks.

[12] For example, the BIS Innovation Hub's Project Icebreaker (BISIH et al (2023)).

[13] For example, the BIS Innovation Hub's Dunbar (BISIH et al (2022b)) and mBridge (BISIH et al (2022a)) projects.

It is also assumed that these participants would need regular security and operational resilience validation and assessments, including independent audit, assurance and certification in order to be able to provide or continue to provide these services.[14]

Merchants, business users, consumers

It is assumed that end users, including merchants, business users and consumers, all play a role in securing their CBDC value, devices and related payment processes. For example, they may be required to maintain the confidentiality of the credentials used to access their CBDC accounts, and maintain the minimum security posture of the devices they use for CBDC.

It is also assumed that there would be requirements for a minimum level of security and associated practices that end user devices and applications would need to satisfy and adhere to before they can be used.

Technology providers

It is assumed that technology providers would play a critical role in a CBDC ecosystem, providing a range of capabilities including:

- Secure and resilient technology infrastructure, compliant with any rules and regulations in a jurisdiction, and assured by an independent party;
- Cyber security services such as cloud-based malware identification, distributed denial-of-service (DDoS) protection services, security monitoring, and intrusion detection and prevention systems;
- Expertise for developing and securing digital currency and payment systems, including independent security validation services;
- Development of digital wallets (software and/or hardware) for holding CBDCs and making CBDC transactions, online or offline;
- Risk management and compliance systems, including CBDC transaction monitoring and behavioural analysis tools;
- DevSecOps (development, security and operations) solutions to integrate application and infrastructure security throughout the system development, change and operations life cycle.

Overall, security and resilience of CBDC systems is an end-to-end ecosystem responsibility, relies on awareness and good practices from all participants, and requires public and private partnership.

4.3 Complexity and risk profile of retail CBDC systems

In developing this framework, it is assumed that a CBDC system would eventually play a key role in the overall payment ecosystem of a given jurisdiction. When a CBDC

[14] Currently some of these financial entities may not be required to go through regular validation of their security posture and related practices. In future, given their potential impact on the CBDC system, we assume they would need to be regularly assessed.

system only plays a “supporting role”, either during the pilot phase or by design, the level to which control objectives for resilience may be applied may not be as extensive, whereas the level to which control objectives are applied for security should always be robust.

As described earlier, a retail CBDC ecosystem could involve a large number of participants and integration points, and therefore create a large attack surface and many points of failure. This complexity, combined with the potential introduction of new technologies, could contribute to increased risks, which could in turn require mature capabilities in the following areas, besides what central banks are typically already doing:

- **An incident monitoring and response capability that operates 24/7:** Any incident related to CBDC systems will create reputational risk for a central bank, so the ability to detect, respond, investigate and recover rapidly as well as managing communications around an incident is paramount. The central bank’s security operations centre (SOC) and incident management function may need to deal with new types of incidents such as a breach of offline CBDC payment devices to counterfeit value, which may require new capabilities and tools. The end-to-end security and resilience of a CBDC system would depend on each participant in the ecosystem, such as infrastructure service providers, commercial banks and PSPs, with some capabilities extending to these participants. The ecosystem is only as strong as its weakest link.

- **Securely implementing and operating maturing technologies at critical infrastructure scale:** It is assumed that some central banks could adopt distributed ledger technology (DLT) for their retail CBDC systems (others may not).[15] DLT has shown some promise in wholesale use cases[16] and has been adopted by some large financial institutions for interbank or intrabank settlements.[17] In cases where DLT might be used, such platforms may require customised security architecture and additional hardening relative to traditional systems. This would also require actors in a CBDC ecosystem to develop, attract and retain new talent required to design, implement and operate secure and resilient CBDC systems. The large-value attacks on DLT protocols and smart contracts in the DeFi space underscore the potential operational and reputational risks.[18]

- **Concentration risk**: Where multiple ecosystem participants rely on the same service provider, this could increase the operational complexity and risk for central banks.

[15] Central banks which have chosen to use DLT for their pilot/production retail CBDCs include the Central Bank of Nigeria, the Eastern Caribbean Central Bank and the Central Bank of Brazil. DLT may be suitable for some central bank requirements for CBDC, whereas for others it may not be,

[16] Such experimental projects include Jasper, Ubin, Stellar, Khoka and Cedar, among others.

[17] As an example, JPM Coin has been used inside JPMorgan Chase for different business units to automatically transfer and settle funds, creating more transparency and efficiency.

[18] See BISIH (2023c).

- **New technologies:** A CBDC system would most likely leverage a range of technologies that have not been previously used or may be in limited use in a central bank. Among the already announced CBDC experiments, pilots and production systems, DLTs, programmability, smart contracts and attention to quantum computing have emerged as common themes. It is assumed that CBDC systems could provide functionality to enable programmability (smart contracts being one example) for new use cases utilising automated CBDC payments when certain conditions are met.[19] However, recent examples of smart contract hacks, which have led to the loss of a significant amount of value in DeFi,[20] serve as an example of the potential security risks CBDC systems could face.

Quantum computing has seen advancement in recent years. Given the known vulnerability of existing cryptographic algorithms to quantum computing, it is assumed that central banks will require CBDC systems to be crypto-agile[21] so upgrades to cryptography can be applied at pace when incumbent encryption algorithms are no longer deemed safe.[22]

In summary, it is assumed that a CBDC system would be complex, with a large attack surface and many potential points of failure, bringing new and elevated risks. This framework for security and resilience has been developed to help central banks navigate this increased complexity and risk profile.

[19] Central banks may decide not to include programmability in their CBDCs at the foundation layer. However, smart contracts could be leveraged by financial institutions or other government agencies at the payment layer.

[20] BIS Innovation Hub (2023c) lists six high-profile DeFi hacks carried out in recent years, of which three were related to security flaws around smart contracts, with a combined loss of over US$ 1 billion.

[21] CBDC systems should be designed to be crypto-agile irrespective of threats from quantum computing.

[22] Recently, researchers have demonstrated that an AI-assisted side-channel attack could compromise some public key quantum-proof cryptography algorithms (see Ngo (2023)).

5. Understanding the framework

This section describes the framework for CBDC security and resilience, covering the objectives, design criteria, threat landscape, industry framework leverages, structure of the framework (steps and control objectives), alignment with enterprise capability domains, and the main content of each of the seven steps.

5.1 CBDC security and resilience: objectives and design criteria

Security and resilience cover the confidentiality, integrity and availability[23] aspects of a system, and the capability to respond to and recover from incidents. Security measures ensure a system's robustness against threats posed by a range of threat actors such as nation states, hacktivists or insiders. Resilience measures ensure a system's robustness against abnormal events such as an outage of a component or a sudden spike in transaction volumes. Overall, the security and resilience measures applied to a CBDC system aim to safeguard the following:[24]

- **Confidentiality**: ensures that sensitive information in the CBDC system is only accessible to the authorised users and systems when required. This could include sensitive financial and technical information such as credentials and cryptographic keys.
- **Integrity**: ensures that data and supporting technologies in the CBDC system, such as a transaction amount or payee information, have not been tampered with, manipulated or corrupted, that CBDC cannot be double-spent, new CBDC is only generated by the central bank or a process authorised by the central bank, etc.
- **Availability**: ensures that a CBDC system will be available 24/7, and provides the required response and transaction processing time.

In developing the framework, the following guiding criteria were drawn from industry:

- **Design for resilience**: The networks, infrastructure and application architecture should be designed with redundancy and failover capabilities. The system should be prepared to adjust and scale dynamically to handle a sudden surge in transaction volumes, and ensure that transaction execution is designed to handle exceptions gracefully, with risk management controls that focus on prevention and are supported by robust incident management and business continuity plans (BCPs).
- **Eliminate single points of failure**: Identify areas where there is lack of redundancy in the CBDC system or supporting infrastructure such as a network service provider, power supplier, cloud service provider, shared services or key personnel. These should be risk assessed for the likelihood and impact of disruption, with the relevant countermeasures identified and applied.

[23] Also referred to as the CIA triad.

[24] Even though data privacy can benefit from security measures, it is not in scope for this framework.

- **Emphasise timely action**: Retail CBDC systems would need to operate 24/7. There would be very little tolerance for system outages. The health and availability of the CBDC system would need continuous monitoring so that incidents could be handled as soon as they were detected. Robust change management, governance, and agile processes would be essential to manage changes in response to incidents, supported by automation solutions used for continuous build, integration, testing, releases and deployment as well as security testing of any changes.
- **Promote technology diversity and interoperability**: Where possible, systems should make use of multiple technology solutions for a given CBDC capability and require each to support standard approaches for integration. For example, end users' CBDC wallets should be able to function even when the financial institution providing the wallet has a service outage. This, however, could come at additional costs and operational overhead, which would need to be evaluated.
- **Implement defence in depth**: When a business impact analysis (BIA) determines that any of the CBDC system components have a severe or high impact on the confidentiality, integrity or availability objectives, preventative defence measures should be implemented at multiple layers,[25] for example across the network, application and data access layers.
- **Assume a breach and be ready to respond**: Even with a focus on preventative controls, incidents should be expected to occur and therefore detection capabilities are essential, supported by readiness to respond to and recover from incidents. Purple-teaming exercises could be important to ensure all ecosystem participants are prepared to respond to different types of incidents that could occur with CBDC systems. Such exercises could involve a range of scenarios involving sophisticated threat actors and events, used to validate the effectiveness of defensive and detective controls, identify any gaps and implement improvements.
- **Introduce changes in staggered releases**: Staggered rollouts could help reduce risk, by enabling changes to be tested in a limited setting before releasing the change at scale. This would allow production issues to be caught and resolved with less impact, or easier roll-back of changes when required.

5.2 Threat landscape for CBDC systems

Ensuring security and resilience must take a risk-based approach. Risk management starts with threat analysis. When assessing the threat landscape for CBDC systems, the following three areas should be considered:

1. **Common threats to financial systems:** This ranges from large-scale attacks, such as the heist experienced by Bangladesh Bank, to the everyday financial crimes

[25] The layers in which defences can be implemented include the network layer, identity and access management layer, application or API gateway layers, host layer, application logic layer, and data layer. Each layer could leverage indicators that are visible at that layer to stop an attack. Having multiple layers of defence reduces the chance of an attack being successful.

committed using social engineering such as phishing, credential theft, SIM swap attacks,[26] or man-in-the-middle attacks.

2. **Emerging threats associated with new technologies:** This could include DLT-related attacks against consensus protocols, cross-chain bridges, oracles, attacks against smart contracts or offline CBDC components, etc.
3. **An expanded attack surface:** This includes the various components in the CBDC ecosystem as described previously, some of which may not be part of the central bank's current threat landscape.

5.2.1 Threat actors

The threat actors for CBDC systems could be explicitly malicious or inadvertently causing an incident. These threat actors could include, but not limited to:

1. **Nation states or nation state-sponsored groups**: these adversaries aim to disrupt or compromise other governments, key organisations, or individuals to damage or gain access to IT systems, information assets or other intended outcomes, to sow fear or distrust, or to create reputational impact.[27] These threat actors are highly skilled and motivated and have significant resources at their disposal. For example, they could try to counterfeit CBDCs through online or offline channels and inject them into the system.
2. **Organised crime groups**: individuals or groups of people that use technology to create malicious incidents on IT systems to steal sensitive data, gain unauthorised use of computing resources, or generate profit. CBDC systems are a particularly attractive target due to their large number of customers, the ever-expanding attack surface due to their heavy reliance on technology, and the fact that they may hold sensitive data on individuals and businesses, as well as the potential to execute fraudulent transactions. In some cases, these threat actors can work with or be sponsored by nation states.
3. **Hacktivist groups**: individuals or groups who typically have strong sentiment against or opposing views to organisations they target. They use online platforms to express these views, showcasing the impact or damage they have caused to support their views. They may disrupt the operations of systems or seek to damage the reputation of a central bank through defacing websites, spreading disinformation, sabotaging payment devices, advertising the compromise of obsolete devices or potential data leaks to sow distrust.
4. **Lone hackers or petty criminals**: operate on an individual basis and are motivated by financial gain or glory from the intellectual challenge of breaching complex systems. For example, they may use malware or phishing to gain end users' CBDC account credentials.
5. **Professional criminals:** have turned their cyber criminal activities into a business. Motivations tend to be financial but they offer "cyber crime as a service", where

[26] SIM swap attacks could be used to compromise a system administrator's account if SMS text messages are used as an authentication factor. A zero-trust security architecture, discussed later in this framework, would not allow SMS texts for authentication.

[27] Non-financial motivations could be harder to disincentivise.

they write malware that can be sold. They may also be working for other threat actors.

