Building the Digital Asset Securities Ecosystem

May 2024

DIGITAL ASSET SECURITIES CONTROL PRINCIPLES: A FRAMEWORK FOR ADOPTION

DTCC clearstream DEUTSCHE BÖRSE GROUP euroclear

In collaboration with BCG

May 2024

Building the Digital Asset Securities Ecosystem

An Industry Paper from DTCC, Clearstream, and Euroclear with the collaboration of BCG

Table of Contents

Letter from the CEOs

Dear industry colleagues,

Time and again, the global financial markets have leaned on financial market infrastructures (FMIs) to drive change. As we are in the midst of rapid evolution in distributed ledger technology (DLT) and digital asset securities (DAS), DTCC, Clearstream, and Euroclear have partnered to play a lead role in the development and adoption of this technology. Between them, the FMIs have decades of experience, a vast network of client relationships from nearly every corner of the financial markets, and a strong track record of supporting market evolution – which has earned the FMIs the trust and respect of market participants, regulators, industry associations, and others. The adoption of digital technology presents opportunities and challenges that require a cohesive, strategic approach, emphasizing the need for collaboration to effectively integrate these innovations into the global financial ecosystem.

The beginning of our collaboration was marked by our first white paper, "Advancing the Digital Asset Era, Together." Building on this, we have worked together to develop the "Digital Asset Securities Control Principles" (DASCP), which are presented in this white paper. The principles serve as a set of guidelines underpinning our collective resolve to uphold the highest standards of integrity, security, and interoperability. This framework is crucial for creating an inclusive, resilient financial ecosystem that is adaptable to technological advancements and responsive to diverse market needs. We would like to thank BCG for its valuable support in enriching and testing this framework.

The DASCP marks the starting point of further industry-wide engagement to enable standardization, drive adoption, and unlock value. To achieve these goals, we intend to put these principles into action. By leveraging them in our digital asset activities, we will effectively demonstrate to clients, regulators, and the broader industry that digital asset securities can be just as safe and secure as traditional assets. We will also advise and support market participants as they leverage the principles in their own business activities.

Ultimately, we believe that industry collaboration is not only the most expedient way – but also the most effective way – to build a robust global digital assets ecosystem. We invite you to join us in this exciting journey that has the potential to redefine global finance, ensuring that this digital transformation benefits the ecosystem and contributes to sustainable economic growth. We look forward to your support and engagement as we collectively expand upon these principles, setting new standards for financial markets worldwide.

Sincerely,

Frank La Salla
CEO, DTCC

Samuel Riley
CEO, Clearstream Securities Services

Valérie Urbain
CEO, Euroclear

"Ultimately, we believe that industry collaboration is not only the most expedient way – but also the most effective way – to build a robust global digital assets ecosystem."

Executive Summary

This white paper presents a comprehensive set of risk management principles and controls designed to unlock the transformative nature of distributed ledger technology (DLT) in the realm of digital asset securities (DAS), excluding cryptocurrencies. It outlines an industry-wide risk and control framework, which serves as a guide to navigate the current set of challenges, fostering operational excellence in financial markets driven by DLT. Through this structured approach, the white paper aims to facilitate the adoption of tokenization into the financial markets, paving the way for its substantial role in the evolution of finance.

DTCC, Clearstream, and Euroclear have developed the Digital Asset Securities Control Principles (DASCP), utilizing our combined decades of experience to effectively manage regulatory compliance and reduce operational risks. This set of principles outlines a safe and efficient ecosystem, identifies potential risks specific to DAS, and provides appropriate recommendations for controls to mitigate these risks.

In fostering these functions, the DASCP framework is designed to be asset class agnostic and technologically neutral, ensuring its adaptability to the diverse operational requirements of organizations across the financial ecosystem.

This framework serves multiple functions:

Regulatory Compliance and Market Integrity:

ensures that DAS operations align with existing and evolving regulatory frameworks, maintaining legal and market integrity.

Risk Management:

provides a structured approach to identify, assess, and manage the specific risks associated with DAS, enhancing market stability and security.

Market Adoption:

facilitates the broader adoption of DAS by setting clear guidelines that will reduce the barrier to entry for new participants.

Interoperability and Efficiency:

provides the basis for subsequent standardization that encourages interoperability between diverse platforms and systems (e.g., other blockchain platforms, legacy, and third-party systems, etc.), crucial for efficient transactions across market players.

Trust Building:

builds trust among issuers, investors, regulators, and market participants, fundamental for sustainable market growth.

The primary objective of this white paper is to catalyze comprehensive understanding, foster collaboration, and spearhead further advancement within the digital asset ecosystem. To ensure our approach remained objective and well-informed, a comprehensive analysis was conducted. It included reviews of approximately 100 regulations, white papers and expert discussions across multiple jurisdictions, as well as over 20 interviews with key market participants and technology vendors.

The initial development of the DASCP marks the beginning of a more expansive initiative. The DASCP will serve as a baseline to help propel the industry toward standards. To ensure the framework remains reflective of the latest industry developments, we plan to transition the stewardship of these principles to a industry association. We believe that a neutral third-party industry association is best positioned to align the digital asset ecosystem on prioritizing, identifying, agreeing, and adopting standards. This move is designed to position the association to actively engage with the broader ecosystem. This involvement is crucial for the DASCP to serve not just as a set of guidelines but as a dynamic catalyst that drives the conversation forward. DTCC, Clearstream, and Euroclear are committed to advising and supporting this work as it continues.

Key Takeaways

1 **Comprehensive Framework Development:**
Undertook the collaborative development of the Digital Asset Securities Control Principles (DASCP), providing a robust framework to support the evolving digital asset ecosystem. This initiative underscores the commitment of DTCC, Clearstream, and Euroclear to shaping the future of finance through innovative technologies.

2 **Foundational Principles for Industry Standardization:**
Establishes critical principles for the successful adoption of DAS, with the DASCP noted for its asset class and technology agnosticism, making them universally applicable. This neutrality is crucial for facilitating a balanced and inclusive dialogue around standards. By serving as a foundational document, the DASCP aims to spark industry-wide discussions that will help shape robust, comprehensive standards for the digital asset marketplace.

3 **Identifying Risks and Establishing Controls:**
Presents a detailed analysis of the potential risks associated with the adoption of DAS and offers a comprehensive set of controls to mitigate these risks. This proactive risk management is intended to safeguard the integrity and stability of the DAS market.

4 **Encouraging Active Industry Participation:**
Invites all stakeholders to actively participate in the evolution of the DASCP, contributing to a collective effort that shapes the future of digital finance.

5 **Future-Proofing Financial Markets:**
Serves as a blueprint for a common and resilient digital asset securities ecosystem, illustrating how the adoption of these principles can help future-proof financial markets against technological disruptions and regulatory changes.

6 **Transition to Industry-Wide Engagement:**
Highlights the pivotal next step of transitioning the stewardship of the DASCP to an industry association. This move is aimed at fostering broader engagement and ensuring the framework's relevance and dynamism in response to an evolving market and technology landscape.

Introduction: Transforming Capital Markets through Digital Asset Securities

The scope of this paper encompasses digital asset securities (subsequently referred to as "DAS") as defined by GFMA. Specifically, it includes securities that utilize DLT to represent or embody rights similar to those of traditional securities, whether these are issued directly on a blockchain (i.e., native security tokens) or are digital representations (i.e., digital twins) of existing securities (e.g., all forms of equity, debt, derivatives, etc.). These digital assets might provide dividends, voting rights, interest payments, or other rights associated with traditional securities. Excluded from this scope are money or money-like digital assets, such as cryptocurrencies, stablecoins, and central bank digital currencies (CBDCs), which function primarily as means of payment or stores of value.

GFMA - Global Financial Markets Association: Impact of Distributed Ledger Technology in Global Capital Markets, 2023

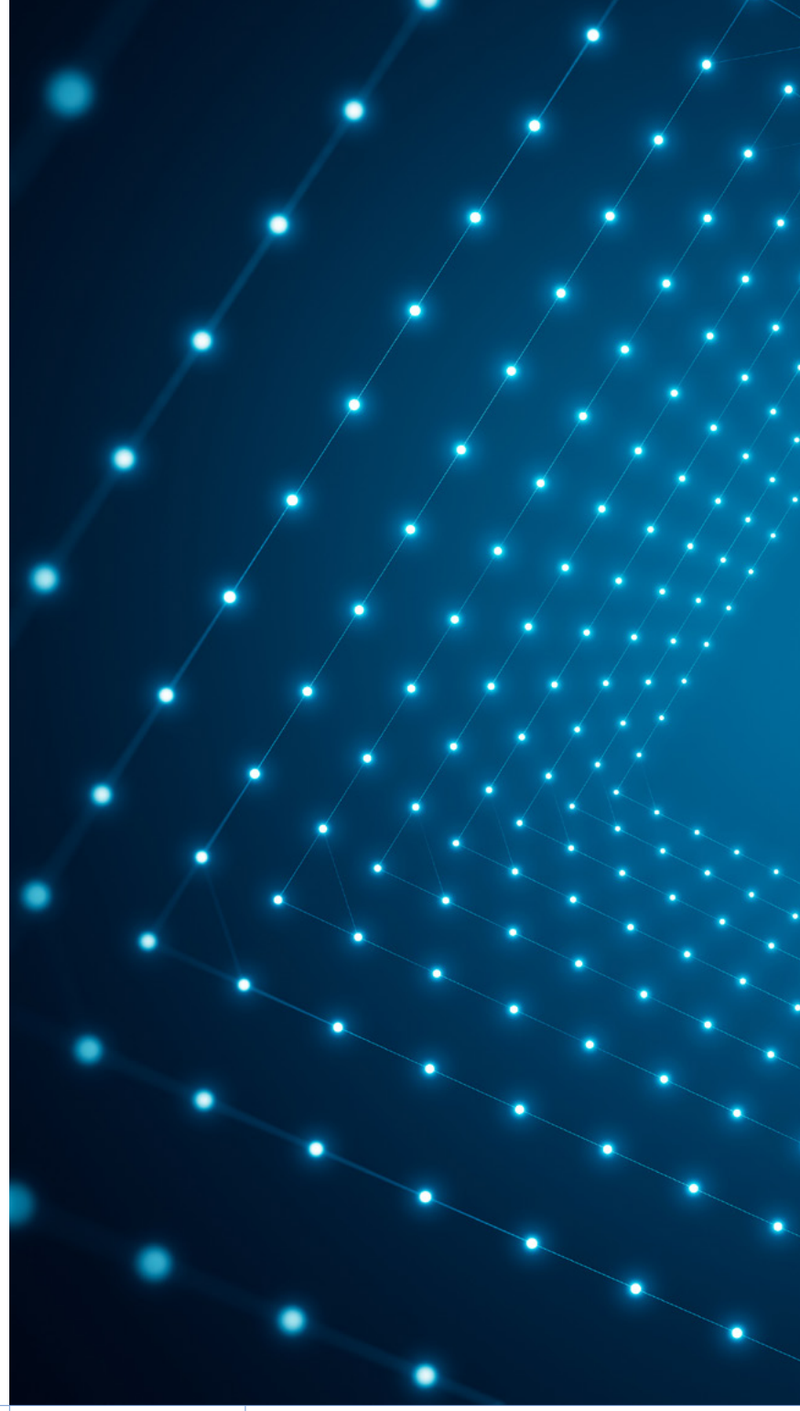
DAS introduce new capabilities in financial services, re-envisioning existing processes and creating trust in real time. Programmability, self-executing automation, and instantaneous reconciliation are key features that have the potential to transform the industry. Central to this transformation is DLT, which enables nearly immediate transaction settlement and creates immutable transaction records. Asset tokenization leverages DLT to create reusable processes that can be quickly adapted to develop new DAS and manage their life cycles, enhancing operational scalability. With these advantages, financial institutions are increasingly investing in DAS to unlock these transformative benefits.

Overall, propelled by smart contracts and automated processes in different areas, annual global infrastructure operational cost savings of ~$15-20 billion have been estimated.[1] Furthermore, due to shortened settlement cycles, DLT impacts on collateral management could release ~$100+ billion annually in freed financial resources.[2]

By 2030, the tokenization of global illiquid assets is projected to be a $16 trillion business opportunity,[3] significantly increasing asset liquidity and expanding market participation. This shift not only promises enhanced efficiency and transparency but also democratizes access to investment opportunities, reshaping the financial landscape for a more inclusive future.

[1, 2] Impact of Distributed Ledger Technology in Global Capital Markets, GFMA, May 2023

[3] Relevance of on-chain asset tokenization in crypto winter, BCG, and ADDX, May 2022



Despite these potential benefits, widespread DLT adoption faces challenges. According to ISSA's recent survey, only 37% of the industry is live with DLT.[4] The full benefits of DAS cannot be realized without more concerted and integrated efforts toward collaboration.

In this context, FMIs have a crucial role to play. Historically the linchpins of the financial system, facilitating clearing, settlement, and recordkeeping, FMIs are now supporting the integration of DAS into the conventional financial fabric. In building upon the foundation laid by our previous collaborative publication, Advancing the Digital Asset Era, Together,[5] this white paper delineates our journey toward adopting Digital Assets.

It recognizes the collaborative efforts needed from FMIs, regulatory bodies, and the broader financial community, advocating for a united approach to address challenges, drive innovation, and seize the opportunities DAS offer. As highlighted by Valérie Urbain, CEO of Euroclear, FMIs are actively working "toward the co-creation of tomorrow's financial system – one that's open, inclusive, efficient, and resilient."[6]

"The digital disruption is there now and ready to scale."

— Dr. Stephanie Eckermann
CEO, Clearstream Banking AG

A Vision for Collaborative Advancement

With this white paper, we are introducing the DASCP, which describes a DAS framework consisting of foundational principles for a secure and efficient ecosystem, risks arising from the implementation and the adoption of the new technology, and controls to effectively mitigate these risks.

During her interview at Sibos 2023, Dr. Stephanie Eckermann, CEO of Clearstream Banking AG, noted that "the digital disruption is there now and ready to scale."[7] The introduction of the DASCP responds to this pivotal realization, acknowledging that scaling DAS is essential for fostering a vibrant ecosystem. By establishing a comprehensive set of controls, the DASCP serves as an initial step toward catalyzing discussions on standardization. This approach positions the DASCP as a critical starting point that paves the way for future endeavors, ultimately helping to drive scale in DAS markets.

[4]DLT in the Real World Survey 2024 – Key Findings, International Securities Services Association, 2024

[5]DTCC, Clearstream, Euroclear, "Advancing the Digital Asset Era, Together", Sept 2023

[6]Valérie Urbain, "Safety by design: Lessons in mainstreaming digital assets with resilience," World Economic Forum, Apr 19, 2024

[7]Dr. Stephanie Eckerman, "Are digital infrastructures finally ready to scale?" Sibos 2023, Sept 2023

"FMIs are actively working toward the co-creation of tomorrow's financial system – one that's open, inclusive, efficient, and resilient."

— Valérie Urbain
CEO, Euroclear

Advancing the Digital Asset Securities Evolution

We believe that the DASCP framework is a foundational starting point for promoting DAS adoption and provides a valuable baseline for the industry:

Guiding the Market Toward Digital Asset Securities Adoption:

With DAS set to transform securities trading and ownership, we are dedicated to clarifying the complexities surrounding these digital innovations and offering insights into how they can enhance the conventional securities markets.

Addressing Challenges and Crafting Solutions for Digital Asset Securities:

The transition to DAS introduces various challenges, from regulatory hurdles to issues of interoperability. Through the DASCP framework, we aim to offer a blueprint that addresses these challenges.

Setting the Stage for Digital Asset Securities Standardization and Interoperability:

For DAS to fully realize their potential, establishing industry-wide standards and ensuring interoperability are vital. This includes engaging not only market participants but also policymakers and regulatory bodies to ensure that the standards align with both industry needs and regulatory frameworks. The DASCP lays the foundation for this comprehensive engagement, aiming to develop standards that facilitate both market growth and regulatory compliance. This collaborative approach is crucial for ensuring the framework's effectiveness and the long-term viability of digital asset securities in the global market.

Fostering Industry Collaboration for Digital Asset Securities Integration:

The successful integration of DAS necessitates joint efforts across the financial ecosystem. We emphasize the importance of collaboration among regulators, technology providers, and financial institutions to establish a cohesive framework that supports the secure and efficient circulation of DAS.

Inspiring Innovation and Future Exploration in Digital Asset Securities:

Looking beyond immediate applications, we are eager to explore the broader possibilities that DAS offer for transforming securities markets and unlocking incremental value for the industry.

Building Adoption and Overcoming Fragmentation

In speaking about the future of digital markets prior to the World Economic Forum in January 2024, Frank La Salla, CEO of DTCC, emphasized the critical need for foundational principles. He noted, "We have initiated a set of control principles that prepare the groundwork for ensuring the emerging tokenized securities market is as efficient and secure as today's securities marketplace. These principles are crafted to lay the foundations, reducing risks by defining clear roles, responsibilities, and the controls necessary for a robust framework."[8] The DASCP is pivotal in this context, designed to address the digital asset landscape's complexities before full standardization can be achieved. The DASCP enhances system resilience, safeguards customer assets, and facilitates seamless transactions through improved connectivity and interoperability, also emphasizing the importance of operational scalability.

The DASCP framework comprehensively covers various value chain activities essential to the life cycle of DAS. These activities include:

- **Issuance:** Involves pre-issuance workflows depending on asset type, registration with Central Securities Depositories (CSDs), and compliance with relevant regulatory frameworks.
- **Clearing:** Encompasses the calculation and request of margins, novation of centrally cleared trades, netting of obligations, and communication of net security / cash obligations.

> **"These principles are crafted to lay the foundations, reducing risks by defining clear roles, responsibilities, and the controls necessary for a robust framework."**
>
> — Frank La Salla
> CEO, DTCC

- **Settlement:** Covers the processes of sending and confirming cash payments, transferring ownership of securities, and ensuring proper reconciliation by involved parties.
- **Custody:** Involves the maintenance, safekeeping, and reporting of ownership records, along with corporate action management on behalf of asset owners.
- **Asset Servicing:** Entails services provided on behalf of the issuer (e.g., processing dividend payments, splits, rights issues, etc.).

It is important to note that the current scope of the DASCP excludes secondary trading activities.

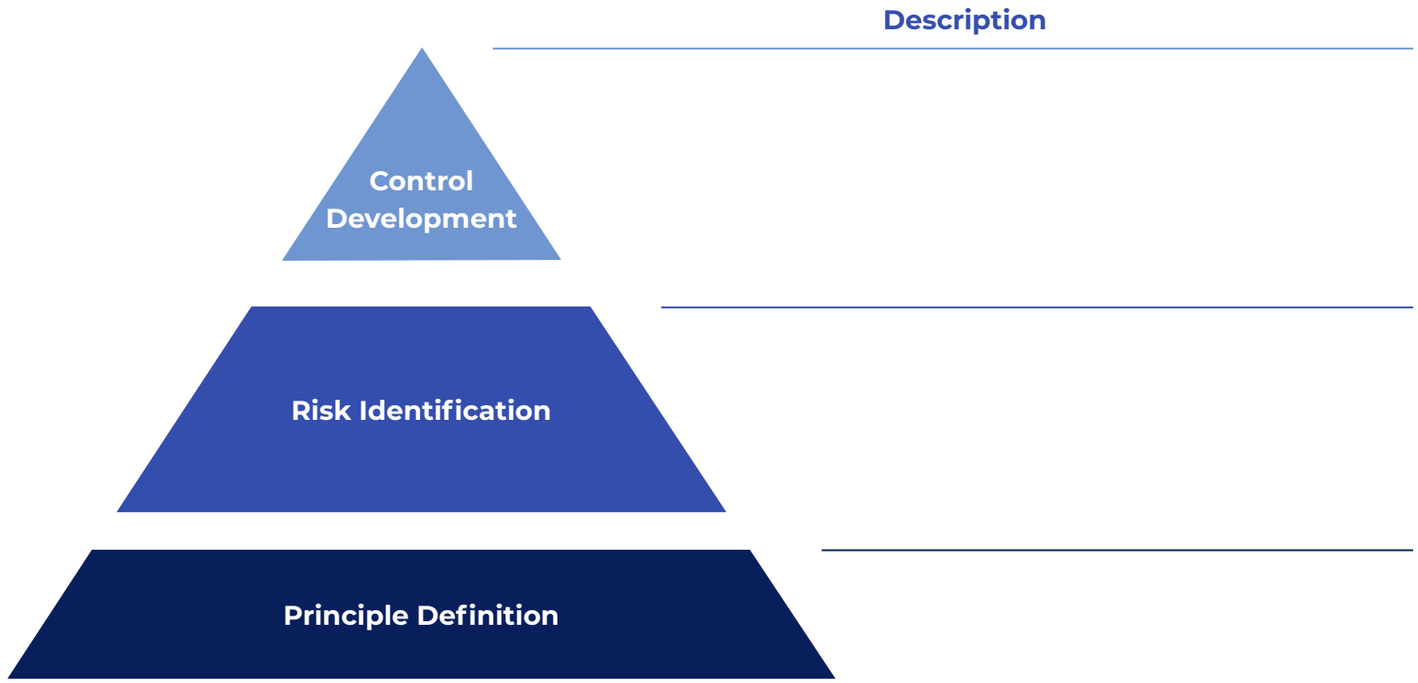
The DASCP framework is designed to be asset class and technology neutral, not advocating for any particular DLT architecture – be it public, private, permissioned, or public permissioned. This ensures its applicability across various DLT platforms without endorsing specific third-party solutions. This technology and asset class agnosticism contributes to the framework's adaptability, ensuring that the DASCP remains relevant and effective amid the rapidly evolving financial landscape.

The DASCP has been methodically assembled and rigorously tested with over 20 market participants. Going forward, we invite all industry stakeholders to engage with and actively drive the evolution of this framework.

[8]Frank La Salla, "Why standards and controls are essential to the future of digital financial markets" World Economic Forum, Jan 16, 2024

To achieve its objectives, the DASCP has been crafted using a structured, layered approach as depicted in the figure to the right and summarized below:

- **Principle Definition Established:** Initially, the DASCP framework identified a set of foundational principles that function as overarching objectives guiding the entire framework.
- **Risk Identification Compilation:** A comprehensive list of risks associated with each principle is compiled, incorporating traditional finance risks adapted for DAS and new risks unique to this sector.
- **Control Development Design:** Controls for each identified risk are then designed, emphasizing flexibility to allow them to serve as adaptable guidelines rather than rigid rules.



Hover over the layers in the pyramid to find out more.

The DASCP was developed in multiple layers along foundational principles, risks, and controls.

At this juncture, the DASCP is not about creating fixed standards; rather, it is laying the necessary groundwork that will inform the development of comprehensive industry standards in the future.

Principles

The rise in DLT initiatives signifies a shift in financial market infrastructure, reminiscent of the robust standards set forth by the Principles for Financial Market Infrastructures (pFMIs) issued by BIS and IOSCO. As tokenization becomes increasingly prevalent, the DASCP has been proactively established to address the challenges of widespread adoption. The DASCP is formulated with an understanding of the core objectives that pFMIs champion: integrity, stability, and confidence in the financial system.

Click on the principles to the right to find out more about each.