6. **Insiders**: individuals who have access to a CBDC system's internal operations (for example system administrators, developers, operators) and could work independently or in collusion with others, such as nation states or organised crime groups, for financial gain or malicious intent. Insiders may also cause accidental or unintentional impacts on CBDC systems through poor change or operational management actions.
7. **Malicious end users**: such end users of the CBDC system will be able to access and exploit CBDC wallets 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.
8. **Third parties**: external entities that provide various technology components such as hosting services, or support personnel to manage the implementation or operations of a CBDC system, could experience a security breach or otherwise behave maliciously to compromise the security or normal operation of the system.
9. **Natural or human-caused disasters**: natural disasters, wars or other disasters could cause large and sustained power and/or network outages for a prolonged period of time. BCPs for such disasters would need to include requirements for CBDC systems.
10. **Cyber warfare vendors:** these are companies that supply cyber weapons. Their products could end up in the wrong hands and be used for criminal activities. Some examples include vendors of spyware, which could be used to target senior leadership or key individuals in a central bank, installed through spear-phishing attacks or spoofed emails, giving criminals access to victims' keystrokes, screen, camera and microphone.
11. **AI bots:** interactive or covert computer programs powered by AI could be used to extract sensitive information, establish fake accounts, break encryption or launch cyber attacks. AI bots could learn and adapt their behaviour to evade detection by security monitoring solutions.

5.2.2 Threat events

The following is a non-exhaustive list of threat events that could compromise the confidentiality, integrity or availability of a CBDC system. These events are not necessarily mutually exclusive, as multiple events can occur in one incident. These threat events are presented in no particular order, and their likelihood and impact may vary.

1. **Distributed denial-of-service (DDoS) attacks**: An attacker can use computing resources they have purchased or a network of compromised computers or IoT devices to launch a massive volume of service requests to a CBDC system or services it relies on, in order to exhaust the computing resources in a critical area of the ecosystem, resulting in a system overload that causes failure, timeouts or performance degradation.
2. **Advanced persistent threat (APT) attacks**: APTs are typically sponsored by nation states or organised crime groups. They penetrate the victim's system, plant

malicious software or create backdoors, and patiently observe network traffic and user and system behaviour, sometimes lying dormant for long periods of time. APTs typically employ advanced techniques to evade intrusion detection technologies, and quietly exfiltrate data from the victim's network or cause damage by installing malware or poisoning data. For example, they could steal significant amounts of money through fraudulent transactions, or compromise a large amount of sensitive information. APTs may attack a supply chain in order to access the intended target. They can also be enabled by insiders.

3. **Malware (wiperware, ransomware, etc) attacks**: An attacker plants malicious software into the target's computers and networks, which subsequently could either destroy certain computing services, become a backdoor for attackers to connect to the victim's network, or be used to hold the victim's information and computing assets hostage for ransom payments. These can remain dormant and hidden until required by an attacker.
4. **Social engineering attacks**: An attacker could use techniques such as phishing, spear-phishing or baiting, SIM swaps, man-in-the-middle, or compromised credentials to take control of an end user's CBDC account or administrative accounts that are used to manage the CBDC system.
5. **Cryptographic key compromise**: A malicious actor could try to obtain the private key for claiming ownership of CBDCs by hacking the computer or device containing the key file, searching through the device's memory for traces of the key, conducting cryptanalysis based on collected data that have been generated using the key, or via side-channel attacks.[28]
6. **Attacks against new technology components related to DLT or smart contracts**: An attacker could find and exploit vulnerabilities in smart contracts, in a DLT consensus protocol, in cross-ledger bridges, in oracles or in governance protocols, for example.
7. **Compromise of the payment process**: As a payment process often involves multiple parties, the logic in the whole chain of steps could have security gaps, which could be exploited by an attacker to make a purchase without paying, redirect payments to a different recipient, replay payment instructions, or harvest payments from wallets that do not require payer consent.
8. **Malicious end user attacks**: An end user of a CBDC system could try to defraud their own CBDC payment device or mobile application, or work with others to jointly attempt different ways to double-spend CBDCs in their possession, or to counterfeit CBDCs.[29]
9. **Insider sabotage attacks**: A disgruntled employee or contractor who has access to a CBDC system could attempt to cause the system to malfunction by damaging the hardware, deleting key information, shutting down services, providing incorrect input or enabling other threat actors.

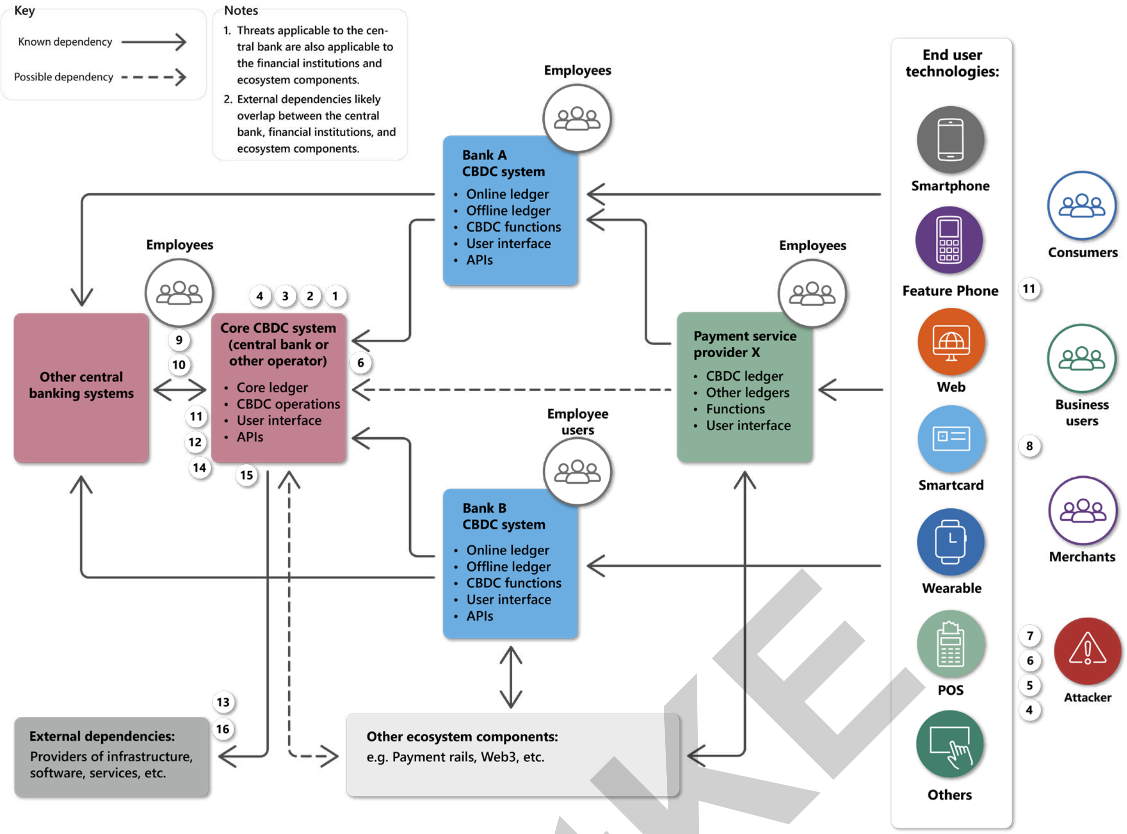
[28] Side-channel attacks can be unpredictable and are relevant for cryptographic modules that are exposed to attackers, for example in offline payment solutions for CBDCs.

[29] Counterfeiting could happen through intrusive means such as physical device breaches or through non-intrusive means such as cryptanalysis or side-channel attacks.

10. **Insider fraud**: A malicious insider may act individually or together with other threat actors to commit financial fraud. The attacker could leverage their privileged access and knowledge of the CBDC system's business logic, and devise ways to defraud the system.
11. **Human error, negligence, or lack of awareness**: A developer may have adopted an open source package with security vulnerabilities without any code scanning or review by a cyber security team. The operations team may have delayed applying a security patch or other critical updates. A system administrator may mistype a command during system maintenance or forget to renew an expiring digital certificate.
12. **Information disclosure due to lack of proper controls**: An employee may gain unauthorised access due to poor or lack of access management controls. A third-party service provider may see sensitive information related to the CBDC system due to a misconfiguration of the shared IT environment it may have access to, or during troubleshooting when regular controls are not effective. Data could also be exposed to attackers due to a gap in the access control logic, etc.
13. **Outage in infrastructure layer**: A catastrophic natural disaster could cause a widespread and prolonged power outage leading to technology failure at the network service provider. Cyber attacks could cause a widespread network service outage. Human errors could also cause a system outage.
14. **Service disruption caused by technology failures**: Software or hardware bugs, failed storage media, software patches or upgrades that are not fully tested, expired service account credentials, etc could cause disruption to a CBDC system. The more technology components involved, the more complexity in the technology stack, the higher the risk of such failures becomes.
15. **Technology obsolescence**: Technologies used for a CBDC system may gradually become obsolete, as vendors may withdraw support, or the technology is outdated and could require an upgrade or a switch over to different technologies. If security patches or bug fixes are no longer available from any vendor, this could create operational, reputational and legal risks for central banks.
16. **Attack against supply chain vendors**: Service and solution providers involved in the supply chains for components of a CBDC system, such as software or hardware, cloud or data centre service providers, could be targets of threat actors. Any compromise could lead to impacts on the integrity or availability of CBDC systems, as well as the confidentiality of sensitive data in the systems.

Figure 3 illustrates the relationship between these threat events and the various participants in the ecosystem.

Figure 3: Threat events that could affect a CBDC ecosystem (simplified view)



5.2.3 Risks

Impacts from incidents described above could compromise the integrity and availability of payment services, and the confidentiality of customer data involved. Any resulting impact is typically measured along operational, reputational and legal dimensions. Areas of impact could include:

1. **Damaged reputation and loss of trust**: A failure or breach of the CBDC system, however small, could damage trust in the CBDC system and the central bank. The contagion risk from such sentiment could have knock-on impacts for other related financial and non-financial systems that rely on or are intertwined with the CBDC system.
2. **Disruption to financial services**: Individuals and businesses cannot make or receive payments because a CBDC system is unavailable or not functioning as normal.
3. **Failure of processes and procedures**: One or more components of the CBDC system are not functioning, causing critical business processes such as payment details validation, risk monitoring or compliance checks to fail, or being bypassed temporarily.
4. **Loss of funds**: End users, commercial banks, and even the central bank could lose money because of a cyber attack that has compromised CBDC systems, accounts or payment processes.

5. **Compromise of sensitive customer data**: As CBDCs are used for payments, data related to payment transactions will be processed in the CBDC ecosystem. A cyber attack or negligence could lead to unauthorised disclosure of such sensitive data.
6. **Loss of integrity in the payment system**: A malfunction or compromise at the network, virtual machine or application level could cause key capabilities such as payment clearance and settlement to not work correctly, undermining trust and confidence in the system.
7. **Loss of efficiency**: A failure or performance issue with the CBDC system may force users to use old or manual processes as a contingency, which could cause significant delays in completing financial transactions.
8. **Increased cost**: Responding to major incidents, and the potential subsequent efforts to strengthen the cyber resilience of CBDC systems, could come at a high cost.

Such risks to CBDC systems arising from the various threat actors and threat events should be assessed using the central bank's enterprise risk management framework. In some cases, the risk management framework may need to be adapted for operating CBDC systems. It could be used to prioritise any remediations required and to assess whether a risk should be mitigated, transferred, or accepted. Results from these analyses and recommendations can be provided by the Chief Risk Officer to senior leadership, an oversight board or risk committee who would make decisions.

A detailed threat modelling tool such as the MITRE ATT&CK framework[30] could help central banks identify controls that are needed in preventing and detecting various threat events and determining appropriate countermeasures. For DLT-specific threats, further analysis is needed as current threat models do not provide full coverage for all DLT-specific attacks.[31]

5.3 Building blocks of the proposed framework

Implementing CBDC systems would be a large business transformation[32] programme. This framework aims to provide a holistic set of security and resilience considerations that could be used as a guide for planning, implementing or operating CBDC systems, in association with the industry standard frameworks and best practices for risk management, information security and business continuity already used. This framework includes some common and existing considerations as well as additional ones covering the adoption of modern digital technologies and practices (eg DevSecOps and the zero-trust security model[33]), maturing technologies such as DLT, and specific considerations for a CBDC and the associated payment capabilities.

[30] The MITRE ATT&CK framework focuses on cyber security events. Resilience events can be modelled similarly but new threat libraries would need to be added to the framework.

[31] See BISIH (2023c).

[32] Business transformation is a holistic view of change that combines both organisational and digital changes.

[33] A detailed description of these trends can be found in Appendix B.

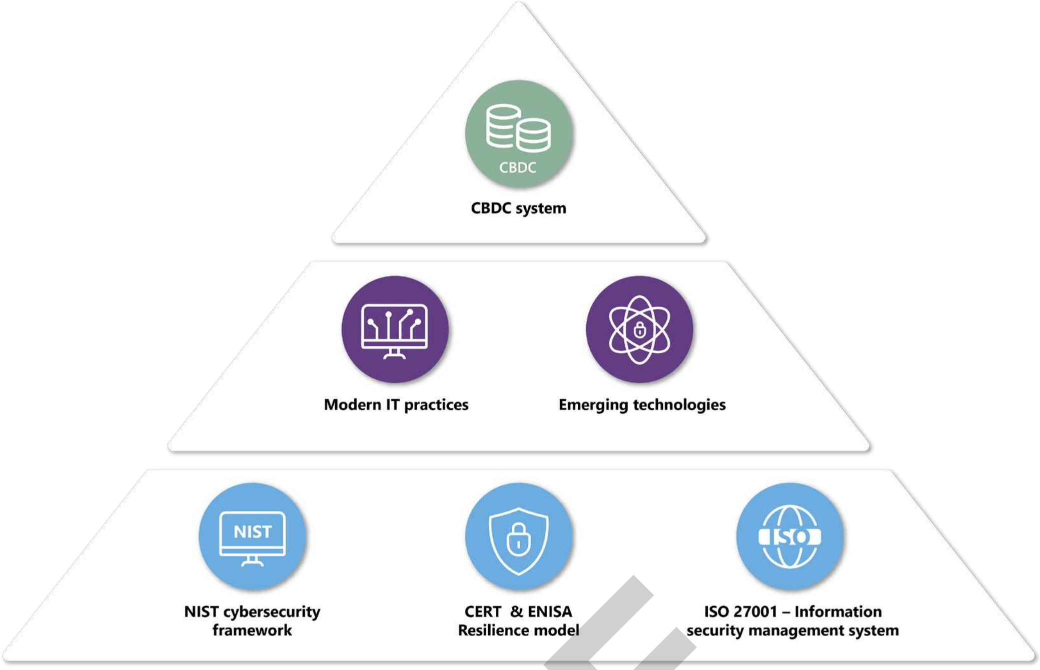
The following industry frameworks and guidelines are used as the source of input for this framework.[34]

- **NIST Cybersecurity Framework Version 1.1**: This provides the capabilities and best practices for dealing with cyber security risks.
- **CERT Resilience Management Model Version 1.2**: This provides a detailed framework and implementation guidance for control objectives related to both security and resilience for any ICT systems.
- **ENISA – Enabling and managing end-to-end resilience**: This focuses on public networks and services.
- **ISO 27001:2022**: This is the industry benchmark for measuring an organisation's maturity in its information security management system, which will prepare the organisation for coping with cyber security challenges.
- **ISO 23257:2022**: This defines the framework for blockchain and DLT solutions. It identifies the key components in such architecture and typical areas of security concerns.
- **Cloud Security Alliance – Security guidance for critical areas of focus in cloud computing v4.0**: This includes security considerations for deploying solutions in a cloud infrastructure or platform.
- **US Department of Defense – Enterprise DevSecOps Reference Design**: This covers the best practices for agile software development, deployment and operations.
- **NIST** – **Zero Trust Architecture**: This describes the zero-trust principles, use cases and its role in the overall security architecture.
- **BIS CPMI and IOSCO – Principles for financial market infrastructures**: Principle 17 provides the key building blocks and considerations for financial market infrastructures (FMIs) to manage operational risks, including information security, scalability and business continuity.
- **BIS CPMI and IOSCO – Guidance on cyber resilience for financial market infrastructures**: This provides guidelines on achieving cyber resilience for FMIs and their dependencies.

Figure 4 below shows the three layers of input used in formulating this framework:

[34] See NIST (2018), SEI (2016), ENISA (2011), ISO (2022, 2022a), Cloud Security Alliance (2017), US Department of Defense (2019), NIST (2020) and BIS CPMI and IOSCO (2012, 2016). A number of other frameworks exist for security or resilience, with similar guidelines or requirements.

Figure 4: Three layers of input used to formulate this framework


CBDC
CBDC system
Modern IT practices
Emerging technologies
NIST
NIST cybersecurity framework
CERT & ENISA Resilience model
ISO
ISO 27001 – Information security management system

The bottom layer represents the three primary sources of input for the baseline control objects. The middle layer represents inputs for control objectives in IT modernisation and DLT, with the top layer representing inputs for currency and payment-related functions.

These common frameworks were leveraged and aggregated to:

1. Provide a set of reliable and comprehensive control objectives that are important for CBDC systems.
2. Provide assurance to practitioners that existing capabilities implemented from or aligned to these frameworks can be leveraged for the CBDC system.

The result of this aggregation is described in the following section.

5.4 The Polaris framework for secure and resilient CBDC systems

To organise the control objectives that have been identified and adapted for CBDC systems, this framework has leveraged the NIST cyber security framework but with two additional steps, namely **prepare** and **adapt**. This framework therefore has seven steps: **Prepare, Identify, Protect, Detect, Respond, Recover and Adapt.**

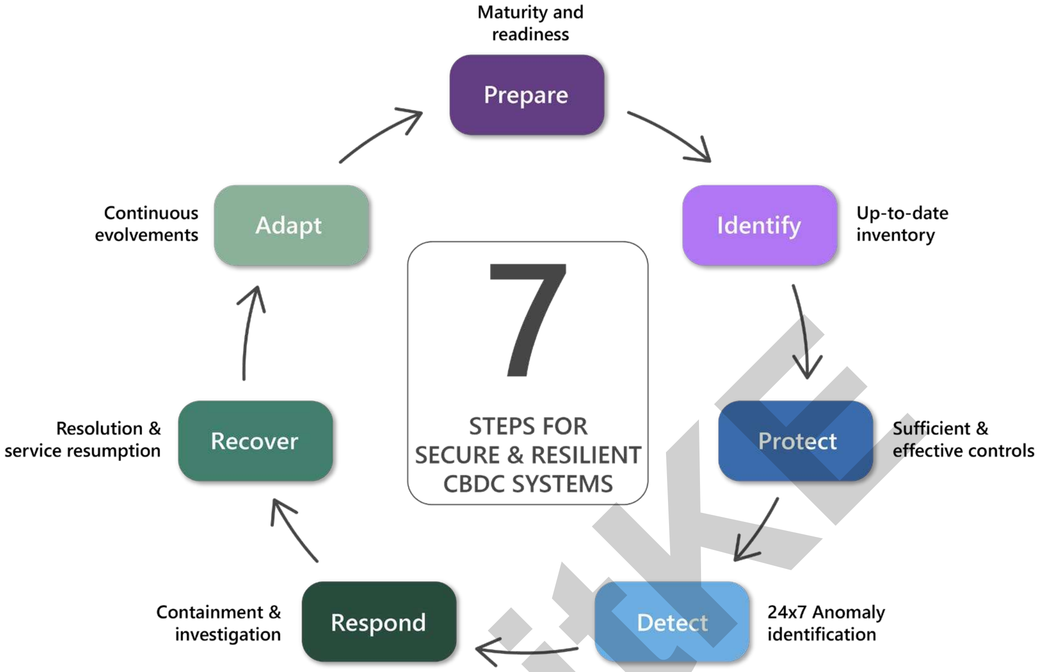
The **prepare** step is separated out from the original NIST framework to highlight a set of fundamental capabilities that would need to be considered for operating a CBDC system in pilot or production.

The **adapt** step is highlighted for central banks to periodically take stock of the learning from incidents as well as new threats or requirements and come up with potential countermeasures to enhance their level of preparedness and protection.

Figure 5 provides an overview of this seven-step framework, with the focus for each step highlighted in the diagram.

Each step includes a set of control objectives to be met for a CBDC system. Each objective is a statement describing the aim or purpose of controls to be implemented in order to address certain risks related to security or resilience.

Figure 5: The seven steps for secure and resilient CBDC systems



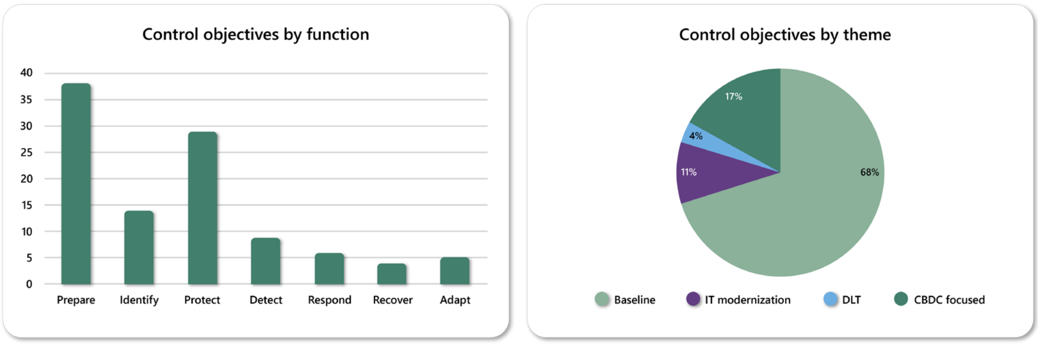
5.4.1 Categorisation of control objectives

This framework comprises 104 control objectives that are grouped under each of the seven steps. Each control objective is categorised along four themes:

- **Baseline** – minimum control objectives that should be met by most ICT systems and are deemed important for CBDC systems;
- **IT modernisation** – objectives that could support modern approaches to security, resilience and risk management, providing a more efficient way to reduce risk;
- **DLT-specific** – objectives that could apply to DLT-based CBDC systems;
- **CBDC-focused** – objectives that could apply to CBDC and payment functions.

Figure 6 summarises the distribution of these control objectives.

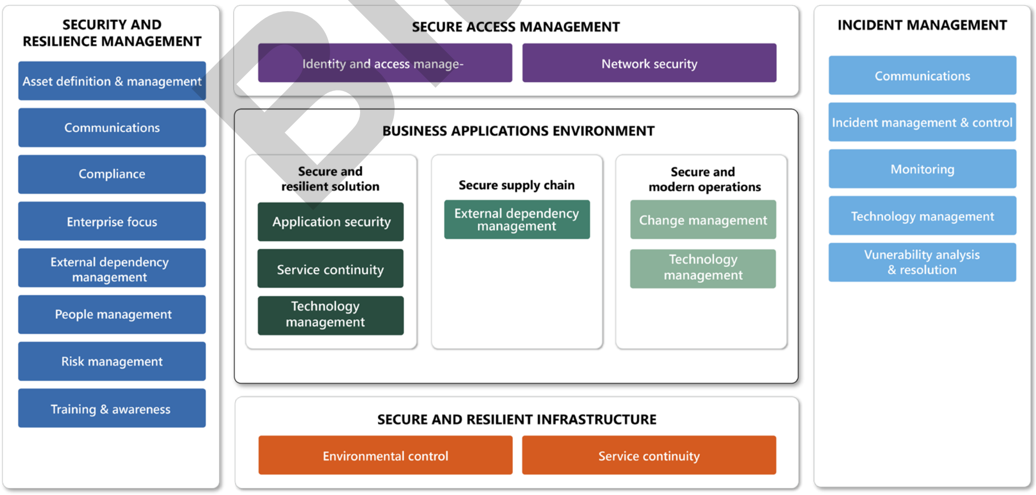
Figure 6: Overview of control objectives



5.4.2 Enterprise capabilities represented in the framework

In the context of an enterprise environment, security and resilience are part of the overall enterprise capabilities. As shown in Figure 7, the control objectives in this framework are organised along the capabilities as defined in the CERT Resilience Management Model, for example asset definition and management, identity and access management, application security, environmental control, communications, etc. These capabilities are further organised under the different domains, namely security and resilience management, secure access management, secure and resilient solutions, secure supply chain, secure and modern operations, secure and resilient infrastructure, and incident response and recovery.

Figure 7: Capability model to support secure and resilient CBDC systems



Each of the seven steps and their key components are detailed below. A full list of the control objectives in each step is provided in Appendix A of this report.

5.4.3 Seven steps to secure and resilient CBDC systems

1. Prepare

This step is intended to guide central banks in assessing their readiness for implementing and operating a secure and resilient CBDC system. This includes commitment from senior leadership, reviewing and possibly updating the enterprise risk management strategy, and augmenting or establishing enterprise capabilities to apply, manage and govern the control objectives listed in the framework.

The objectives listed in this step fall under two themes: **baseline** and **IT modernisation**.

Baseline capabilities are key and can include:

- Management commitment, with defined roles and responsibilities in the central bank;
- Established information security and business continuity functions and governance structure;
- 24/7 monitoring and alerting function;
- Established risk management, compliance and change management practices;
- Established infrastructure that supports the need for on-site and off-site backup and recovery, among other capabilities.

IT modernisation capabilities that central banks could consider adopting to enhance their security and resilience maturity in the context of CBDC systems could include:

- Using DevSecOps to streamline and automate the process to build, test, deploy and operate software, to achieve agility without compromising quality control;
- Modern security techniques such as security-as-code and security guardrails enforced at the infrastructure level to contain potential impacts caused by security vulnerabilities at the application level;
- Capabilities at the infrastructure or application level to facilitate automated scaling of computing resources to efficiently accommodate the dynamic change of transaction volume;
- Zero-trust security practices including strong authentication, least privilege, network segmentation, and continuous validation of identity and trust, etc.