The principles below are listed in order of priority, but all are vital to building a secure DAS ecosystem:

Legal Certainty:

Ensuring operations comply with existing laws and regulations to maintain market integrity and investor confidence.

Regulatory Compliance:

Encouraging alignment with regulatory frameworks to build a foundation of trust and safety in digital asset markets.

Resilience and Security:

Developing robust infrastructure capable of resisting disruptions, while protecting sensitive data and ensuring the continuous operation of digital asset services.

Safeguarding Customer Assets:

Implementing governance over smart contracts to manage and protect customer assets within the digital asset ecosystem securely.

Connectivity and Interoperability:

Facilitating transactions and flexible settlements across diverse networks to enable the seamless transfer and settlement of DAS.

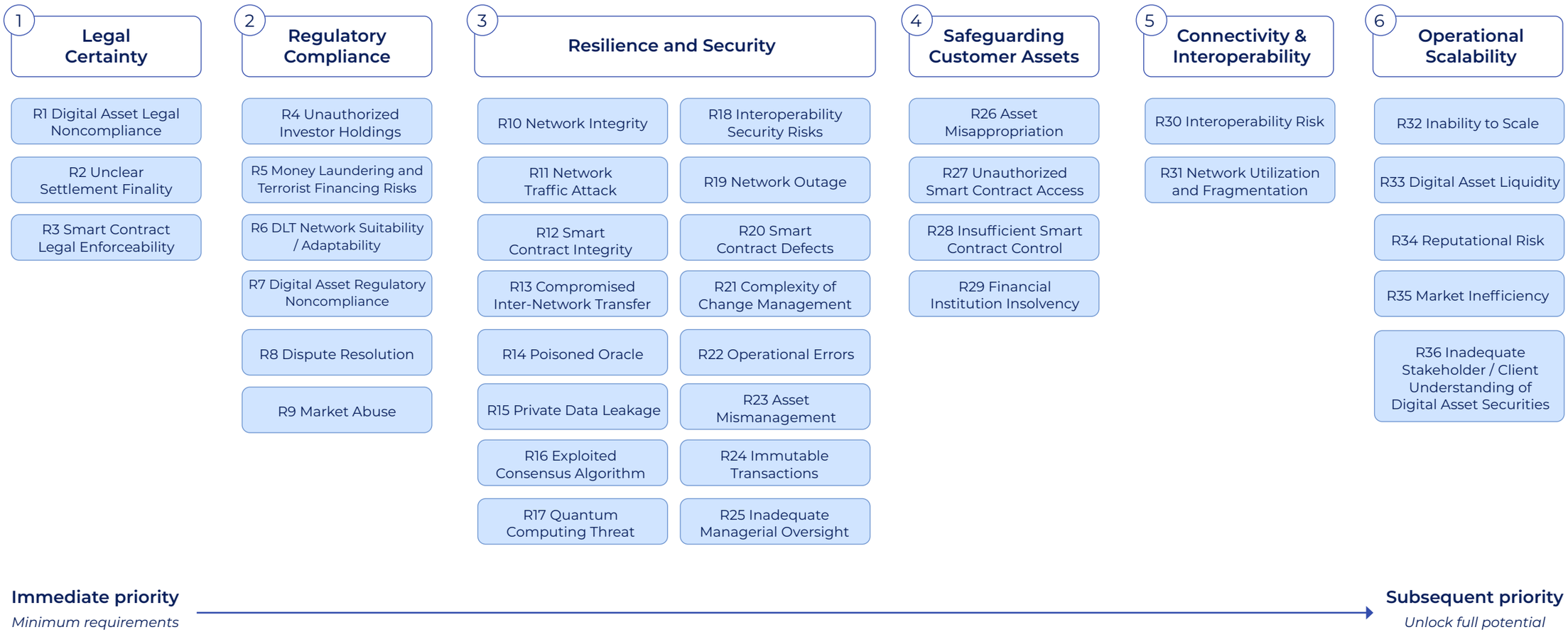
Operational Scalability:

Striving for efficiency and cost-effectiveness through standardized roles and smart contract functions to accommodate market growth.

Risks

Building on the foundational principles outlined above, it is crucial to systematically manage a wide range of risks. Adopting a risk-first approach ensures that emerging risks associated with DAS are proactively identified and effectively mitigated. This establishes a solid basis for safeguarding market integrity and building investor trust, which are critical for the adoption and growth of digital asset markets.

These risks, spanning the entire value chain, were identified along with the outlined principles to ensure robustness and exhaustiveness of the framework. Some risks inherently impact multiple principles. For conciseness, they were assigned to the principle with the highest importance, as depicted in the figure below.



Controls

The comprehensive risk inventory establishes a foundation for developing targeted controls essential for managing identified risks, thereby supporting the transition toward a DAS ecosystem aligned with our foundational principles.

These controls are designed to be adaptable, serving as a broad framework. Thus, they function more as guidelines rather than rigid controls and are crafted to address multiple risks, offering flexibility to adjust to different technologies and products. These controls are also dynamic, allowing for iterative updates to keep pace with the changing risk landscape and emerging technological advancements.

The following controls have been derived and mapped to the risks they are mitigating. Each control mitigates at least one risk, with many controls addressing multiple risks.

A secondary layer of control categorization organizes controls into four distinct groups, each distinguished by a unique suffix appended to the control number:

L ⟶ Legal:

Addresses adherence to regulatory requirements and legal frameworks, ensuring that DAS operations comply with applicable laws and compliance standards.

S ⟶ Smart Contract Governance:

Ensures the accuracy, authorization, and performance of smart contracts.

R ⟶ Resilience and Data Protection:

Protects systems against disruptions and secures sensitive information.

N ⟶ Network Settlement:

Fosters reliable and timely transaction processing within the DLT network.

As illustrated in the figure below, controls also have been organized into a taxonomy comprised of four categories – Legal, Smart Contract Governance, Resiliency and Data Protection, and Network Settlement – each categorized according to its required mitigating measures to enhance clarity. The specific risk that the control mitigates is listed below the control.

Legal

- C1-L Participation Guidelines — R1, R35
- C2-L Product Eligibility — R1, R7
- C3-L Network and Oracle Vetting — R1, R6, R10, R14, R35
- C4-L Participant Roles, Responsibilities, and Obligations — R1, R3, R8, R25, R26
- C5-L Service Providers Responsibilities / Limitation of Liability — R1
- C6-L Terms and Conditions — R1, R29
- C7-L Governance — R1, R6, R35
- C8-L Rule Enforcement and Arrangements — R1, R9
- C9-L Regulatory Approval and Oversight — R1
- C10-L Asset Safeguarding and Segregation — R4, R23, R25, R26, R27, R29
- C11-LPolicies and Procedures — R7, R35
- C12-L Education and Training for Stakeholders on Digital Asset Securities — R36

Smart Contract Governance

- C13-S Smart Contract Auditing Guidelines — R3
- C14-S Certification — R3, R12
- C15-S Investor Compliance and Access Control — R4, R5
- C16-S Multiparty Transaction Validation — R4, R5, R7, R12, R23, R26, R28
- C17-S Dispute Resolution Mechanism — R8
- C18-S Code Auditing — R12, R16, R20, R35
- C19-S Smart Contract Entitlements — R16, R23, R24, R26, R27, R28
- C20-S Quantum-Resistant Signature Algorithms — R17
- C21-S Intraoperability between DLT Networks — R18, R22, R30, R32
- C22-S Token Specification Model — R22, R32
- C23-S Data / Properties — R22, R32
- C24-S Functions / Behaviors — R22, R32
- C25-S Bookkeeping — R22, R29, R32
- C26-S Account Structure — R22, R29, R32
- C27-S Key Life Cycle Management — R26, R27
- C28-S Smart Contract Roles — R28, R32
- C29-S Emergency Stop — R28, R32
- C30-S Account Pause — R28, R32
- C31-S Token Pause — R28, R32

Resilience & Data Protection

- C32-R Audit Trail — R2, R12, R14, R16, R23, R24, R26, R27
- C33-R Data Life Cycle Management — R7
- C34-R Data Subject Access Rights Enforcement — R7, R24
- C35-R Event Monitoring and Alerts — R9, R14, R16, R19, R22, R25, R30, R33
- C36-R Redundancy and Concurrency — R10, R11, R19
- C37-R Backups — R10, R11, R19, R21
- C38-R Failure Prevention, Detection, and Recovery — R10, R11, R19, R21
- C39-R Recovery Testing — R10, R19, R21
- C40-R Private Data Segregation — R15
- C41-R Anonymization and Pseudonymization — R15
- C42-R Identity Verification — R15
- C43-R Geographical Distribution — R19
- C44-R Feature Deployment Process — R21
- C45-R Data Integrity Correction — R22

Network Settlement

- C46-N Data Lineage — R1, R12, R15, R21, R23, R27
- C47-N Encumbrance Mechanism — R2
- C48-N Settlement Proofs — R2
- C49-N Fail to Settle Process — R2
- C50-N Transaction Sequencing — R2, R13
- C51-N Cross-Ledger Data and Inventory Balances — R2, R13
- C52-N Compliance and Policy Management — R4, R5
- C53-N Continuous Management Education — R5
- C54-N Legacy Infrastructure Integration — R30, R32
- C55-N Third-Party Integration Guidelines — R30
- C56-N Community Engagement Framework — R31, R34
- C57-N Liquidity Management Strategies — R33

An Important Step toward Standards

The DASCP is a strategic road map, aiming to provide the industry with a proposal on how DAS can be managed, regulated, and scaled. Such a strategic road map paves the way for standards by:

- **Forging a Common Language:** A shared understanding of terminology and concepts is a cornerstone of effective standardization.
- **Enabling Regulatory Clarity:** Developed in collaboration with BCG, which reviewed over 100 regulations and engaged with more than 20 key market participants to ensure alignment with both existing and emerging global regulatory frameworks. This clarity in regulation is critical for the advancement of DAS.
- **Providing a Blueprint for Industry-Wide Alignment:** Developing the capabilities to form an aligned perspective on controls is essential for subsequent industry-wide alignment processes. The principles act as a guiding force in the subsequent phases of DAS adoption, ensuring that standards reflect the collective insights of the entire industry.

Case Study: Translating Principles into Practice

The DASCP framework serves as a pragmatic approach for streamlining compliance in DAS transactions. Far from theoretical, these controls are derived from real-world applications, demonstrating efficiency and adherence to regulatory standards. These controls ensure transactions not only adhere to legal standards and offer interoperability across platforms but also provide robust risk management, reflecting their adaptability and comprehensiveness amid global regulatory diversity.

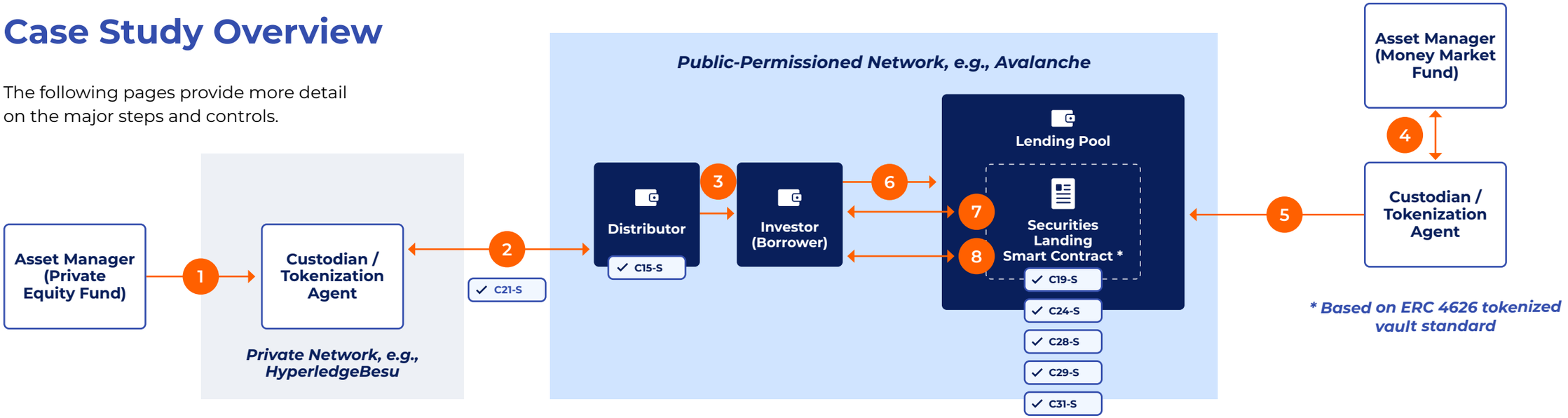
This case study showcases the framework's application in a scenario involving token issuance, transfer, and lending, where the risk management controls are seamlessly integrated into the digital asset transaction flow. This example presents the automation of numerous processes using digital assets, ensuring accurate controls, and reducing manual oversight.

In translating these principles into practice, the figure on page 17 maps the controls applied at each transactional junction, demonstrating how specific risks are addressed through tailored controls. The central role of smart contracts is evident throughout the process, offering a robust means to automate intricate transaction sequences, ensure regulatory adherence, and protect the integrity of the loan's data and functions.

The DASCP framework is designed for flexibility, allowing organizations to adapt high-level controls to their specific operational needs. This case study highlights how the framework supports customization to meet diverse organizational requirements effectively. It exemplifies how a regulatory aligned framework can be a powerful catalyst for operational efficiency, ultimately contributing to the maturation and growth of the DAS market.

Case Study Overview

The following pages provide more detail on the major steps and controls.



Major steps:

1. Asset Tokenization
2. Token Transfer
3. KYC Enforcement
4. Money Market Fund (MMF) Issuance
5. MMF Tokenization for Lending
6. Collateral Deposit
7. Lending Pool Transactions
8. Automated Lending Operations

Principle	Risk	Control
Connectivity and Interoperability	R30 Interoperability Risk	C21-S Intraoperability between DLT Networks
Regulatory Compliance	R4 Unauthorized Investor Holdings	C15-S Investor Compliance and Access Control
Resilience and Security	R23 Asset Mismanagement	C19-S Smart Contract Entitlements
Operational Scalability	R32 Inability to Scale	C24-S Functions / Behaviors
Safeguarding Customer Assets	R28 Insufficient Smart Contract Control	C28-S Smart Contract Roles C29-S Emergency Stop C31-S Token Pause

Description of major steps:

1 Asset Tokenization:

An asset manager issues a private security, such as a private equity fund, which is then tokenized on a private blockchain by a custodian.

2 Token Transfer:

The custodian moves the newly created PE (Private Equity) tokens from the private ledger to a public-permissioned ledger for wider distribution.

3 KYC Enforcement:

As tokens are distributed, KYC compliance checks are performed to ensure all investors meet regulatory standards, despite the change in blockchain.

4 Money Market Fund (MMF) Issuance:

In parallel, an asset manager issues a Money Market Fund.

5 MMF Tokenization for Lending:

The custodian tokenizes the MMF shares and makes them available for lending in the Securities Lending Market.

6 Collateral Deposit:

Investors with tokenized PE fund shares deposit these tokens into the lending pool to serve as collateral.

7 Lending Pool Transactions:

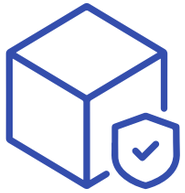
Using the collateral provided, investors borrow more liquid assets (e.g., MMF shares) from the lending pool.

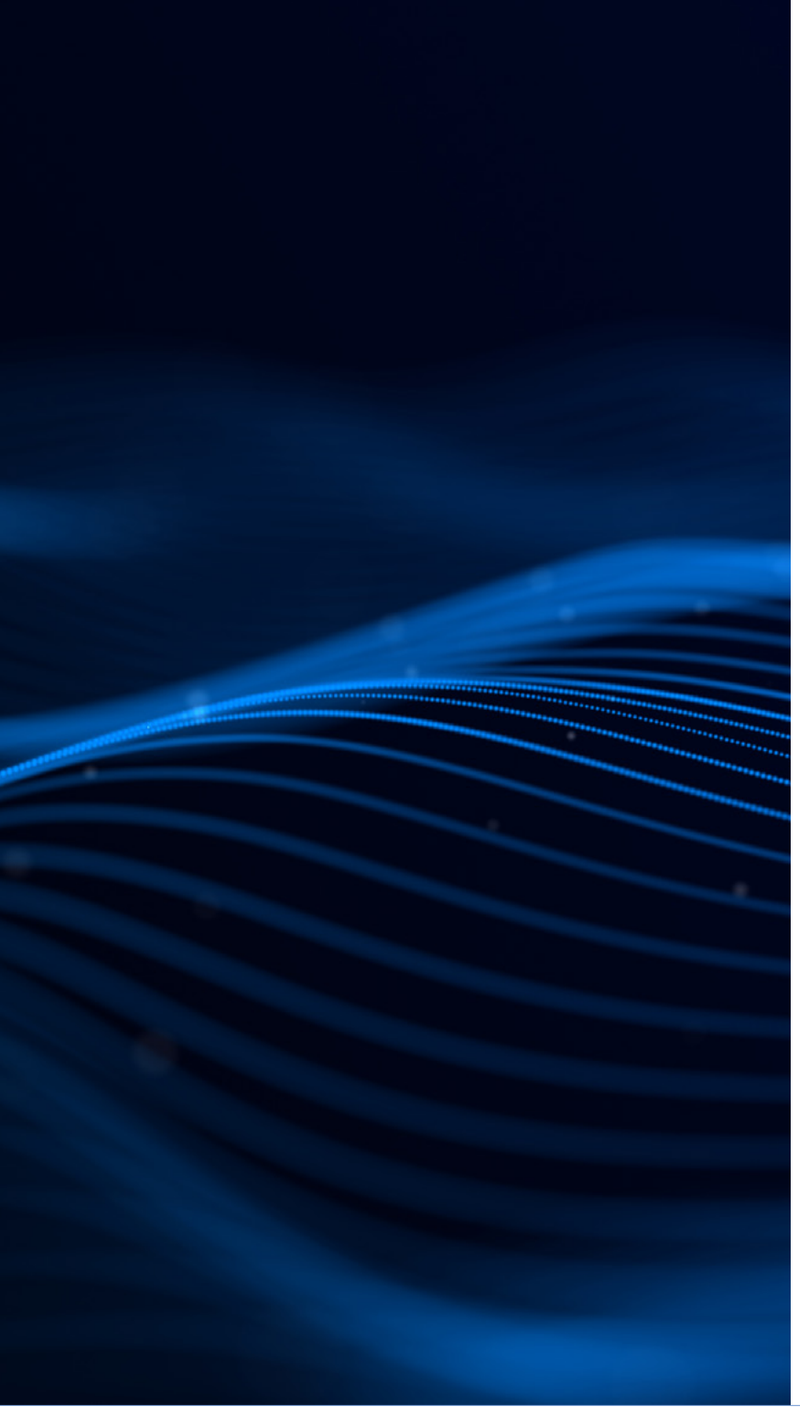
8 Automated Lending Operations:

The lending process, powered by smart contracts, automates the workflow, including the deposit, loan issuance, and approval, and upon maturity, manages repayment and interest distribution and returns the securities to their original owners.

The chart below presents a detailed illustration of the DASCP controls in action, delineating the specific methods used for its implementation. While these examples highlight the controls' functionality and the potential for smart contracts to reinforce the robustness of the DAS market, they are intended to serve as illustrations of what can be achieved. They are not prescriptive; organizations are encouraged to interpret and adapt controls to fit their unique environments, strategies, and compliance needs. This illustrative approach reaffirms the DASCP framework's commitment to flexibility and its capacity to accommodate a diverse range of technologies and operational scenarios, ensuring its broad applicability and relevance across the financial industry.

Principle	Risk	Control	Smart Contract Control Activities
Connectivity and Interoperability 	**R30 Interoperability Risk:** The risk pertains to the complexities of integrating digital assets with traditional financial systems and, potentially, multiple blockchain architectures (e.g., public, public-permissioned, and private) to ensure seamless transactions across the entire financial spectrum.	**C21-S Intraoperability Between DLT Networks:** Adhere to industry-accepted cross-network communication protocols specifically designed for blockchain interoperability. This includes standardized protocols for asset representation, transaction formats, and data exchange between different blockchain networks, ensuring seamless and secure interactions across diverse blockchain platforms.	Specific smart contracts and token standards, along with cross-chain interoperability protocols (lock / mint), ensure token transferability from one chain to another, adhering to both internal compliance and industry-accepted cross-network communication protocols for asset representation, transaction formats, and data exchange.
Regulatory Compliance 	**R4 Unauthorized Investor Holdings:** Potential for regulatory noncompliance and financial repercussions if a non-compliant or unauthorized investor holds or transfers a digital asset security. This includes breaches of investor accreditation, investment caps, or other regulatory standards not related to AML or CTF.	**C15-S Investor Compliance and Access Control:** Implement mechanisms that only allow authorized investors that are in good compliance standing (e.g., KYC, sanctions, etc.) to hold registered securities while restricting others who are not, which could be facilitated by allow-lists, verifiable credentials, or other relevant protocols.	Smart contract checks the client's wallet for required credentials and completes the transfer only if the investor is compliant with the fund terms.

Principle	Risk	Control	Smart Contract Control Activities
Resilience and Security 	**R23 Asset Mismanagement:** Digital assets are at risk of being lost, stolen, or erroneously transferred due to breaches in operational controls, system vulnerabilities, or inadequate asset management protocols.	**C19-S Smart Contract Entitlements:** Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.	A smart contract, combined with a specific token standard, grants the lending decision to the lending pool, ensuring that only the lending pool can issue and approve a loan. This ensures immutability of roles, entitlement, and processes, thus eliminating the risk of unauthorized use or access to the loan's data and functions.
Operational Scalability 	**R32 Inability to Scale:** DLT networks may not efficiently manage or scale to accommodate surging transaction volumes, impacting critical functions such as post-trade capture and overall transaction throughput (including suitable customer support), potentially degrading system performance and reliability.	**C24-S Functions / Behaviors:** Conform to a common set of functions, behaviors, and service level agreements that support various security life cycle operations such as issuance and settlement.	Smart contracts enable automation and atomic settlement of transactions, which provides scalability to perform large volumes of standardized yet complex operations in seconds. For example, for the lending transaction, the smart contract performed six functions in one step (deposit, issuance, approval, deposit, hair-cutting, and pledging).
Safeguarding Customer Assets 	**R28 Insufficient Smart Contract Control:** A custodian and/or relevant intermediary does not have the requisite control over the digital asset securities / tokens or smart contracts functions.	**C28-S Smart Contract Roles:** Define standard roles to determine who can access smart contract data and functions. **C29-S Emergency Stop:** Ensure that smart contracts have an embedded kill switch or process to halt all activity, which can be accessed by a role with elevated permissions. **C31-S Token Pause:** Ensure that a user can freeze or pause activity for all or some of the token inventory, controlled by either the agent of the investor or a role with elevated permissions.	Token standard and smart contract configuration were used to bring off-chain KYC compliance rules into on-chain token configuration, enabling the operations to halt or pause any token activity when participants did not match KYC criteria (e.g., jurisdiction). This ensured that only a role with elevated permission (compliance officer) could freeze or unfreeze activity over the token factory.



Next Steps in the Evolution of the DASCP

To foster open dialogue and collective intelligence, we intend to engage the industry through a series of in-depth discussions involving key stakeholders from across the financial sector. These exchanges will serve as a platform to share insights and best practices, as well as to collaboratively address the concerns and challenges faced by various players in implementing the control principles.