Central banks could leverage these where possible or develop a plan to establish such capabilities if they are deemed strategic investments. Without some of these capabilities, there may be continued reliance on legacy processes, which may not support potential requirements for secure and resilient CBDC systems, and could introduce operational risks, additional costs and longer recovery time from incidents.

2. Identify

This step is intended to guide central banks to identify the information assets, systems and networks used for CBDC systems, as well as external dependencies, that would need to be protected and have resilience measures applied.[35] Central banks should consider the following activities:

- Identifying the information assets, systems and networks for a CBDC system to be managed, including integration points and vendor dependencies;

- Monitoring emerging threats, vulnerabilities and risks that could affect CBDC systems, including external dependencies, and determining possible mitigation measures required;

- Defining the security and resilience requirements for the CBDC core functions, online and offline, from both the system's and the end user's perspective;

- Defining security requirements for online and offline digital wallets that end users will use to hold and use CBDCs;

- Defining the roles and responsibilities of actors in the CBDC ecosystem (for example, commercial banks and financial institutions) in ensuring end-to-end security and resilience.

Once these are defined, they should be communicated, with actions assigned to specific owners. Tasks and progress should be tracked and reported.

3. Protect

This step covers objectives for the technical and non-technical controls and measures that would need to be implemented to protect the CBDC system against and mitigate the impact of security and resilience incidents. This step also includes controls specific to DLT if this is used for a CBDC system.

In addition to the typical emphasis on areas such as network security, identity and access management, application security, resilient architecture and design, and secure and modern operations, the following could be applicable to CBDC systems:

- When user identification is required, leverage an established identity scheme to avoid any additional exposure of user data;

[35] Actions such as asset and risk identification are part of this step and are detailed in the control objectives set out in Appendix A.

- Due diligence on the security of payment devices, applications and workflows, to minimise the attack surface and possibility of compromise;[36]

- Due diligence on the security of cryptographic keys that are used to secure digital wallets and transactions;

- Testing and certification of offline CBDC solutions according to the security criteria defined by the central bank;

- A real-time monitoring and risk-based decision capability to identify suspicious or anomalous CBDC transactions or compromised digital wallets and take appropriate actions such as blocking a wallet, adjusting transaction limits or other risk management parameters.

Comprehensive security validation and testing of the CBDC system would help central banks verify whether sufficient controls have been implemented.

4. Detect

With an evolving cyber threat landscape, and the complexity of a CBDC system and its dependencies, incidents should be expected to happen. Central banks and participants in the CBDC ecosystem would need to be able to detect incidents before they escalate. Some considerations could include:

- Gaining awareness of potential threats or vulnerabilities through sharing of threat intelligence or coordination of incident response efforts between CBDC ecosystem participants. This could involve the formation of a CERT focused on CBDC systems, as they could be considered critical infrastructure;

- Establishing a baseline pattern (network traffic, end user behaviour, etc) and constantly comparing the observations against the known patterns for normal behaviour in order to identity possible incidents. This analysis could benefit from a security information and event management (SIEM) system that collects and correlates event logs from multiple sources;

- Proactively scanning the network and systems to detect vulnerabilities or indications of compromise. This could be regular vulnerability scanning, "red-teaming" exercises, or a targeted "threat hunting" activity. With an evolving cyber threat landscape, detection and response capabilities would need to continually adapt;

- Developing a strategy for monitoring and detecting potential incidents with offline payments, as real-time monitoring is not possible.

Detection capabilities must operate 24/7, with alerts being reviewed and responded to around the clock, typically overseen by a SOC capability.

[36] The BIS Innovation Hub's Project Sela is experimenting with various practices to minimize the attack surface including architecture design, transaction authorization, and data management.

5. Respond

Given the unpredictable nature of certain high-impact events such as natural disasters or cyber attacks, and the criticality of a CBDC system to a nation's financial system, central banks should have a dedicated incident response team with clear roles and responsibilities. This team needs to be ready to respond to incidents at any time, and would need to treat an incident as its highest priority until systems and services are restored to a satisfactory level.

- An incident response team would be led by an incident manager and include a dedicated executive in charge of physical and cyber security such as a Chief Security Officer, in addition to members of the SOC.
- The team could also include members from other functions, including executives or management from affected business areas, legal, communications or risk management, and have support and delegated authority from senior leadership to resolve the incident.
- This matrix team should be familiar with the incident response and recovery processes through participation in "tabletop" or "purple-teaming" exercises, and be capable of performing root cause analysis, impact containment, eradication of vulnerabilities and remediation of damages that have been caused by the incident.
- The incident response team would also need to have established contact with incident response functions at participants in the CBDC ecosystem, and be able to engage them as appropriate throughout an incident response process.

6. Recover

This step is about restoring impacted services to normal operations. Activities may include restoration from backups and replacing, repairing or upgrading hardware and software. The recovery process may need to be coordinated with other participants in the ecosystem; therefore, preparatory plans and processes would need to be established. The following points would be some important considerations:

- A CBDC system would need to resume normal operation as soon as possible;
- Clear and timely communication to the public and businesses would be essential, to provide clarity and certainty;
- Transactions that were pending or in an incorrect state would need to be resolved.[37]

[37] Some cases may need to be resolved via a dispute resolution process; however, further work would be required to determine how this would need to be designed to handle such incidents according to their severity.

It would be important to test and simulate how recovery processes would need to happen in practice, particularly when maturing technologies (eg DLT) are used, at an early stage.

7. Adapt

The "adapt" step enables the CBDC system to adjust its operational parameters and go through changes as needed. This includes:

- Leveraging technologies or services that can automatically scale up when demand is high, for example using a DDoS protection service that can absorb much more network traffic volume than a central bank's network can handle, adopting virtual machine management services that can auto-scale, etc;
- Learning from each incident and making adjustments (eg increasing capacity, hardening certain services, introducing new controls, training) as needed;
- Proactively making changes to the CBDC system and associated business processes (based on findings from the incident, in response to new cyber threats).

The framework for secure and resilient CBDC systems is an iterative process. The "prepare" and "identify" steps should be carried out periodically to reassess maturity and readiness and review identified new threats. The "protect" and "detect" steps are "always on", making sure that existing controls are still effective while implementing new controls as required. The "respond" and "recover" steps are largely responsive, as a reaction to a security or resilience incident. The "adapt" step could be carried out in different stages, for example during design, in operation, after each incident, and on a regular basis.

6. Applying the framework

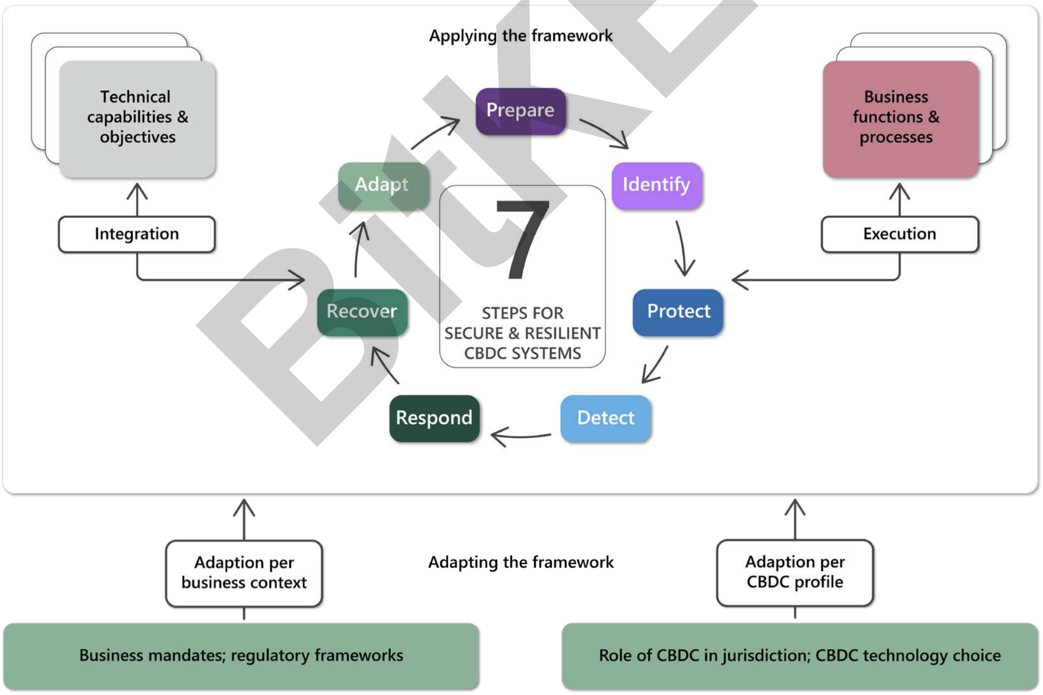
This section describes how to apply this Polaris framework for CBDC security and resilience.

6.1 Adapting the framework

As shown in Figure 8, this framework could be adapted according to a central bank's mandate, operational context, legal and regulatory obligations, technology solutions used for a CBDC system, broader public service objectives for CBDC systems, associated risk appetite, and business continuity and incident response strategy.

The adapted framework could be applied and implemented through integration and potential changes to the technical and business areas of the central bank and other participants in the CBDC ecosystem.

Figure 8: Adapting the framework


Applying the framework
Technical capabilities & objectives
Integration
Prepare
Identify
Adapt
7
STEPS FOR SECURE & RESILIENT CBDC SYSTEMS
Protect
Recover
Detect
Respond
Business functions & processes
Execution
Adaption per business context
Adapting the framework
Adaption per CBDC profile
Business mandates; regulatory frameworks
Role of CBDC in jurisdiction; CBDC technology choice

This adaptation effort could be led by a chief security officer, who would be familiar with the context and the associated business processes and technical capabilities of the organisation.

6.2 Roles and responsibilities within the central bank

Within the central bank, the following set of business roles or functions would typically be directly involved in overseeing, managing and implementing the security and resilience framework for the CBDC system, although many other functions and teams would be likely to contribute to its security and resilience. It should be noted that all roles in a central bank contribute to the security and resilience of the organisation and its systems.

1. Central bank senior leadership and board

Leadership endorsement and support is a key success factor for any security and resilience programme. The CBDC project team needs to make the central bank's management aware of the importance of these two key elements, and the amount of work needed to meet the objectives. Central bank management should also commit to emphasising the importance of these in their communications to central bank staff, participants in the CBDC ecosystem and the general public. Ideally, members of the central bank's executive team (eg the chief security officer and the executive accountable for the CBDC system operations) should be appointed as the owners of security and resilience for the CBDC system, who would then make sure that such topics are regularly discussed at senior leadership, board and executive meetings, so any risks are included in the central bank's risk register, discussed and prioritised, resources are sufficiently allocated, and any change required is executed.

2. Chief security officer

The chief security officer (CSO) is responsible for the day-to-day security (physical and cyber) and resilience of the organisation as a whole, including the CBDC system. They would lead the effort of adapting the framework to their jurisdiction (as described earlier), set a target and timeline for achieving maturity (to be described later), and define the minimum security and resilience requirements that would have to be met before the CBDC system could go into pilot, and what additional requirements would have to be met before production.

They would define the proper sourcing strategy for supporting the security and resilience needs of the CBDC system, ensuring that sufficient resources will be ready to perform the ongoing monitoring, detection, response and recovery activities once the CBDC system goes into pilot or production, as well as the security due diligence for ongoing changes.

They would establish regular communication with their counterparts in the other participants in a CBDC ecosystem (eg financial institutions and major technology suppliers), and provide regular updates to the accountable executive(s) responsible for the CBDC system as well as to the central bank's senior leadership and board.

Given the critical importance of a CBDC system and the evolving cyber threat and risk landscape, the CSO should be an executive-level role that reports to the governors and works in close cooperation with the chief risk officer (CRO) and chief information officer (CIO), as opposed to reporting to the CIO or chief operating officer.

3. Enterprise governance committees and functions

This group of functions manages the central bank's overarching governance frameworks that encompass all projects and business activities, such as the risk register, the information security policy, the audit function, the vendor management function, etc. These functions should incorporate CBDC-related components into their work and ensure that CBDC is covered in future activities. For example, the technology risk management function should incorporate CBDC-related risks into its risk register and start tracking and reporting these risks. Similarly, the business continuity function needs to incorporate CBDC into its set of business processes to manage, and include CBDC-related business and technology functions in the overall business continuity and test procedures.

4. Steering/stakeholder committees

The CBDC programme steering committee should include a senior executive who covers the security and resilience aspects of the system. This could be the chief (information) security officer or a suitable delegate who ensures that security and resilience requirements are implemented as planned, prioritised, appropriately resourced and any issues resolved.