Also, we plan to transition the stewardship of the DASCP to an industry association, ensuring its continuous enhancement and compliance with global regulations. Industry associations play a pivotal role in uniting market participants around common goals. This strategic move not only guarantees continuous improvement and expansion of the DASCP but also empowers the association to leverage it as a foundational document. This will facilitate the integration of secondary trading risks and controls, and the development of additional standards to bolster interoperability, security, and compliance in the digital asset securities landscape.

We will continue to shape the market effectively as we build upon the foundation of our previous collaborative efforts that call for pioneering cash on-chain initiatives and establishing new standards.[9] We are committed to continuously sharing insights and supporting adaptations of the DASCP to meet specific regional requirements, technology stacks, and operational environments. By disseminating these customizations within the community, we aim to accelerate the adoption and enhance the effectiveness of the DASCP across diverse financial ecosystems.

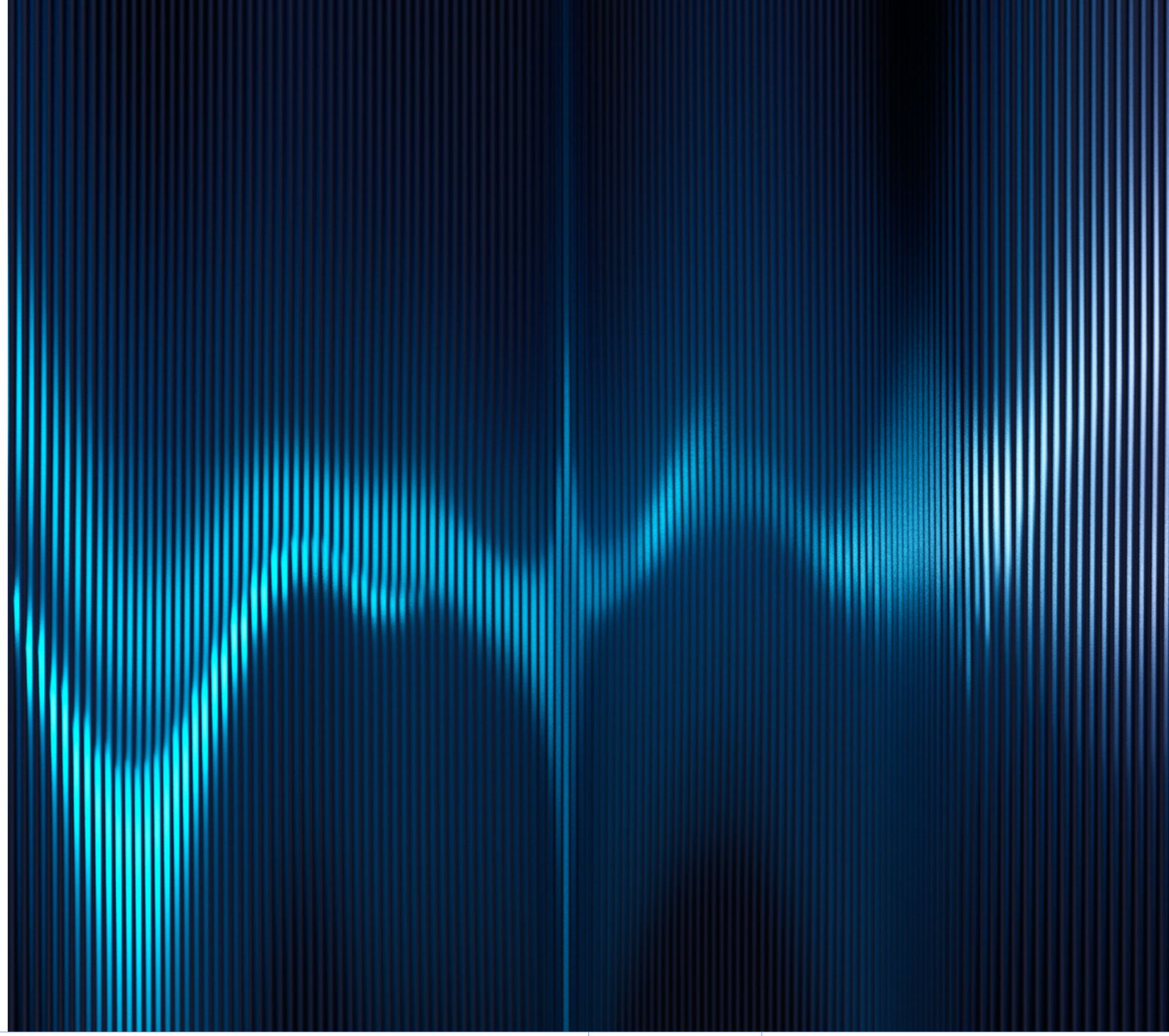
[9]DTCC, Clearstream, Euroclear, "Advancing the Digital Asset Era, Together," Sept 2023

A United Path Forward: The Imperative for Collective Action

It is important to recognize that the DASCP is just one of several critical components required for full-scale adoption. Ongoing developments in interoperability, cash on-chain initiatives, scalable solutions, and the formulation of strong business cases remain essential to achieving comprehensive integration and value realization.

We extend our gratitude to all participants whose engagement has been helpful in shaping a framework that promises to be both foundational and transformative. Integrating these principles into future standards will be vital for enhancing security, efficiency, and promoting broad-based innovation within the industry.

We are committed to not just working together but to moving forward with a purpose. This is a call for industry-wide mobilization to support a vision. Let us unite in this endeavor to build a robust, integrated financial future. Together, we can advance the era of digital asset securities.



Appendix

Complete Risk and Control Taxonomy

The detailed descriptions of risks and controls, as well as a view on which risks are mitigated by which controls, is shown below.

Detailed Risk Description:

To enhance the effectiveness of our framework, each risk is aligned with one of six principles, ranked from highest to lowest priority. (1) Legal Certainty is deemed the most urgent, while (6) Operational Scalability is considered the least. This ranking does not diminish the importance of any principle, as all are required to establish a vibrant DAS ecosystem. When a risk could be associated with multiple principles, it is assigned to the principle of highest priority. By doing so, we not only ensure a concise framework presentation but also prioritize the risk management process.

Detailed Controls Description:

Controls are mapped to the risks they are mitigating in a way that one control addresses either one or multiple risks.

Download the Digital Asset Securities Control Principles.

1. Legal Certainty

Return to Principles overview on page 11

This figure shows the risks associated with the principle “Legal Certainty,” as well as the controls to mitigate these risks:

Risks

R1 Digital Asset Legal Noncompliance

Risk of financial loss or other damages due to noncompliance with rapidly evolving global legal standards governing digital assets. This includes challenges in adapting to diverse regulatory environments, ensuring compliance across jurisdictions, and managing the complexities of integrating digital and conventional asset regulatory frameworks.

Controls

→	**C1-L Participation Guidelines:** Establish fair and open but risk-based criteria (financial, jurisdictional, etc.) for user types and third-party service providers permitted to participate in a product, program, or service offering. Include advanced due diligence and continuous compliance monitoring tailored to digital asset markets, ensuring alignment with evolving jurisdictional regulations.
→	**C2-L Product Eligibility:** Identify clear standards and requirements for the product types (e.g., bonds) supported, including thorough due diligence for new listings and ongoing disclosure requirements. Ensure transparency about the financial and operational health of issuers to maintain regulatory compliance and inform stakeholders.
→	**C3-L Network and Oracle Vetting:** Conduct thorough checks on network and oracle alignment with DLT standards and governance structures before integrating third-party tools. Validate reliability and security SLAs for all networks and oracles rigorously.
→	**C4-L Participant Roles, Responsibilities, and Obligations:** Clearly define and document service participants’ roles, responsibilities, and obligations, integrating geographic and identity-specific nuances to align with legal and operational standards by jurisdiction.
→	**C5-L Service Providers’ Responsibilities / Limitation of Liability:** Clearly document the roles, responsibilities, and obligations of the service provider and cover both legal and operational aspects of a given service. Moreover, provisions that describe limitations of liability for a given service provider must be clearly defined.
→	**C6-L Terms and Conditions:** Establish a legal basis for a service based on rules and/or contractual agreements that bind both the service provider and stakeholders. The terms of service should also establish the parameters for transfer, custody, control of assets consistent with applicable laws, regulations, and other regulatory requirements for the service provider and stakeholders.
→	**C7-L Governance:** Define clear governance arrangements, detailing oversight and management of the service.
→	**C8-L Rule Enforcement and Arrangements:** Monitor and enforce rules effectively, and maintain the authority to discipline, limit, suspend, or terminate participant activities, as well as to halt and resume transactions for certain assets (i.e., Security Tokens) as necessary.
→	**C9-L Regulatory Approval and Oversight:** Complete all required rule filings, no-action relief, or other regulatory approvals and notifications prior to implementation.
→	**C46-N Data Lineage:** Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

1. Legal Certainty (continued)

Return to Principles overview on page 11

Risks	Controls
R2 Unclear Settlement Finality Settlement finality is not achieved or/and settlement status unclear.	**C32-R Audit Trail:** Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.
	C47-N Encumbrance Mechanism: Implement a process to encumber funds or securities, preventing double spending until the transaction is fully settled.
	C48-N Settlement Proofs: Provide verifiable proof or evidence that different transaction legs were finalized, including their precise time stamps across various networks.
	C49-N Fail to Settle Process: Implement procedures to reverse, cancel, or otherwise undo transactions and / or its economic impacts in the event of a settlement failure.
	C50-N Transaction Sequencing: Implement nonces and/or transaction sequencing models that ensure transactions are processed in the appropriate order and prevent replay attacks.
	C51-N Cross Ledger Data and Inventory Balances: Track shared data and reconcile or balance inventory across networks.
R3 Smart Contract Legal Enforceability Differences in the legal status, recognition, and enforceability of smart contracts in various jurisdictions, which could impact cross-border transactions and asset custody.	**C4-L Participant Roles, Responsibilities, and Obligations:** Clearly define and document service participants' roles, responsibilities, and obligations, integrating geographic and identity-specific nuances to align with legal and operational standards by jurisdiction.
	C13-S Smart Contract Auditing Guidelines: Establish comprehensive guidelines for auditing smart contracts, which are designed as machine-executable legal agreements, to ensure not only their compliance with relevant laws but also to explicitly verify and reflect their enforceability terms. These guidelines should include detailed procedures for reviewing the legal and technical aspects of smart contracts to validate their ability to be enforced as per the terms set within them under applicable legal frameworks.
	C14-S Certification: Ensure that when smart contracts are deployed to networks that are governed by different parties, there are processes in place such that a trusted party can validate the integrity of a given smart contract.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

2. Regulatory Compliance

Return to Principles overview on page 11

This figure shows the risks associated with the principle “Regulatory Compliance,” as well as the controls to mitigate these risks:

Risks	Controls
R4 Unauthorized Investor Holdings Potential for regulatory non-compliance and financial repercussions if a noncompliant or unauthorized investor holds or transfers a digital asset security. This includes breaches of investor accreditation, investment caps, or other regulatory standards not related to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF).	**C10-L Asset Safeguarding and Segregation:** Implement stringent controls to ensure customer assets are safeguarded and segregated from the custodian’s or broker-dealer’s own assets. This includes maintaining customer assets with a trusted, regulated custodian and establishing clear separation protocols to prevent asset commingling and misuse.
	C15-S Investor Compliance and Access Control: Implement mechanisms that only allow authorized investors that are in good compliance standing (e.g., KYC, Sanctions, etc.) to hold registered securities, while restricting others who are not, which could be facilitated by allow lists, verifiable credentials, or other relevant protocols.
	C16-S Multiparty Transaction Validation: Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
	C52-N Compliance and Policy Management: Implement and enforce transaction policies consistently across all networks. Include mechanisms to verify and record compliance for each transaction.
R5 Money Laundering and Terrorist Financing Risks Potential for misuse of the platform for obscuring illicit funds or funding terrorism, due to inadequate AML or CTF controls. This risk involves failure to implement effective KYC procedures, insufficient transaction monitoring, and noncompliance with mandatory financial reporting standards, leading to legal and reputational damage.	**C15-S Investor Compliance and Access Control:** Implement mechanisms that only allow authorized investors that are in good compliance standing (e.g., KYC, Sanctions, etc.) to hold registered securities, while restricting others who are not, which could be facilitated by allow-lists, verifiable credentials, or other relevant protocols.
	C16-S Multiparty Transaction Validation: Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
	C7-L Governance: Define clear governance arrangements, detailing oversight and management of the service.
	C8-L Rule Enforcement and Arrangements: Monitor and enforce rules effectively, and maintain the authority to discipline, limit, suspend, or terminate participant activities, as well as to halt and resume transactions for certain assets (i.e., Security Tokens) as necessary.
	C52-N Compliance and Policy Management: Implement and enforce transaction policies consistently across all networks. Include mechanisms to verify and record compliance for each transaction.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

2. Regulatory Compliance (continued)

Return to Principles overview on page 11

Risks	Controls
R6 DLT Network Suitability / Adaptability The DLT network may currently be unsuitable, or struggle to align with the rapidly evolving technological standards and/or regulations required for managing digital asset securities (e.g., smart contracts may not be flexible enough to accommodate future regulatory changes, leading to potential noncompliance and/or and operational inefficiencies).	**C3-L Network and Oracle Vetting:** Conduct thorough checks on network and oracle alignment with DLT standards and governance structures before integrating third-party tools. Validate reliability and security SLAs for all networks and oracles rigorously.
	C7-L Governance: Define clear governance arrangements, detailing oversight and management of the service.
R7 Digital Asset Regulatory Noncompliance Securities are noncompliant with varied and possibly conflicting securities regulations (e.g., codes of conduct, standards set by government bodies, or industry regulators) across disparate jurisdictions and asset classes.	**C2-L Product Eligibility:** Identify clear standards and requirements for the product types (e.g., bonds) supported, including thorough due diligence for new listings and ongoing disclosure requirements. Ensure transparency about the financial and operational health of issuers to maintain regulatory compliance and inform stakeholders.
	C11-L Policies and Procedures: Document comprehensive policies and procedures that cover all aspects of business operations and IT functionalities, including protocols for blockchain management and smart contract deployment. Incorporate regular testing strategies such as simulations, stress tests, and security audits to ensure compliance with security standards and regulatory requirements. Regularly update these policies and testing methods to align with technological advancements and regulatory changes.
	C16-S Multiparty Transaction Validation: Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
	C33-R Data Life Cycle Management: Manage and document the process of data collection, usage, transfer, storage, security, retention, and deletion.
	C34-R Data Subject Access Rights Enforcement: Create privileged roles that have the right to access data, amend data, or respond to requests for a given person's data to be erased and where appropriate, arrangements detailing oversight and management of the service.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

2. Regulatory Compliance (continued)

Return to Principles overview on page 11

Risks	Controls
R8 Dispute Resolution The risk that decentralized governance within DLT environments may hinder predictable dispute resolution across networks.	**C4-L Participant Roles, Responsibilities, and Obligations:** Clearly define and document service participants' roles, responsibilities, and obligations, integrating geographic and identity-specific nuances to align with legal and operational standards by jurisdiction.
	C17-S Dispute Resolution Mechanism: Implement a mechanism for dispute resolution that provides clear escalation paths and ensures consistent outcomes across DLT networks.
R9 Market Abuse The risk of insufficient surveillance to prevent market manipulation, ensuring transparent and fair practices align with market integrity standards.	**C8-L Rule Enforcement and Arrangements:** Monitor and enforce rules effectively, and maintain the authority to discipline, limit, suspend, or terminate participant activities, as well as to halt and resume transactions for certain assets (i.e., Security Tokens) as necessary.
	C35-R Event Monitoring and Alerts: Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security

Return to Principles overview on page 11

This figure shows the risks associated with the principle “Resilience and Security,” as well as the controls to mitigate these risks:

Risks	Controls
R10 Network Integrity The integrity of the overall DLT network is compromised due to an attack, issue with the consensus algorithm, manipulated through nodes with supermajority power, etc.	**C3-L Network and Oracle Vetting:** Conduct thorough checks on network and oracle alignment with DLT standards and governance structures before integrating third-party tools. Validate reliability and security SLAs for all networks and oracles rigorously.
	C36-R Redundancy and Concurrency: Ensure technology resilience capabilities are in place to guarantee continuity of service and that there isn’t a single point of failure due to a logical loss of a major DLT / network node or loss of all nodes in a geographic region.
	C37-R Backups: Regularly record and store copies of the ledger and service-related data to prevent loss of data integrity or availability due to destruction or corruption of data.
	C38-R Failure Prevention, Detection and Recovery: Implement processes and mechanisms for detecting failures and seamlessly transitioning to backup systems to prevent disruptions and maintain data integrity. These processes entail reporting, recovering, and resolving several different types of failures.
	C39-R Recovery Testing: Regularly simulate and validate recovery processes to ensure the system’s ability to restore data accurately and securely in the case of unexpected incidents, such as failures and crashes, to test the recovery performance of the system, including industry required performance testing.
R11 Network Traffic Attack The DLT network cannot be accessed due to a network traffic attack such as Distributed Denial of Service (DDoS).	**C36-R Redundancy and Concurrency:** Establish a legal basis for a service based on rules and/or contractual agreements that bind both the service provider and stakeholders. The terms of service should also establish the parameters for transfer, custody, control of assets consistent with applicable laws, regulations and other regulatory requirements for the service provider and stakeholders.
	C37-R Backups: Regularly record and store copies of the ledger and service-related data to prevent loss of data integrity or availability due to destruction or corruption of data.
	C38-R Failure Prevention, Detection and Recovery: Implement processes and mechanisms for detecting failures and seamlessly transitioning to backup systems to prevent disruptions and maintain data integrity. These processes entail reporting, recovering, and resolving several different types of failures.
	C46-N Data Lineage: Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks	Controls
R12 Smart Contract Integrity The integrity of the smart contract on the DLT network is compromised due to a code or external libraries vulnerabilities.	**C14-S Certification:** Ensure that when smart contracts are deployed to networks that are governed by different parties, there are processes in place such that a trusted party can validate the integrity of a given smart contract.
	C16-S Multiparty Transaction Validation: Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
	C18-S Code Auditing: Ensure all smart contract code is tested for vulnerabilities, bugs, performance issues, or defects by an independent third-party auditor.
	C32-R Audit Trail: Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.
	C46-N Data Lineage: Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.
R13 Compromised Inter-Network Transfer Inter-network asset transfer integrity is compromised.	**C50-N Transaction Sequencing:** Implement nonces and/or transaction sequencing models that ensure transactions are processed in the appropriate order and prevent replay attacks.
	C51-N Cross Ledger Data and Inventory Balances: Track shared data and reconcile or balance inventory across networks.
R14 Poisoned Oracle Off-chain data tampering from a compromised oracle (i.e., poisoned oracle scenario).	**C3-L Network and Oracle Vetting:** Conduct thorough checks on network and oracle alignment with DLT standards and governance structures before integrating third-party tools. Validate reliability and security SLAs for all networks and oracles rigorously.
	C32-R Audit Trail: Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.
	C35-R Event Monitoring and Alerts: Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks	Controls
R15 Private Data Leakage Customers' personal data or proprietary data is leaked or stolen.	**C40-R Private Data Segregation:** Segregate and restrict access to confidential data such as personal information, client-, and firm-specific proprietary data that should not be broadly available on a given network.
	C41-R Anonymization and Pseudonymization: Anonymize or pseudonymize sensitive data to protect individual or entity privacy.
	C42-R Identity Verification: Establish a system or process for verifying client identities and compliance status, which may include internal mechanisms, third-party digital identity verification services, or other suitable methods.
	C46-N Data Lineage: Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.
R16 Exploited Consensus Algorithm Consensus mechanism is exploited such that the network may function inappropriately, leading to unauthorized transfers of digital assets, unauthorized censorship of transactions, double-spending, or operational disruption to the transaction validation process.	**C18-S Code Auditing:** Ensure all smart contract code is tested for vulnerabilities, bugs, performance issues or defects by an independent third-party auditor.
	C19-S Smart Contract Entitlements: Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.
	C32-R Audit Trail: Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.
	C35-R Event Monitoring and Alerts: Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.
R17 Quantum Computing Threat Quantum computing is able to break asymmetric encryption and back into a private key from a public key.	**C20-S Quantum-Resistant Signature Algorithms:** Implement a quantum-resistant signature algorithm, and a periodic audit process for reviewing and documenting quantum-resistant algorithms utilized within the system to ensure ongoing security efficacy against quantum threats.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks	Controls
R18 Interoperability Security Risks Security vulnerabilities arising from connecting the digital asset platform with other blockchain networks or traditional financial systems.	**C21-S Intraoperability Between DLT Networks:** Adhere to industry-accepted cross-network communication protocols specifically designed for blockchain interoperability. This includes standardized protocols for asset representation, transaction formats, and data exchange between different blockchain networks, ensuring seamless and secure interactions across diverse blockchain platforms.
R19 Network Outage A singular event, such as a natural disaster, a common failure point, or a pervasive network issue, could simultaneously incapacitate multiple critical components, nodes, or networks, resulting in extensive operational disruptions and systemic instability.	**C35-R Event Monitoring and Alerts:** Implement a system to monitor and audit operations in realtime and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.
	C36-R Redundancy and Concurrency: Ensure technology resilience capabilities are in place to guarantee continuity of service, and there isn't a single point of failure due to a logical loss of a major DLT / network node or loss of all nodes in a geographic region.
	C37-R Backups: Regularly record and store copies of the ledger and service-related data to prevent loss of data integrity or availability due to destruction or corruption of data.
	C38-R Failure Prevention, Detection and Recovery: Implement processes and mechanisms for detecting failures and seamlessly transitioning to backup systems to prevent disruptions and maintain data integrity. These processes entail reporting, recovering, and resolving several different types of failures.
	C39-R Recovery Testing: Regularly simulate and validate recovery processes to ensure the system's ability to restore data accurately and securely in the case of unexpected incidents, such as failures and crashes, to test the recovery performance of the system, including industry required performance testing.
	C43-R Geographical Distribution: Strategically distribute data across diverse geographic locations, within regulatory boundaries, to minimize the impact of regional disruptions and ensure systems can be operationally rotated.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks	Controls
R20 Smart Contract Defects DLT smart contracts are not operational due to a software bug or defect.	**C18-S Code Auditing:** Ensure all smart contract code is tested for vulnerabilities, bugs, performance issues or defects by an independent third-party auditor.
R21 Complexity of Change Management The decentralized and immutable nature of DLT presents substantial challenges for network modifications. This risk particularly affects the platform's ability to deploy new features, update smart contracts, or address vulnerabilities through software patches. The consensus requirement for changes introduces complexities in timely adaptation and innovation, making the management of software updates, enhancements, and security fixes inherently difficult.	**C37-R Backups:** Regularly record and store copies of the ledger and service-related data to prevent loss of data integrity or availability due to destruction or corruption of data.
	C38-R Failure Prevention, Detection, and Recovery: Implement processes and mechanisms for detecting failures and seamlessly transitioning to backup systems to prevent disruptions and maintain data integrity. These processes entail reporting, recovering, and resolving several different types of failures.
	C39-R Recovery Testing: Regularly simulate and validate recovery processes to ensure the system's ability to restore data accurately and securely in the case of unexpected incidents, such as failures and crashes, to test the recovery performance of the system, including industry required performance testing.
	C44-R Feature Deployment Process: Establish processes for deploying new features or updates that minimize disruption and ensure network integrity.
	C46-N Data Lineage: Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks

R22 Operational Errors

Errors, failures, or bottlenecks arise during the security life cycle as smart contract code does not conform to standard market practices.