5. CBDC programme team

The CBDC programme team is tasked with specifying, designing, implementing, testing and deploying the CBDC systems and associated supporting functions, including the handover into operations. It could use the framework to derive some security and resilience requirements. The programme team should work with the enterprise governance functions to ensure that the CBDC programme follows and leverages existing governance processes and frameworks, but also identifies how these would need to be updated.

The programme team would need to inform the IT infrastructure team of their requirements, and work together with them on specifying the environment configuration for the CBDC system components. The programme team should detail the various CBDC system components needed to establish the necessary incident detection, response and recovery strategy and procedures.

6. Change management function

Applying this framework could lead to a central bank identifying capabilities that may need to mature or new capabilities that need to be established. It is critical for central banks to implement change management strategies for CBDC systems at an early stage to ensure any changes and their impacts are identified, planned for, and communicated to all stakeholders.

On the other hand, a resilient CBDC system relies on the central bank and other involved institutions being responsive, agile and coordinated in their change processes when an incident response leads to the need to make a change to the system.

Depending on the solution used for a CBDC system or the nature of the change, a central bank may find itself in a position of needing to manage and operate multiple versions of the system for a certain period of time. This would require careful planning, regular and early communication, change roadmaps and clear details on how different versions might be supported and for how long, and guidance on switchover or migration.

7. The IT infrastructure team

The infrastructure team would need to allocate sufficient computing, network and storage resources to support the operation and resilience requirements of a CBDC system. Any supporting infrastructure together with the deployed CBDC components would need to meet the security and resilience requirements. Robust processes for deployment and roll-back when managing changes to the CBDC system would need to be in place. Regular vulnerability scans and security updates of the software and network components supporting a CBDC system should always be prioritised.

8. The security and resilience functional teams

Under the leadership of the CSO,[38] the functions accountable for security and resilience would need to be involved in each phase of the CBDC programme to ensure that security and resilience requirements and activities are implemented.

These functional teams would need to analyse the architecture components of the CBDC solution, identify new technologies and new dependencies, and ensure the control objectives in this framework are applied. They would need to develop the security and resilience plan and key milestones for the CBDC programme, overseen by and reviewed with the CSO. They would also ensure that threat modelling is performed at a detailed level to help shape the overall security and resilience focus areas for the CBDC programme. They would work with both the programme and infrastructure team to ensure the proper protective and detective controls are implemented. Threat intelligence channels may need to be established or enhanced to cope with the new threat landscape engendered by the CBDC system.

6.3 Roles and responsibilities across the ecosystem

Besides the central bank, a CBDC ecosystem could involve commercial banks, PSPs, other intermediaries, end users including merchants, and technology solution and service providers. This ecosystem would depend on public-private partnerships.

The central bank could take the lead on defining the end-to-end security and resilience objectives, requirements and standards for CBDC systems in collaboration with actors in the ecosystem, as well as assessing risks and defining risk tolerance and levels of acceptance. These could form part of any requirements that participants would need to implement, demonstrate and validate in order to be allowed to operate within an CBDC ecosystem. In addition, central banks could take the lead (working with other authorities and the private sector) to ensure that security requirements for digital wallets, which could include offline payment functionality, are defined.

[38] In some organisations, the resilience functional team could be under a different leadership. This would require coordination between the chief (information) security officer and the leadership for the resilience function.

The security and resilience of a CBDC system depends on its weakest link. In that regard, central banks need to ensure not only that the CBDC system has implemented all the necessary measures, but also that all participants (eg financial institutions or PSPs) are meeting security requirements, both initially and for ongoing participation.[39]

The resilience requirement for the CBDC system and its subcomponents should be defined within the broader set of resilience requirements that apply to a given nation's payment services.

Central banks need to ensure that the resilience of a CBDC system is regularly assessed, possibly through tabletop exercises, with risks, including concentration risk, assessed and managed.

The following table summarises the roles and responsibilities of the major actors in a CBDC ecosystem in assuring its security and resilience:

Table 1: Security and resilience: roles and responsibilities of different actors

Actor	Security	Resilience
Central bank	• Identify needs for security talent and capabilities to support the cyber security needs of the CBDC and foster capacity-building in meeting such demands. • Establish ownership and accountability on cyber security for the CBDC at the senior executive level. • Facilitate cyber security intelligence-sharing among the CBDC ecosystem participants. • Define security-related supervision requirements for financial institutions	• Identify gaps in the jurisdiction's capacity to provide resilient technology infrastructure, and work with other government bodies to foster the development of such capabilities. • Ensure that the resilience requirements for the central bank's and financial institutions' CBDC components are well defined and regularly reviewed. • Make sure the central bank meets its CBDC resilience requirements.

[39] Adherence to security requirements plus assurance, vetting and certification could form part of any regulatory requirements established for certain participants in a CBDC ecosystem.

	participating in the CBDC ecosystem. • Certify private sector firms who can validate the security of CBDC wallets and other CBDC system components based on the established requirements.	• Consider the inclusion of CBDC system resilience validation as part of the central bank's supervision of financial institutions.
Financial institution	• Follow the central bank's requirements and industry best practices to implement the security measures in its CBDC systems. • Engage vendors who are certified by the central bank to conduct independent security assessments of its CBDC systems. • Follow established requirements in developing or selecting CBDC wallets.	• Make sure its CBDC components meet the resilience requirements as defined with the central bank. • Make sure that users who receive CBDC from one institution can use it on services provided by another institution. • Make sure users can use their CBDC offline per the central bank's requirements.
Technology provider	• Provide CBDC-related security design and testing services to central banks and financial institutions. • Develop CBDC wallets that meet security and resilience requirements defined with the central bank, ideally by enhancing wallets that end users are already familiar with. • Provide an independent security assessment service for CBDC components managed by the central bank or financial institutions.	• Under the government's guidance, establish resilient technology infrastructure. • Standardise its technologies and modernise its system resilience capabilities to support modern mechanisms such as auto-scaling and transparent workload shifting between data centres and even between service providers.

As part of fostering a public-private partnership supporting a CBDC system, a central bank could consider establishing a cyber resilience coordination function in its jurisdiction (or leverage an existing one). Such a function could enable all participating actors in a CBDC ecosystem to co-ordinate, establish roles and responsibilities, participate in readiness and purple-teaming exercises, adopt common processes and use the opportunity to enhance their cyber resilience posture.

End user solutions supporting CBDC, online or offline, are another area that would need to involve multiple actors in the ecosystem. This framework could be used to derive some security and resilience requirements for such solutions. Independent parties could be identified to test, assure and certify end user solutions to be used for CBDCs.[40]

6.4 Path to readiness and maturity

Several case studies have underscored that a central bank's operational capabilities,[41] as well as its existing technology profile, could be a major source of operational risk for the CBDC project.[42] This framework has been developed to help mitigate such risks. The capabilities defined by the control objectives, if required by a central bank, do not all need to be implemented to the highest maturity level before a CBDC system pilot can be launched.

Below are the key steps for a central bank to assess its needs and formulate a plan to achieve a sufficient level of security and resilience, using its risk tolerance for the CBDC system.

1. Formulate a plan for all required capabilities

Control objectives in the "prepare" step in the framework, especially those categorised as "baseline applied to CBDC", would need to be established before a CBDC system could move into a pilot, and would be essential before moving to a production (live) phase. The rest of the control objectives in the framework should be reviewed to determine what is required, the maturity level needed, and by when. A method such as the Capability Maturity Model Integration (CMMI) model (SEI (2010)) would be used. This would be a risk-based approach that considers the benefits of launching a CBDC system, and the mitigating controls to manage risks associated with not fully implementing a capability in a given phase of a CBDC programme. When taking this approach, central banks should to be cautious in monitoring the pilot system and be ready to contain the impact of potential incidents, as the reputational impact could affect further phases of the CBDC programme.

Figure 9 illustrates how a central bank could go through each control objective in the framework, decide if it is relevant, and if so, when and how the capability should be

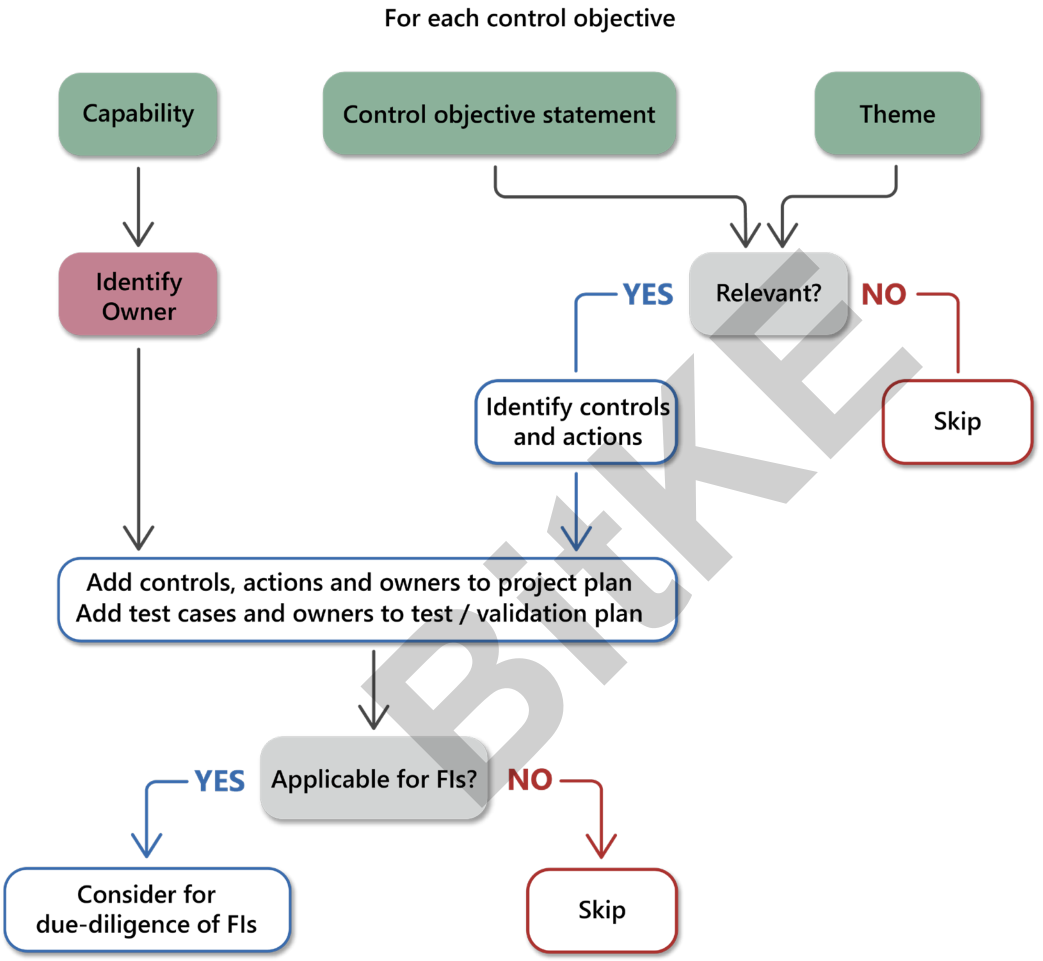
[40] Requirements for security and resilience, assessment, assurance and certification could form part of regulatory requirements for certain actors participating in a CBDC ecosystem.

[41] This includes the central bank's internal employees, third-party vendors and external consultants.

[42] CBDC Task Force report on CBDC information security and operational risks to central banks, forthcoming.

implemented and to what extent, and who should own the implementation of this capability. In this process, central banks could use industry standard guidelines, when needed, in determining the specific controls to be implemented to meet an objective,[43] and the capability domain information in each control objective to identify the appropriate owner(s) for implementation, testing or validation of the controls.[44] The CBDC programme team should also identify the capabilities other participants in a CBDC ecosystem would need to implement and by when, and keep track of progress.

Figure 9: Formulating an implementation plan for required capabilities


For each control objective
Capability
Control objective statement
Theme
Identify Owner
YES
Relevant?
NO
Identify controls and actions
Skip
Add controls, actions and owners to project plan
Add test cases and owners to test / validation plan
YES
Applicable for FIs?
NO
Consider for due-diligence of FIs
Skip

[43] The CERT Resilience Management Model (SEI (2016)) and the Payment Card Industry Data Security Standard (Payment Card Industry Security Standards Council (2022)) provide detailed implementation guidelines on the type of controls to be implemented to satisfy certain control objectives.

[44] For example, the first control objective under "Protect" is "The central bank establishes a separate (or segregated) network segment for its CBDC components where possible. The theme is "Baseline applied to CBDC" which means that this control objective for network segregations is assumed to be part of existing practices at A central bank.

2. Work with stakeholders to execute the plan

With the support of the executive from the central bank, the CBDC project team would work with internal and external stakeholders to make sure the required capabilities are implemented based on the defined timeline.

For external dependencies, the central bank's team would need to establish contact, communicate expectations, and regularly validate progress to make sure the external parties would be able to complete their tasks. The central bank team would need to identify independent parties who could conduct testing and validation and provide evidence to the central bank on the successful fulfilment of these objectives by external parties.

3. Regular updates to executives on status and strategic guidance

Through the executive sponsor of the CBDC security and resilience work, the CBDC project team should regularly update the steering committee and central bank management on the status of implementing the required capabilities for security and resilience, both on the central bank side and for external institutions, so that they understand the dependencies and the risks associated with any missing capabilities, and provide guidance and support on internal and external resources, timeline adjustments and necessary scope changes.

The project team should also bring strategic recommendations to the executives, such as training and talent development for the central bank, incentives to foster private sector development to support the CBDC programme, and liaison with college education programmes to develop a pool of talent for long-term needs of the CBDC ecosystem.

7. Summary

The implementation of retail CBDC systems means that central banks would be developing and updating mass market products and serving retail consumers, which is a space that most central banks are not familiar with. Combined with the complexity of the ecosystem, and the potential critical role they would play in the financial market infrastructure, retail CBDC systems bring a significant amount of risk to a central bank, especially reputational risks that could stem from a security breach or outage at any of the participating institutions in the ecosystem.

The Polaris framework for secure and resilient CBDC systems has been developed to assist central banks in managing this complexity and new risk landscape with a well defined set of control objectives, organised under well known enterprise capability domains, along a seven-step iterative process.

The threat landscape for CBDC systems as laid out in this report provides a starting point for central banks to take a risk-based approach by understanding and managing the threats to the security and resilience of their CBDC systems.

The framework highlights the importance of looking at the CBDC as an ecosystem, in which the central bank can take the leadership role but the eventual outcome would highly depend on the success of a public-private partnership, a long-term strategy for establishing and maturing capabilities across the participating institutions, and fostering the development of a pool of talent and a robust private sector. The framework helps central banks identify areas that need development, both inside the central bank and across the jurisdiction, and could help inform technology providers on the opportunities and expectations awaiting them.

With the constantly evolving cyber threat landscape, the various emerging technologies that will play important roles in CBDC solutions, and the nascent nature of CBDC business and technology models, it is expected that the framework will need to be updated at regular intervals in the future in collaboration with central banks and the private sector.

8. Appendix A: Control objectives in the framework

The appendix contains the complete list of the control objectives in the framework for secure and resilient CBDCs, as organised by the seven steps.

Prepare

	Capability	Control objective	Theme
1	Enterprise Focus	The board and senior leadership of the central bank take an active role and accountability in establishing a broad understanding of the security and resilience approach for the CBDC system, through clear communication of its objectives to all relevant parties, including bank personnel, third parties and intragroup entities.	Baseline applied to CBDC
2	Enterprise Focus	Senior management of the central bank implement the security and resilience strategy for the CBDC solution and ensure that financial, technical and other resources are appropriately allocated in order to support the central bank's overall security and operational resilience approach.	Baseline applied to CBDC
3	Enterprise Focus	Information security and resilience roles and responsibilities for the CBDC system are defined and allocated within the central bank. This could include the creation of a dedicated executive-level owner for cyber and physical security, accountable to the senior leadership.	Baseline applied to CBDC
4	Enterprise Focus	The central bank's information security policies are updated to cover CBDC, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed regularly.	Baseline applied to CBDC
5	People Management	The central bank has committed to allocate enough resources to support the implementation and ongoing management of the security and resilience programme for the CBDC system as well as for any enterprise-wide dependencies.	Baseline applied to CBDC

6	Communications	Contact with relevant authorities is established and maintained by the central bank in reporting and resolving incidents affecting the CBDC system.	Baseline applied to CBDC
7	Communications	The central bank has established contact with special interest groups or other specialist security forums and professional associations to receive threat intelligence relevant to the CBDC system.	Baseline applied to CBDC
8	Change Management	Robust change management capabilities are applied to CBDC-related change initiatives affecting people, processes and technologies in the central bank and its service and solution providers.	Baseline applied to CBDC
9	Service Continuity	The central bank has established a service continuity capability that includes a cyber resilience incident response and recovery plan (including defined processes, roles and responsibilities, and technology solutions) that applies to the CBDC system.	Baseline applied to CBDC
10	External Dependencies Management	The central bank's CBDC service continuity plan includes exit strategies to maintain the CBDC system's operational resilience in the event of a failure or disruption at a third party impacting the CBDC system's operations, which should include escrowing the third party's software source code and other artifacts that can be used to reconstruct the software, where applicable.	Baseline applied to CBDC
11	Service Continuity	At least once a year, the central bank reviews, tests and refreshes its processes, resource allocation and toolset that support the incident response plan covering the CBDC components. The test includes its suppliers and third-party providers where appropriate.	Baseline applied to CBDC
12	Compliance	The central bank conducts regular audit reviews (internal and external) of the processes and technologies applied to the CBDC system including security controls, business continuity plans and incident response.	Baseline applied to CBDC

13	Service Continuity	Where required, a backup copy of each of the central bank's CBDC applications and its supporting infrastructure components is maintained in a separate disaster recovery site to provide resilience in case of a disruption of the primary site.	Baseline applied to CBDC
14	Service Continuity	At least once a year, the central bank tests the resilience of its CBDC solution.	Baseline applied to CBDC
15	Service Continuity	The central bank has established and tested its technologies and controls for any remote management of systems, balancing security and business continuity needs.	Baseline applied to CBDC
16	People Management	The central bank has implemented an employee termination policy and associated access management and monitoring procedures to make sure that terminated employees cannot compromise the confidentiality, integrity and availability of the CBDC system.	Baseline applied to CBDC
17	Change Management	The central bank has established a configuration change controls process for its CBDC system.	Baseline applied to CBDC
18	Environmental Control	The central bank ensures that physical and environmental security best practices are applied to all its CBDC technology hosting facilities, and reviews such practices on a regular basis.	Baseline applied to CBDC
19	Environmental Control	All of the facilities used to operate the CBDC system are protected from power failures and other disruptions caused by failures in supporting utilities.	Baseline applied to CBDC
20	Environmental Control	Cables carrying power, data or supporting information services for the CBDC systems are protected from interception, interference or damage.	Baseline applied to CBDC
21	Environmental Control	Protection against malware, including ransomware, is implemented and supported by appropriate user awareness and regular mandatory training, including attestation to complying with policies and processes in a code of conduct.	Baseline applied to CBDC

22	External Dependencies Management	The central bank has defined and implemented processes and procedures to manage the information security and supply chain risks associated with the use of a supplier's products or services for the CBDC system, including due diligence in selecting, contracting, ongoing monitoring, assurance and audit, exit strategy and offboarding.	Baseline applied to CBDC
23	External Dependencies Management	The central bank has validated the integrity of any hardware and external software used in the CBDC system.	Baseline applied to CBDC
24	Training and Awareness	The central bank has informed and trained its internal personnel, both regular and privileged users, about their roles and responsibilities with regard to the CBDC solution, including its security and resilience.	Baseline applied to CBDC
25	Identity and Access Management	The central bank has established an identity and access life cycle management process to assign, review, and re-certify its internal users' role-based access privileges to all its CBDC system components.	Baseline applied to CBDC
26	Service Continuity	The central bank has implemented and tested a break-glass solution to allow privileged access for managing the CBDC sysem in case of a failure in the regular access control system.	Baseline applied to CBDC
27	Identity and Access Management	The central bank has implemented multifactor authentication for all internal users' access to its financial systems, including hardware-based multifactor authentication for its privileged users.	IT modernisation
28	Application Security	The central bank has integrated information security into its process for managing application development, including a security architecture review function and security testing carried out by a team that is independent of the project team, and requires CBDC applications to pass security testing before any major release can go into production.	Baseline applied to CBDC
29	Application Security	The central bank has implemented its application security testing function and processes, including a combination of automated and manual testing, with both static	Baseline applied to CBDC

		and dynamic code analyses, covering both custom-developed and third-party code (open source, COTS, etc), with a risk-based framework for deciding whether a new application or release can go into production.	
30	Application Security	The central bank has implemented security gates in its DevSecOps pipelines to automate the security testing of its applications, including but not limited to software composition analysis, static code analysis, dynamic application scan, configuration checks, etc, and uses a risk-based approach to decide whether the pipeline needs to stop or can move forward.	IT modernisation
31	Application Security	The central bank has set up separate development, testing and production environments for its applications, with separate access control and appropriate security measures configured for each.	Baseline applied to CBDC
32	Technology Management	Where possible, the central bank has implemented security guardrails to leverage capabilities in the underlying platform to prevent CBDC applications and infrastructure configurations from deviating from the security baseline.	IT modernisation
33	Service Continuity	The central bank has adopted a microservice architecture and enabled auto-scaling where feasible and appropriate for CBDC applications and modules, and has implemented a strategy to migrate such microservice modules to a new infrastructure when a hosting facility is having issues.	IT modernisation
34	Change Management	The central bank has adopted an agile application deployment and roll-back strategy (combined with the microservice architecture where applicable) for the CBDC system, including the "blue/green deployment" approach where appropriate, to increase application resilience when deploying changes.	IT modernisation

35	Application Security	The central bank has implemented DevSecOps pipelines and/or provisioning and configuration management scripts to automate infrastructure and environment management for its CBDC applications, with little or no manual access to such environments during normal operations.	IT modernisation
36	Identity and Access Management	Where possible, the central bank enforces just-in-time authorisation for administrators to manually manage the CBDC technology components, with detailed logging of who performed what activities, at what time, and using what network devices.	IT modernisation
37	Network Security	The central bank applies network security best practices in areas such as DDoS protection, firewall, intrusion detection and prevention, etc for all its technology environments that support the CBDC, and conducts network-level penetration tests on a regular basis.	Baseline applied to CBDC
38	Network Security	The central bank keeps its regular employee users outside of the corporate network that is directly or indirectly connected to its CBDC system.	IT modernisation

Identify

	Capability	Control objective	Theme
1	Enterprise Focus	The central bank's role in the CBDC ecosystem is defined and communicated.	CBDC-focused
2	Asset Definition and Management	The central bank has developed and maintained an inventory of information, systems and other digital assets for the CBDC solution and their interdependencies, assigned owners for such assets, and received acknowledgment from the owners.	Baseline applied to CBDC
3	External Dependencies Management	The central bank has identified all external dependencies related to its CBDC solution, and has assigned internal owners and received acknowledgment from the owners.	Baseline applied to CBDC

4	Risk Management	The central bank has identified and documented both internal and external threats to the CBDC solution, and formulated its risk response to the threats to which its CBDC solution could be vulnerable, with established controls to mitigate risks to an acceptable level. The central bank has established a process to continuously monitor and update such threats, vulnerabilities, risks and controls.	Baseline applied to CBDC
5	Risk Management	The central bank has established sufficient controls and procedures to identify new threats (internal and external) and new vulnerabilities in its CBDC system and supporting environment, and uses its risk management process to analyse and manage these new threats and vulnerabilities.	Baseline applied to CBDC
6	Service Continuity	The central bank has defined its CBDC system's resilience requirements at all levels and components, and for all operating states (eg under duress/attack, during recovery, normal operations), in order to support the service continuity plan.	Baseline applied to CBDC
7	Service Continuity	The central bank has defined its strategy for CBDC transaction integrity during system or technology failures, including how to resume interrupted transactions, how to restore balances and positions when value is lost in an interrupted transaction, etc.	CBDC-focused
8	Service Continuity	Operating procedures for the central bank's CBDC solution are documented and made available to personnel who need them, including during emergencies and potential outages of the central bank's regular corporate network.	Baseline applied to CBDC
9	Compliance	Legal and regulatory requirements and other obligations relevant to information security, data protection, data privacy, etc related to the CBDC and the central bank's approach to meet these requirements are identified, documented and kept up to date.	Baseline applied to CBDC

10	Application Security	The central bank has identified, specified and approved information security requirements for its CBDC application or application components, to be either developed or procured.	Baseline applied to CBDC
11	Service Continuity	The central bank has decided whether it is going to support offline CBDC payments when either the back-end CBDC service is not reachable or the end user has no access to a smartphone, internet, or power.	CBDC-focused
12	Technology Management	If applicable, the central bank has defined security requirements for offline CBDC payment solutions so that risks associated with the use of offline payment technologies are within the central bank's risk appetite/tolerance.	CBDC-focused
13	Technology Management	The central bank has specified requirements for CBDC wallet providers to allow such wallets to interoperate with each other so that end users can continue to use the CBDCs in the wallet in case the wallet provider has a service outage, etc.	CBDC-focused
14	Compliance	The handling of personally identifiable information (PII) in the central bank's CBDC solution meets applicable legal and regulatory requirements in the jurisdiction, with appropriate disclosure to end users where applicable.	Baseline applied to CBDC

Protect

	Capability	Control objective	Theme
1	Network Security	The central bank establishes a separate network segment for its CBDC components where possible.	Baseline applied to CBDC
2	Application Security	The central bank has implemented layered defence for its CBDC applications and APIs, including web application firewall, API gateway with security and rate limiting enabled, data encryption in transit, authentication, authorisation, and logging and monitoring per the security policies of the central bank.	Baseline applied to CBDC