Controls

C21-S Intraoperability Between DLT Networks: Adhere to industry-accepted cross-network communication protocols specifically designed for blockchain interoperability. This includes standardized protocols for asset representation, transaction formats, and data exchange between different blockchain networks, ensuring seamless and secure interactions across diverse blockchain platforms.

C22-S Token Specification Model: Define smart contract requirements through a human readable markup language that models smart contract specifications and can be easily understood by business, operations, and IT personas.

C23-S Data / Properties: Ensure data properties embedded into a smart contract conform to recognized nomenclature and conventions. Data must sufficiently identify and describe the security (e.g., standard security IDs) and incorporate or have access to the data required to process life cycle events.

C24-S Functions / Behaviors: Conform to a common set of functions, behaviors, and service level agreements that support various security life cycle operations such as issuance and settlement.

C25-S Bookkeeping: Conform to an accounting model that supports both private (non-publicly traded) and public (publicly traded) securities. Adapt the accounting model to comply with international digital asset securities reporting standards.

C26-S Account Structure: Conform to a common model to represent investor accounts that delineate what accounts are customer vs. proprietary and have the appropriate level of attribution.

C35-R Event Monitoring and Alerts: Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.

C45-R Data Integrity Correction: Create privileged roles that can edit and modify data to ensure the accuracy, consistency, and reliability of financial records.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks	Controls
R23 Asset Mismanagement Digital assets are at risk of being lost, stolen, or erroneously transferred due to breaches in operational controls, system vulnerabilities, or inadequate asset management protocols.	**C10-L Asset Safeguarding and Segregation:** Implement stringent controls to ensure customer assets are safeguarded and segregated from the custodian's or broker-dealer's own assets. This includes maintaining customer assets with a trusted, regulated custodian and establishing clear separation protocols to prevent asset commingling and misuse.
	C16-S Multiparty Transaction Validation: Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
	C19-S Smart Contract Entitlements: Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.
	C32-R Audit Trail: Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.
	C46-N Data Lineage: Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

3. Resilience and Security (continued)

Return to Principles overview on page 11

Risks	Controls
R24 Immutable Transactions Due to the nature of immutable blockchains, if there is an error or processing issue, securities cannot be transferred back to the original owner.	**C19-S Smart Contract Entitlements:** Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.
	C32-R Audit Trail: Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.
	C34-R Data Subject Access Rights Enforcement: Create privileged roles that have the right to access data, amend data, or respond to requests for a given person's data to be erased, where appropriate.
R25 Inadequate Managerial Oversight The risk that operations are compromised due to insufficiently qualified management and/ or insufficient governance structures, potentially leading to operational vulnerabilities and regulatory noncompliance.	**C4-L Participant Roles, Responsibilities, and Obligations:** Clearly define and document service participants' roles, responsibilities, and obligations, integrating geographic and identity-specific nuances to align with legal and operational standards by jurisdiction.
	C10-L Asset Safeguarding and Segregation: Implement stringent controls to ensure customer assets are safeguarded and segregated from the custodian's or broker-dealer's own assets. This includes maintaining customer assets with a trusted, regulated custodian and establishing clear separation protocols to prevent asset commingling and misuse.
	C35-R Event Monitoring and Alerts: Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.
	C53-N Continuous Management Education: Mandate ongoing training programs for management in digital asset security and regulatory compliance. Include fit and proper tests for management to strengthen oversight.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

4. Safeguarding Customer Assets

Return to Principles overview on page 11

This figure shows the risks associated with the principle “Safeguarding Customer Assets,” as well as the controls to mitigate these risks:

Risks

R26 Asset Misappropriation

There is misappropriation of digital asset securities through various means, including but not limited to code vulnerabilities, unauthorized actions by intermediaries, or fraudulent misuse of access privileges.

Controls

- **C4-L Participant Roles, Responsibilities, and Obligations:** Clearly define and document service participants’ roles, responsibilities, and obligations, integrating geographic and identity-specific nuances to align with legal and operational standards by jurisdiction.
- **C10-L Asset Safeguarding and Segregation:** Implement stringent controls to ensure customer assets are safeguarded and segregated from the custodian’s or broker-dealer’s own assets. This includes maintaining customer assets with a trusted, regulated custodian and establishing clear separation protocols to prevent asset commingling and misuse.
- **C16-S Multiparty Transaction Validation:** Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
- **C19-S Smart Contract Entitlements:** Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.
- **C27-S Key Life Cycle Management:** Implement a secure multiparty cryptographic system that ensures comprehensive key life cycle management. This system should include detailed protocols for the generation, distribution, storage, and secure destruction of cryptographic keys. Ensure that these key management practices rigorously prevent unauthorized access and are in full compliance with current regulatory standards for digital asset security. Additionally, incorporate regular reviews and updates to adapt to emerging security technologies and threats.
- **C32-R Audit Trail:** Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

4. Safeguarding Customer Assets (continued)

Return to Principles overview on page 11

Risks

R27 Unauthorized Smart Contract Access

There is unauthorized manipulation or exploitation of smart contract functions due to factors such as technical vulnerabilities, inadequate access controls, and compromised security protocols. This includes but is not limited to unauthorized alterations to smart contract code, data breaches via smart contract interfaces, and exploitation of flaws in smart contract design.

Controls

C10-L Asset Safeguarding and Segregation: Implement stringent controls to ensure customer assets are safeguarded and segregated from the custodian's or broker-dealer's own assets. This includes maintaining customer assets with a trusted, regulated custodian and establishing clear separation protocols to prevent asset commingling and misuse.

C19-S Smart Contract Entitlements: Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.

C27-S Key Life Cycle Management: Implement a secure multiparty cryptographic system that ensures comprehensive key life cycle management. This system should include detailed protocols for the generation, distribution, storage, and secure destruction of cryptographic keys. Ensure that these key management practices rigorously prevent unauthorized access and are in full compliance with current regulatory standards for digital asset security. Additionally, incorporate regular reviews and updates to adapt to emerging security technologies and threats.

C32-R Audit Trail: Maintain a comprehensive record of digital asset events / transactions, both on-chain and relevant external activities, with precise synchronized time stamps. Enforce standards for synchronizing clocks across all DLT systems and external activity sources to ensure uniform time-stamping. The audit trail must support the full-system recovery and verification of the process for resilience purposes.

C46-N Data Lineage: Implement a comprehensive data lineage process for transactions and related data processes. This process must track the journey of data from its origin through all transformations and uses until its final state.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

4. Safeguarding Customer Assets (continued)

Return to Principles overview on page 11

Risks	Controls
R28 Insufficient Smart Contract Control A custodian and/or relevant intermediary does not have the requisite control over the digital asset securities / tokens or smart contracts functions.	**C16-S Multiparty Transaction Validation:** Implement collaborative transaction validation mechanism that requires approvals from multiple authorized parties to enhance transaction security. This mechanism includes provisions for periodic updates to address emerging security challenges and maintain compliance with industry standards.
	C19-S Smart Contract Entitlements: Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.
	C28-S Smart Contract Roles: Define standard roles to determine who can access smart contract data and functions.
	C29-S Emergency Stop: Ensure that smart contracts have an embedded kill switch or process to halt all activity, which can be accessed by a role with elevated permissions.
	C30-S Account Pause: Ensure that a user can freeze or pause activity for a given investor or wallet, controlled by either the agent of the investor or a role with elevated permissions.
	C31-S Token Pause: Ensure that a user can freeze or pause activity for all or some of the token inventory, controlled by either the agent of the investor or a role with elevated permissions.
R29 Financial Institution Insolvency A broker-dealer or custodian becomes insolvent, and protections are not in place to ensure customer assets are bankruptcy remote.	**C6-L Terms and Conditions:** Establish a legal basis for a service based on rules and/or contractual agreements that bind both the service provider and stakeholders. The terms of service should also establish the parameters for transfer, custody, control of assets consistent with applicable laws, regulations, and other regulatory requirements for the service provider and stakeholders.
	C10-L Asset Safeguarding and Segregation: Implement stringent controls to ensure customer assets are safeguarded and segregated from the custodian's or broker-dealer's own assets. This includes maintaining customer assets with a trusted, regulated custodian and establishing clear separation protocols to prevent asset commingling and misuse.
	C25-S Bookkeeping: Conform to an accounting model that supports both private (non-publicly traded) and public (publicly traded) securities. Adapt the accounting model to comply with international digital asset securities reporting standards.
	C26-S Account Structure: Conform to a common model to represent investor accounts that delineate what accounts are customer vs. proprietary and have the appropriate level of attribution.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

5. Connectivity and Interoperability

Return to Principles overview on page 11

This figure shows the risks associated with the principle “Connectivity and Interoperability,” as well as the controls to mitigate these risks:

Risks	Controls
R30 Interoperability Risk The risk pertains to the complexities of integrating digital assets with traditional financial systems and, potentially, multiple blockchain architectures (e.g., public, public -permissioned, and private) to ensure seamless transactions across the entire financial spectrum.	**C21-S Intraoperability Between DLT Networks:** Adhere to industry-accepted cross-network communication protocols specifically designed for blockchain interoperability. This includes standardized protocols for asset representation, transaction formats, and data exchange between different blockchain networks, ensuring seamless and secure interactions across diverse blockchain platforms.
	C35-R Event Monitoring and Alerts: Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.
	C54-N Legacy Infrastructure Integration: Provide a method or abstraction layer that enables users to access their security holdings through either classic or new DLT infrastructure.
	C55-N Third-Party Integration Guidelines: Establish rigorous guidelines for third-party services integration to maintain security across interconnected platforms.
R31 Network Utilization and Fragmentation The risk that a digital assets platform faces diminished operational viability and value due to low user engagement and transaction volume.	**C56-N Community Engagement Framework:** Ensure the existence of a stakeholder collaboration program that enhances risk management and platform security through active feedback and problem-solving channels. This program should provide specific forums and channels for feedback, issue reporting, and collaborative problem-solving. Establish best practices and shared standards through active feedback and collaborative initiatives.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

6. Operational Scalability

Return to Principles overview on page 11

This figure shows the risks associated with the principle “Operational Scalability,” as well as the controls to mitigate these risks:

Risks

R32 Inability to Scale

DLT networks may not efficiently manage or scale to accommodate surging transaction volumes, impacting critical functions such as post-trade capture and overall transaction throughput (including suitable customer support), potentially degrading system performance and reliability.