3	Service Continuity	The central bank's CBDC solution is implemented with redundancy and failover capabilities that are sufficient to meet availability requirements, considering a failure in application, virtual machine, database, storage, hardware, networks, power, data centre, etc.	Baseline applied to CBDC
4	Application Security	The central bank has designed the CBDC architecture in such a way as to minimise the attack surface for sensitive data and CBDC value, for example by reducing the number of parties in the ecosystem to hold financial value or store/process unencrypted sensitive data.	CBDC-focused
5	Identity and Access Management	The central bank leverages the national ID regime available in its jurisdiction to define end user (including businesses) identity and authentication strategy for its CBDC solutions, when user identification is required.	CBDC-focused
6	Application Security	The CBDC system has implemented capabilities to block certain CBDC wallets (online or offline) that have shown suspicious behaviour so that they can no longer be used to receive CBDCs or make CBDC payments until the suspicion is resolved.	CBDC-focused
7	Application Security	The central bank applies secure coding principles and practices to the development of its CBDC applications. All software code related to the creation, transfer and destruction of CBDCs must be peer-reviewed to validate the integrity of the code logic.	Baseline applied to CBDC
8	Technology Management	Configurations (including security configurations) for CBDC components managed by the central bank, such as hardware, software, services and networks, are established, documented, implemented and monitored for any changes.	Baseline applied to CBDC
9	Technology Management	The central bank has hired a reputable third party to review and test its DLT architecture design to make sure its consensus algorithm, together with the network architecture and strategy to manage hard/soft forks, would be fault tolerant and Byzantine fault tolerant (if	DLT

		required), with residual risks accepted by the central bank.	
10	Technology Management	The central bank has hired a reputable third party to review and test its DLT design to make sure transaction finality under all circumstances meets the central bank's requirements on timeliness and resilience.	DLT
11	Technology Management	The central bank has hired a reputable third party to review and test any cross-chain bridges that are used to send its CBDC to another system, or other digital currency tokens to the central bank's system, to ensure the integrity of such bridges.	DLT
12	Technology Management	The central bank has defined and tested a strategy for making necessary changes to the DLT architecture, including switching to a different consensus protocol, to ensure that CBDCs (including those issued before the change) and payment operations can continue to function.	DLT
13	External Dependencies Management	The central bank ensures that any third-party facilities that can trigger CBDC transactions, such as oracles, have a robust architecture that meets the central bank's resilience requirements.	Baseline applied to CBDC
14	Technology Management	The central bank has implemented data encryption at rest and data encryption in transit where applicable in its CBDC solution, using approved cryptography algorithms and configurations.	Baseline applied to CBDC
15	Technology Management	The central bank has securely protected its encryption keys and digital wallet ownership keys related to the CBDC, using secure key vault, with strict access control, strong physical security, and defined key rotation frequency and procedures, based on crypto-durability analysis.	Baseline applied to CBDC
16	Application Security	The central bank has hired a reputable third party to conduct an independent code review and security testing of its key CBDC application	CBDC-focused

		functions, including all smart contracts, with all findings addressed and retested to the central bank's satisfaction.	
17	Technology Management	The central bank has a well defined and regularly tested backup facility and recovery procedure for its CBDC-related encryption keys and digital wallet ownership keys.	Baseline applied to CBDC
18	Identity and Access Management	The central bank requires multi-signature approval for transactions that will generate new CBDCs, or transfer CBDCs with an amount greater than a predefined threshold.	CBDC-focused
19	Service Continuity	Backing up of information related to the CBDC system is conducted, maintained and tested for data restoration by the central bank. At least some copies of the backup are stored in a separate facility that would provide resilience in the event of disruption in the primary facility.	Baseline applied to CBDC
20	Service Continuity	The central bank has defined and tested its plan to maintain the information security of the CBDC systems at an appropriate level during different disruption scenarios.	Baseline applied to CBDC
21	Training and Awareness	End users of CBDC are made aware of their responsibilities in securing their CBDC accounts, wallets and any software or hardware they use to manage their CBDCs.	CBDC-focused
22	Technology Management	CBDC wallet providers have followed the central bank's requirements to make their CBDC wallets interoperable with other CBDC wallets so that end users can continue to use the CBDCs in their wallets in case the wallet provider has a service outage, etc.	CBDC-focused
23	Technology Management	The cental bank has established a mechanism for its CBDC components and CBDC components managed by other parties to have their clocks synchronised to an agreed time source.	Baseline applied to CBDC
24	Technology Management	The CBDC solution supports the secure transfer of an end user's CBDCs from one device or wallet to another, after sufficient user authentication. The process is designed to prevent double-spending, replay, payment	CBDC-focused

		redirection and the use of counterfeited CBDCs.	
25	Service Continuity	The CBDC solution supports the recovery of end users' CBDCs lost due to losing access to their wallet or wallet device, or due to a broken transaction, after sufficient user validation and meeting predefined provisions, wherever possible.	CBDC-focused
26	Application Security	The CBDC mobile app has adopted proper mobile app security mechanisms such as certificate pinning, integration with the key chain or secure enclaves where applicable, etc.	Baseline applied to CBDC
27	Technology Management	CBDC-related information stored on, processed by or accessible via the user's software or hardware (browser, mobile app, hardware devices, etc) is protected for confidentiality and integrity purposes.	CBDC-focused
28	Application Security	The central bank has implemented proper session management for its CBDC applications, including setting proper cookie flags, session timeouts, and continuous validation of the user's trustworthiness, with re-authentication being triggered based on the level of risk of the user-initiated actions.	IT modernisation

Detect

	Capability	Control objective	Theme
1	Technology Management	The central bank has acquired sufficient technologies to support detection of and response to anomalies and applied these technologies to the CBDC components, including vulnerability scans, real-time log collection and correlation using a security information and event management (SIEM) tool, threat hunting, forensics, etc.	Baseline applied to CBDC

2	Monitoring	The central bank has established a baseline of network traffic patterns for users and systems related to the CBDC solution, defined thresholds for alerting, and implemented such alerts.	Baseline applied to CBDC
3	Monitoring	The central bank has established processes to receive, analyse and respond to detected anomalies, imminent cyber threats and reported vulnerabilities related to its CBDC systems, from both internal and external sources (eg internal testing, security bulletins, or security researchers).	Baseline applied to CBDC
4	Monitoring	When an alert is triggered or received, event data related to the central bank's CBDC systems (including user, network, device, software, etc) are available for correlation and analysis to determine whether an anomalous event has occurred and its potential impact, with results reported to management.	Baseline applied to CBDC
5	External Dependencies Management	The central bank routinely assesses its CBDC suppliers and third-party partners using independent attestations or other forms of evaluations to confirm they are maintaining their security and resilience postures and meeting their contractual obligations.	Baseline applied to CBDC
6	Vulnerability Analysis and Resolution	All of the central bank's CBDC system components go through regular security assessments, such as penetration testing and red-teaming, to validate their security posture.	Baseline applied to CBDC
7	Monitoring	The central bank's monitoring function for the CBDC system, including the team and the supporting technologies, operates 24/7, and has resilience and redundancy as required.	Baseline applied to CBDC
8	Vulnerability Analysis and Resolution	The central bank regularly assesses and manages the resilience vulnerabilities related to its CBDC system.	Baseline applied to CBDC

Respond

	Capability	Control objective	Theme

1	Incident Management and Control	The central bank has established and implemented procedures for the identification, collection and preservation of evidence related to CBDC incidents.	Baseline applied to CBDC
2	Incident Management and Control	The central bank has established a CBDC emergency response team that includes representatives from financial intermediaries and other related public and private organisations to coordinate on CBDC-related security information and response actions in case of an incident.	CBDC-focused
3	Incident Management and Control	The central bank executes its response plan upon occurrence of an incident related to its CBDC systems, including root cause analysis, containment, mitigation/eradication and service restoration.	Baseline applied to CBDC
4	Incident Management and Control	The central bank's personnel know their roles and order of operations when responding to an incident related to its CBDC system.	Baseline applied to CBDC
5	Communications	The central bank follows its incident response plan for information-sharing and collaboration with stakeholders when responding to a CBDC-related incident.	Baseline applied to CBDC
6	Vulnerability Analysis and Resolution	The central bank actively mitigates newly identified vulnerabilities related to its CBDC system, and documents accepted risks.	Baseline applied to CBDC

Recover

	Capability	**Control objective**	**Theme**
1	Incident Management and Control	The central bank conducts regular tabletop exercises to simulate scenarios that have caused disruption of the CBDC systems, and walks through the recovery plan to identify gaps and improvement areas, using the predefined recovery time objective (RTO) and recovery point objective (RPO) as benchmarks.	Baseline applied to CBDC

2	Incident Management and Control	The central bank executes its recovery plan, including communicating its recovery activities to internal and external stakeholders as well as executive and management teams in a timely manner, after the CBDC incident has been analysed with the root cause understood.	Baseline applied to CBDC
3	Incident Management and Control	The central bank ensures data integrity is preserved during the recovery process, including the status of all CBDC transactions and member positions at the time of a disruption.	CBDC-focused
4	Incident Management and Control	The central bank takes all necessary steps to repair its reputation after a CBDC incident.	Baseline applied to CBDC

Adapt

	Capability	Control objective	Theme
1	Technology Management	Where feasible, the central bank has adopted adaptive technologies in its solution architecture to fully leverage auto-scaling and elastic services to cope with periodic spikes of normal or attack traffic.	IT modernisation
2	Incident Management and Control	The central bank has implemented a process to learn from CBDC incidents affecting its own or other CBDC solutions to gain new insight with regard to mitigations, capabilities, technologies and processes.	Baseline applied to CBDC
3	Incident Management and Control	The central bank continuously improves its incident detection, response and recovery processes.	Baseline applied to CBDC
4	Technology Management	After each incident, the central bank reviews its security and resilience architecture to see if changes should be made to prevent such incidents or respond to them automatically in the future.	Baseline applied to CBDC
5	Technology Management	The central bank has defined and tested a strategy to switch its CBDC system to more secure cryptographic algorithms when an	CBDC-focused

		existing one is deemed unsecure or vulnerable to maturing quantum technologies, including algorithms used in CBDC components managed by other institutions in the ecosystem.	

9. Appendix B: Enabling technologies for security and resilience

The following technologies and techniques could be adopted to better achieve security and resilience when implementing and operating CBDC systems.[45]

- **Auto-scaling**: This is an infrastructure management method that is often available in cloud computing environments. It dynamically adjusts the amount of computational resources in a pool of virtual servers based on the load that the application is experiencing. This includes automatic scaling up and scaling down, so that the application owner gets the desired performance when needed, and pays for fewer resources when the traffic is light for the application.
- **Blue/green deployment**: This is an application release model that gradually transfers user traffic from a previous version of an application or microservice to a new release – with both versions running in production. The old version is called the blue environment, while the new version is known as the green environment. Once production traffic is fully transferred from blue to green, blue can become standby in case of roll-back or pulled from production and archived. This technique could be suitable for certain changes, provided that having two different versions of the application would not introduce any unfair experience among different user populations.
- **Cloud computing**: The ability to leverage computing platforms managed by a service provider and comply with an organisation's risk and legal framework is a significant step for an organisation. A cloud platform could potentially provide a more resilient infrastructure, as cloud providers typically have resources and advanced techniques to secure the service they provide, but customers have to do their part as security is a shared responsibility when using cloud services.
- **Contingency technologies**: As the ability to respond to and recover from incidents is a key component of being cyber-resilient, central banks need to establish capabilities with the understanding that certain functions may not be working during incident response. For example, establishing an out-of-band communications channel is prudent in case users cannot securely log in or use the regular communication channels because of a service outage associated with the incident. Similarly, a break-glass identity and access management solution should be established for system administrators in case the regular solution is not working during an emergency. Finally, a digital vault should be established that contains all that is needed to jump

[45] This list excludes the fundamental cyber security technologies and systems that would already be in place such as those for intrusion detection and prevention (IDS/IPS), firewalls, malware and virus scanning, identity and access management, multifactor authentication, authorisation, monitoring and audit and SIEM systems as well as physical access controls.

start the most critical functions for the business continuity needs of the CBDC system.

- **DevSecOps**: A short name for development, security and operations, this pipeline approach for software development and operation life cycle focuses on automation and codification of every step. With DevSecOps, as soon as a new piece of code is checked into a project's code repository, the pipeline will automatically compile it, deploy it in a test environment, run unit test cases, integration test cases, trigger security tests, etc, and eventually use the test results to automatically decide whether this change can move on to be deployed to trigger the next level of validation. On the deployment and operation side, the environment configurations and operational parameters are defined in the pipeline, using infrastructure-as-code, etc. This practice greatly shortens the timeline for deploying new changes, and reduces the amount of manual work in operating the system in production. It improves security through both automated security checks built into the pipeline, and reduced manual intervention by system administrators during operation.

- **Edge computing**: This could enable the continuation of payment services to a certain extent even when the CBDC services provided by the central bank or commercial banks are temporarily not available. Edge computing could also be leveraged to reduce the load on such central services and therefore reduce the risk of failure. Edge computing could help enable the distributed architecture a CBDC system may need.

- **Identity-as-a-service**: This allows users to connect to and use identity management services from the cloud, leveraging the service provider's vast amount of data about identities and ongoing cyber attacks against them. This allows an organisation to validate users while they are still outside its network perimeter, and fully leverage identity as part of the perimeter defence.

- **Infrastructure-as-code with security guardrails**: As part of IT modernisation and the adoption of DevSecOps, infrastructure specification can now be fully expressed as code. Platform-neutral specifications such as the open source Terraform tool make this approach even more appealing. Security guardrails can be embedded into such specifications to ensure that all workloads deployed into the enterprise's account operate within well defined security boundaries. Such a security guardrail can provide a certain level of assurance of the security posture of all workloads that are covered by it.

- **Microservices, container architecture and microservice management framework**: Being able to decompose system functions into small chunks in the form of microservices has demonstrated advantages in terms of agility and manageability. Deploying such microservices in containers allows such modules to be easily shifted among virtual machines or even across different computing platforms, for example between an on-premises data centre and a cloud platform. In addition, by adopting an open standard technology such as Kubernetes to manage microservices deployed in containers, one not only gets auto-scaling and other benefits, but can also move the workload to other platforms that support Kubernetes. This provides greater resilience and avoids vendor and technology lock-in.

- **Offline technologies**: Offline payment technologies could provide a layer of resilience for payment systems in the event of a temporary outage or where internet or telecommunications connectivity is unavailable. These include technologies for offline purses, payment generation and transmission, fraud detection, etc.[46]
- **Privacy-enhancing technologies**: When it comes to end user data, even though most central banks may choose not to directly interact with end users, there may be times when it becomes necessary for a central bank to investigate CBDC transaction irregularities, in which case it may become necessary to access user data. Privacy-enhancing technologies such as differential privacy, zero-knowledge proof and federated learning can be leveraged to gain insight from data without breaching end user privacy. Such technologies could enhance a central bank or financial institution's ability to respond to and recover from incidents with minimum impact.[47]
- **Zero-trust security**: This refers to a collection of security practices including strong multifactor authentication, using identity as part of the access perimeter, providing employees access to the applications they need without giving them access to the corporate network, continuous security posture monitoring of a user's application session, and granular network segmentation. These practices are built on years of lessons learned from security breaches and meant to reduce an enterprise's security attack surface or contain the impact of inevitable breaches caused by phishing and other common attacks.

Central banks should assess the benefit and cost of adopting the above technologies as part of their CBDC projects. As technologies are always evolving, central banks should continuously watch for the adoption readiness of new technologies, and decide if and when such technologies should be leveraged for achieving their business objectives.

[46] See BISIH (2023a).

[47] See BISIH (2023b).

10. Glossary

Advanced persistent threat (APT): A cyber attack performed by a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorised access to a computer network and remains undetected for an extended period. The adversary typically studies the victim's network and information assets during the period in order to exfiltrate a large amount of data, or find an optimal moment to trigger an act that will result in a large-amount financial gain by the attacker or severe damage to the victim.

Attack surface: The collective components of an information system (software, hardware, network, processes and human) that allow an attacker to probe, manipulate, control or maintain a presence in the system and potentially compromise its confidentiality, integrity or availability. A smaller attack surface means that the system is less exploitable and an attack less likely.

Baiting: A form of social engineering where an attacker uses a false promise, rewards or other means to infect a victim's system(s) and extract sensitive information. For example a target may receive enticing offers, some may appear legitimate, requiring them to download some content which then infects their system with malware. Targets may receive promotional good such as branded USB pen drives, which when inserted into their machine will infect it with malware. Sometimes, such media are left in conspicuous areas where an individual may pick it up out of curiosity. In other cases, an attacker may pretend to be from technical support from a suppler, and could trick a target into disclosing details or insert an infected device into their system.

Blue team: A group of individuals from within the organisation who test information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and make certain all security measures will continue to be effective after implementation.

Byzantine fault tolerance: The capability for a system to keep functioning correctly as long as a certain majority (eg two thirds) of the network agree or reach consensus. This property is important in a system where some actors could either fail or act maliciously.

Control objective: A statement that defines the aim or purpose of specific controls at an organisation or service organisation in order to address the risks that the controls are intended to mitigate. Criteria are often defined for evaluating the effectiveness of controls associated with the control objective.

Cyber risk management: The process used by an organisation to establish an enterprise-wide framework to manage the likelihood and impact of a cyber attack and develop strategies to mitigate, respond to, learn from and coordinate its response to a cyber attack. The management of an organisation's cyber risk should support the business processes and be integrated in the FMI's overall risk management framework.

Cyber threat intelligence: Information about an ongoing cyber attack that is detected by other organisations or indication of an imminent attack from known actors, sometimes with sufficient information for mitigating the impact of such an attack.

DevSecOps: Stands for development, security and operations. It is an approach to culture, automation and platform design that integrates security as a shared responsibility throughout the entire IT life cycle, making security validation an embedded component of the software development and integration pipeline, and an embedded part of the system operation processes from provisioning and monitoring to change management.

Distributed denial of service (DDOS): A cyber attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. It is accomplished by flooding the targeted machine or resource with superfluous requests from many different sources in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Man-in-the-middle attack: A cyber attack in which the attacker secretly intercepts and possibly alters the communications between two parties who believe they are directly communicating with each other, by positioning themselves between the communicating parties.

MITRE ATT&CK: A knowledge base and model of cyber adversary behaviour, based on real-world observations, that documents their tactics, techniques and common knowledge. It is a framework and tool that helps organisations understand and improve their security readiness and uncover vulnerabilities in their defences.

Phishing: A form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware. **Purple team**: A group of cyber security professionals, typically consisting of members from both the blue and red teams, who simulate malicious attacks and penetration testing in order to identify security vulnerabilities and recommend remediation strategies for an organisation's IT infrastructure.

Recovery point objective: A period of time in which an enterprise's operations must be restored following a disruptive event, for example a cyber attack, natural disaster or communications failure, ensuring that the restored operations contain the most up-to-date version of the enterprise's data.

Recovery time objective: The maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs.

Red team: An independent group that challenges an organisation's cyber resilience by simulating adversarial attacks to test its defences and improve their effectiveness. A red team assesses the organisation's cyber resilience from an adversary's perspective.

Risk appetite: The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives.

Side-channel attack: A security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware rather than targeting the program or its code directly.

SIM swap: An attacker knows a victim's mobile phone number, contacts the victim's mobile carrier and convinces them to port the victim's mobile phone number to a SIM card that the attacker controls. Once this change happens, calls and text messages to the victim's mobile phone number will be received by the attacker.

Spear phishing: A form of social engineering, similar to phishing, not typically initiated by random hackers but instead by certain threat actors targeting a specific organisation or individual to gain unauthorised access to sensitive information.

Threat hunting: A proactive approach to identifying previously unknown or ongoing non-remediated threats within an organisation's network. It typically involves going through network traffic logs and using knowledge of normal traffic patterns or known indications of compromises to identify anomalies.

Zero-day: A computer-software vulnerability previously unknown to those who should be interested in its mitigation, but which becomes known to attackers, who actively exploit it before it is known to the organisations which use the vulnerable software or before a patch has become available to mitigate the vulnerability.

Zero-knowledge proof: A method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is true.

Zero trust: A cyber security strategy that starts with the "assume breach" mindset, takes the "always verify" approach to users, devices, networks and applications, and emphasises the "least privileges" principle when granting an entity access to network resources.

11. References

Atlantic Council (2022): *Missing key: the challenge of cybersecurity and central bank digital currency*, June.

Auer, R and R Böhme (2020): "The technology of retail central bank digital currency", *BIS Quarterly Review*, March, pp 85–100.

Bank for International Settlements (2022): *Annual Economic Report 2022*, June.

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

——— (2021): *Central bank digital currencies: system design and interoperability*, September.

Basel Committee on Banking Supervision (2018): *Cyber-resilience: range of practices*, December.

BIS Committee on Payments and Market Infrastructures (BIS CPMI) and International Organization of Securities Commissions (IOSCO) (2012): *Principles for financial market infrastructures*, April.

——— (2016): *Guidance on cyber resilience for financial market infrastructures*, June.

BIS Innovation Hub (2023a): *Project Polaris: a handbook for offline payments with CBDC*, May.

——— (2023b): *Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders*, May.

——— (2023c): *CBDC cyber threat modelling gaps: lessons learned from mapping DeFi cyber attacks to the MITRE ATT&CK® framework*, July.

BIS Innovation Hub, Bank of Israel, Central Bank of Norway, Sveriges Riksbank (2023): *Project Icebreaker: breaking new paths in cross-border retail CBDC payments*, March.

BIS Innovation Hub and Hong Kong Monetary Authority (2022): *Project Aurum: a prototype for two-tier central bank digital currency (CBDC)*, October.

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

BIS Innovation Hub, Reserve Bank of Australia, Central Bank of Malaysia, Monetary Authority of Singapore and South African Reserve Bank (2022b): *Project Dunbar: international settlements using multi-CBDCs*, March.

Cloud Security Alliance (2017): *Security guidance for critical areas of focus in cloud computing,* v4.0, July.

Doerr, S, L Gambacorta, T Leach, B Legros and D Whyte (2022): "Cyber risk in central banking", *BIS Working Papers*, no 1039, September.

European Union Agency for Cybersecurity (ENISA) (2011): *Enabling and managing end-to-end resilience*, January.

International Organization for Standardization (ISO) (2022): *Blockchain and distributed ledger technologies: reference architecture, first edition (ISO 23257)*, February.

——— (2022a): *Information security management systems: requirements, third edition (ISO 27001)*, October.

Kosse, A and I Mattei (2022): "Gaining momentum – results of the 2021 BIS survey on central bank digital currencies", *BIS Papers*, no 125, May.

Ngo, K (2023): *Side-channel analysis of post-quantum cryptographic algorithms*, March.

National Institute of Standards and Technology (NIST) (2018): *Framework for improving critical infrastructure cybersecurity, version 1.1*, April.

——— (2020): "Zero trust architecture", *SP 800-207*, August.

Payment Card Industry Security Standards Council (2022): *Payment card industry data security standard – requirements and test procedures version 4.0*, March.

Software Engineering Institute (SEI) (2010): *CMMI® for development, version 1.3*, November.

——— (2016): *CERT Resilience Management Model, version 1.2*, February.

Statista (2022): *Number of Internet of Things (IoT) connected devices worldwide 2019-2021*, *with forecasts to 2030*, www.statista.com/statistics/1183457/iot-connected-devices-worldwide, November.

US Department of Defense (2019): *Enterprise DevSecOps reference design*, August.

World Economic Forum (2023): *Global Risks Report 2023*, January.

World Informatix Cyber Security (2021): *The Bangladesh cyber heist: 5 years later*.

12. Acknowledgments

Bank for International Settlements

Beju Shah (Head of Nordic Centre, BIS Innovation Hub)

William Zhang (Adviser, BIS Innovation Hub)

David Whyte (Head of BIS Cyber Resilience Coordination Centre)

Sameh Mekhail (Deputy Head of BIS Cyber Resilience Coordination Centre)

Wipawadee Auyporn (Security specialist, BIS Cyber Resilience Coordination Centre)

Jonathan Lee (Security specialist, BIS Cyber Resilience Coordination Centre)

PA Consulting (quality assurance)

Andreas Joachim Nielsen (Consultant)

Sam Lascelles (Managing consultant)

Alexander McGill (Associate Partner)

David Biggin (Partner)

Special acknowledgments for input, review, feedback and support

BIS Innovation Hub: Cecilia Skingsley, Ross Leckow, Cristina Picillo, Esther Rey Losada, Daniel Eidan, Balthazar Rodriguez, Jack Ho, Leanne Zhang, Ben Dovey, Susanne Bohman, Grimur Sigurdarson, Bjorn Segendorff, Hachem Hassan, Xin Zhang.

Tomer Mizrahi (CTO, Bank of Israel), BIS Innovation Network Cybersecurity Working Group members, Arvinder Bharath (Digital Expert Lead, IMF), Frankosiligi Solomon (Senior Digital Expert, IMF), Yu Gao (Security Architecture Lead, World Bank), Axel Kristinsson (Central Bank of Iceland), Anders Flaglien (ICT Security, Norges Bank), Ian Vitek (Security Specialist, Sveriges Riksbank), Henrik Axelsson (IT Security Architect, Sveriges Riksbank), Viktor Mollborg (Business Architect, Sveriges Riksbank).

ISBN 978-92-9259-654-5