Controls

→	**C21-S Intraoperability Between DLT Networks:** Adhere to industry-accepted cross-network communication protocols specifically designed for blockchain interoperability. This includes standardized protocols for asset representation, transaction formats, and data exchange between different blockchain networks, ensuring seamless and secure interactions across diverse blockchain platforms.
→	**C22-S Token Specification Model:** Define smart contract requirements through a human readable markup language that models smart contract specifications and can be easily understood by business, operations, and IT personas.
→	**C23-S Data / Properties:** Ensure data properties embedded into a smart contract conform to recognized nomenclature and conventions. Data must sufficiently identify and describe the security (e.g., standard security IDs) and incorporate or have access to the data required to process life cycle events.
→	**C24-S Functions / Behaviors:** Conform to a common set of functions, behaviors and service level agreements that support various security life cycle operations such as issuance and settlement.
→	**C25-S Bookkeeping:** Conform to an accounting model that supports both private (non-publicly traded) and public (publicly traded) securities. Adapt the accounting model to comply with international digital asset securities reporting standards.
→	**C26-S Account Structure:** Conform to a common model to represent investor accounts that delineate what accounts are customer vs. proprietary and have the appropriate level of attribution.
→	**C28-S Smart Contract Roles:** Define standard roles to determine who can access smart contract data and functions.
→	**C29-S Emergency Stop:** Ensure that smart contracts have an embedded kill switch or process to halt all activity, which can be accessed by a role with elevated permissions.
→	**C30-S Account Pause:** Ensure that a user can freeze or pause activity for a given investor or wallet, controlled by either the agent of the investor or a role with elevated permissions.
→	**C31-S Token Pause:** Ensure that a user can freeze or pause activity for all or some of the token inventory, controlled by either the agent of the investor or a role with elevated permissions.
→	**C54-N Legacy Infrastructure Integration:** Provide a method or abstraction layer that enables users to access their security holdings through either classic or new DLT infrastructure.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

6. Operational Scalability (continued)

Return to Principles overview on page 11

Risks	Controls
R33 Digital Asset Liquidity This risk arises from the rapid and substantial liquidity shifts in digital asset markets, potentially amplified by real-time settlement and other settlement methods.	**C35-R Event Monitoring and Alerts:** Implement a system to monitor and audit operations in real time and automatically generate alerts. Ensure that alerts are triggered based on predefined thresholds of key metrics to promptly identify and respond to operational anomalies or deviations from standard procedures.
	C57-N Liquidity Management Strategies: Develop comprehensive strategies to actively manage liquidity levels for digital assets, ensuring the availability of sufficient resources to meet these needs in various market conditions. Incorporate regular stress testing to evaluate the robustness of liquidity under various market conditions and ensure the adequacy of these asset pools.
R34 Reputational Risk The inherent newness of DLT can enhance reputational risk due to its association with high-profile controversies and the potential for misuse. Public perception is influenced by DLT's complex nature, often leading to misunderstandings and negative connotations from its early-use cases.	**C56-N Community Engagement Framework:** Ensure the existence of a stakeholder collaboration program that enhances risk management and platform security through active feedback and problem-solving channels. This program should provide specific forums and channels for feedback, issue reporting, and collaborative problem-solving. Establish best practices and shared standards through active feedback and collaborative initiatives.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

6. Operational Scalability (continued)

Return to Principles overview on page 11

Risks	Controls
R35 Market Inefficiency The risk that structural issues or implementation frictions within the DLT ecosystem lead to significant disparities between the intrinsic value of digital assets and their market pricing, facilitating undue arbitrage opportunities.	**C1-L Participation Guidelines:** Establish fair and open but risk-based criteria (financial, jurisdictional, etc.) for user types and third-party service providers permitted to participate in a product, program, or service offering. Include advanced due diligence and continuous compliance monitoring tailored to digital asset markets, ensuring alignment with evolving jurisdictional regulations.
	C3-L Network and Oracle Vetting: Conduct thorough checks on network and oracle alignment with DLT standards and governance structures before integrating third-party tools. Validate reliability and security SLAs for all networks and oracles rigorously.
	C7-L Governance: Define clear governance arrangements, detailing oversight and management of the service.
	C11-L Policies and Procedures: Document comprehensive policies and procedures that cover all aspects of business operations and IT functionalities, including protocols for blockchain management and smart contract deployment. Incorporate regular testing strategies such as simulations, stress tests, and security audits to ensure compliance with security standards and regulatory requirements. Regularly update these policies and testing methods to align with technological advancements and regulatory changes.
	C18-S Code Auditing: Ensure all smart contract code is tested for vulnerabilities, bugs, performance issues or defects by an independent third-party auditor.
R36 Inadequate Stakeholder / Client Understanding of Digital Asset Securities Risks associated with inadequate educational and training programs for stakeholders and clients. It emphasizes the essential need for comprehensive and effective training to ensure that all involved parties fully understand the technological frameworks, regulatory landscapes, and operational processes unique to digital asset securities.	**C12-L Education and Training for Stakeholders on Digital Asset Securities:** Implement comprehensive education and training programs for all stakeholders involved with digital asset securities. These programs should cover the fundamental principles of digital assets, the associated technologies, regulatory compliance requirements, risk factors, and best practices.

L – Legal, **S** – Smart Contract Governance, **R** – Resilience and Data Protection, **N** – Network Settlement

Contributors

This white paper is a synergistic collaboration between DTCC, Clearstream, and Euroclear, augmented by support from the Boston Consulting Group. The strategic direction and guidance originated from the Steering Committee, while the Working Group – consisting of industry experts and practitioners – drove the effort and provided oversight. In addition, the Steering Committee and Working Group would like to express their gratitude to the contributing partners for their expertise and for sharing their valuable perspectives during the development of the DASCP framework.

Steering Committee:

Nadine Chakar

Managing Director and Global Head of DTCC Digital Assets

Jens Hachmeister

Managing Director and Head of Issuer Services and New Digital Markets at Clearstream

Philippe Laurensy

Managing Director and Head of Product Strategy and Innovation at Euroclear

Kaj Burchardi

Managing Director, BCG Platinion Netherlands

Working Group

Renée Berman
Managing Director, DTCC Digital Assets

Doug Meyers
Director, CSS Strategy, DTCC

Robert Lanni
Analyst, DTCC Digital Assets

Thilo Derenbach
Head of Sales and Business Development
Digital Securities Services, Clearstream

Vic Arulchandran
Digital Securities Services at Clearstream

Jorgen Ouaknine
Global Head of Innovation and
Digital Assets, Euroclear

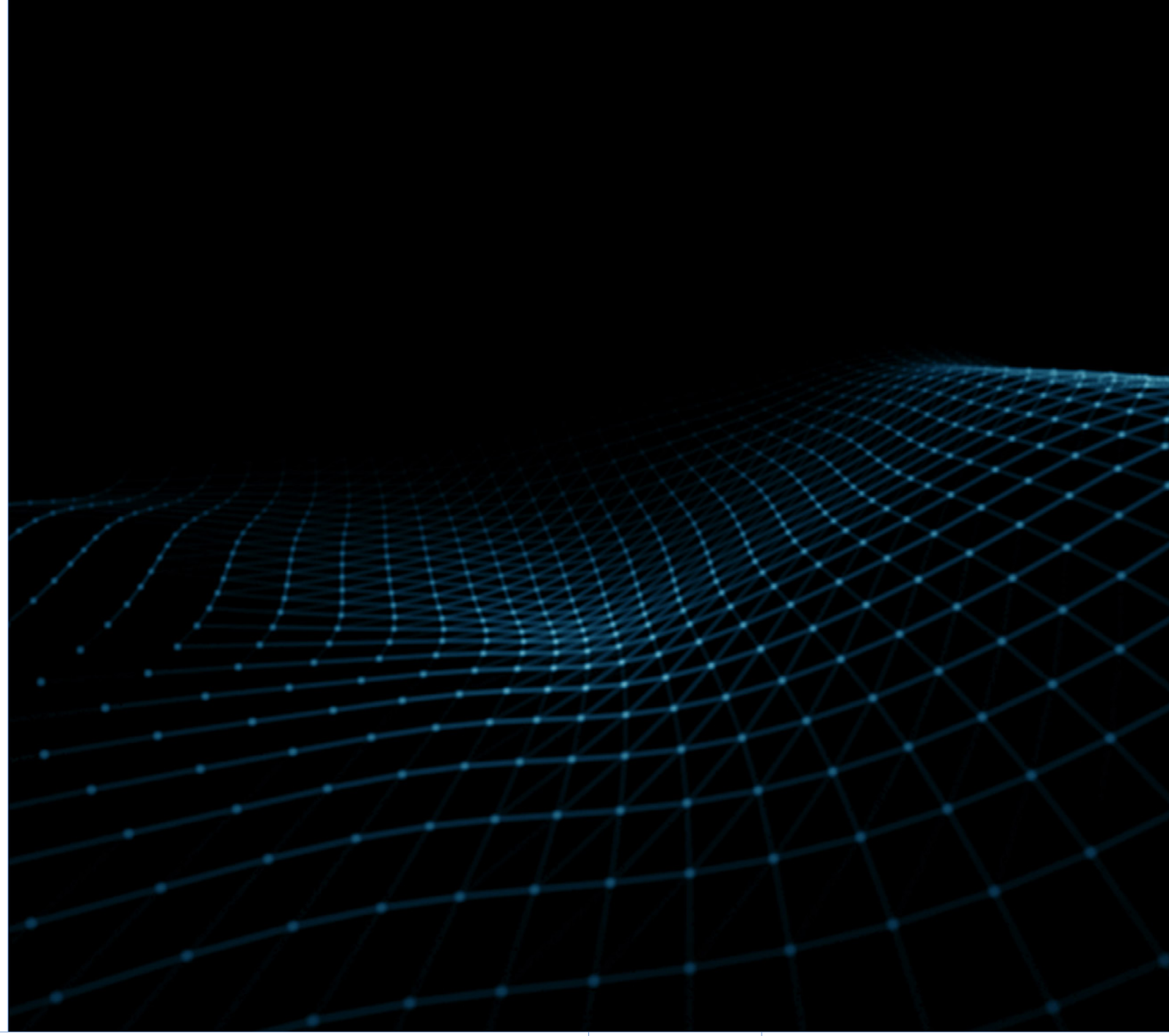
Stephanie Lheureux
Head of Digital Assets Excellence
Center at Euroclear

Frédéric Brugère
Managing Director and Partner

Bernhard Kronfellner
Partner and Associate Director

Bob Baksa
Associate Director

Alexandre Lefoulon
Principal IT Architect



About DTCC, Clearstream, Euroclear, and BCG

With over 50 years of experience, DTCC is the premier post-trade market infrastructure for the global financial services industry. From 20 locations around the world, DTCC, through its subsidiaries, automates, centralizes, and standardizes the processing of financial transactions, mitigating risk, increasing transparency, enhancing performance, and driving efficiency for thousands of broker-dealers, custodian banks, and asset managers. Industry-owned and governed, the firm innovates purposefully, simplifying the complexities of clearing, settlement, asset servicing, transaction processing, trade reporting, and data services across asset classes, bringing enhanced resilience and soundness to existing financial markets, while advancing the digital asset ecosystem. To learn more, visit dtcc.com.

Clearstream is the innovative and trusted post-trade business for the global markets. It runs the leading securities and funds servicing ecosystems of tomorrow. The company operates the German and Luxembourg central securities depositories and an international central securities depository for the Eurobonds market. With 18 trillion euros in assets under custody, it is one of the world's largest settlement and custody firms for domestic and international securities. Its digital post-trade platform D7 provides a fully digital alternative to conventional physical issuance and processing of securities. It also delivers premier fund execution, distribution, data, and reporting services, covering over 55 fund markets worldwide. Clearstream is part of the Deutsche Börse Group, an international exchange organization and provider of innovative market infrastructures. To learn more, visit us at clearstream.com.

Euroclear group is the financial industry's trusted provider of post-trade services. Guided by its purpose, Euroclear innovates to bring safety, efficiency, and connections to financial markets to sustain economic growth. Euroclear provides settlement and custody to domestic and cross-border securities for bonds, equities and derivatives, and investment funds. As a proven, resilient capital market infrastructure, Euroclear is committed to delivering risk-mitigation, automation, and efficiency at scale for its global client franchise. The Euroclear group comprises Euroclear Bank, the International CSD, as well as Euroclear Belgium, Euroclear Finland, Euroclear France, Euroclear Nederland, Euroclear Sweden, Euroclear UK and International and MFEX by Euroclear. To learn more, visit euroclear.com.

Boston Consulting Group is a global consulting firm that partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG's success depends on a spirit of deep collaboration and a global community of diverse individuals determined to make the world and each other better every day. To learn more, visit bcg.com.