DEPÓSITO CENTRAL DE VALORES

Disclosure Framework
Principles for Financial Market Infrastructures
(PFMI)

April 2026

Reporting Institution: **Depósito Central de Valores**
Jurisdiction where the FMI operates: **Chile**
Authority responsible for the regulation, supervision, or oversight of the FMI: **Financial Market Commission (CMF)**
Date of disclosure: **04/30/2026**
The information provided here is also available at **www.dcv.cl**
For more detailed information, please contact **Cristian Peña (cpena@dcv.cl)**

GLOSSARY

AFP	Administradora de Fondos de Pensiones (Pension Fund Manager)
BCP	Business Continuity Plan
BCCH	Banco Central de Chile (Central Bank of Chile)
BCS	Bolsa de Comercio de Santiago (Santiago Stock Exchange)
BEC	Bolsa Electrónica de Chile (Electronic Stock Exchange of Chile)
BIA	Business Impact Analysis
CCLV	CCLV Contraparte Central S.A. (CCLV Central Counterparty ltd.)
CCP	Central Counterparty
CF	Core consideration
CMF	Comisión para el Mercado Financiero (Financial Market Commission)
CSD	Central Securities Depository
CPMI	Committee on Payment and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems (now CPMI)
DVP/ECP	Delivery versus Payment
IMF	Financial Market Infrastructure
GRC	Governance, Risk, and Compliance (GRC)
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Standards Organization
KPI	Key Performance Indicators
RTGS	Real-Time Gross Settlement
MOU	Memorandum of Understanding
OLA	Operational Level Agreement
OTC	Over the Counter
PFMI	Principles for Financial Market Infrastructures
PS	Payment System
RPO	Recovery Point Objective
RTGS	Real-time gross settlement system
RTO	Recovery Time Objective
SSAE	Statement on Standards for Attestation Engagements
SSS	Securities Settlement System
SWIFT	Society for Worldwide Interbank Financial Telecommunication

CONTENTS

PREAMBLE

This Disclosure Framework regarding the implementation of compliance with the "Principles for Financial Market Infrastructures" (PFMI) by Depósito Central de Valores S.A., Depósito de Valores (DCV), aims to explain to its users, authorities, and the public how DCV has implemented and complies with the PFMI.

The PFMI, published in April 2012 by the Committee on Payments and *Market Infrastructures* of *the International Organization of Securities Commissions* (CPMI-IOSCO), constitutes a comprehensive framework of international standards aimed at strengthening the safety and efficiency of financial market infrastructures (FMI). These principles address, among other aspects, risk management, corporate governance, the applicable legal framework, resilience and operational continuity, as well as transparency and disclosure of information.

The PFMI consists of 24 principles, 14 of which apply to all financial market infrastructures. The remaining principles apply depending on the nature of the infrastructure, including specific principles for securities settlement systems (SSSs), central securities depositories (CSDs), and central counterparties (CCPs), among which are principles applicable exclusively to the latter.

The Disclosure Framework contributes to a clearer understanding of the DCV's activities, its risk profile, and risk management practices, thereby facilitating sound decision-making by its stakeholders. To this end, Principle 23 of the PFMI establishes that Financial Market Infrastructures must promote transparency toward the public and stakeholders through the Disclosure Framework, which must be based on the "Disclosure and Assessment Framework Methodology" published in December 2012 by the CPMI-IOSCO.

As it operates solely as a central securities depository (CSD), principles 1, 2, 3, 10, 11, 15, 16, 17, 18, 20, 21, 22, and 23 apply to the DCV.

I. EXECUTIVE SUMMARY

The DCV holds in custody publicly traded securities, primarily those held by institutional investors (insurance companies, banks, pension fund managers, and investment funds), as well as those held in custody by brokerage firms, either on their own account or on behalf of their clients. Likewise, the DCV electronically records securities trading transactions and facilitates the transfer of ownership resulting from trading transactions carried out by its depositors, originating in the stock market as well as in the over the counter (OTC) market.

The DCV was established in 1993 and began operations in 1995. The DCV operates as a central securities depository (CSD) in Chile and is the only entity providing this service in the country. It is an entity owned by its users, which includes stockbrokers (through the stock exchanges) and institutional investors.

The primary legal framework governing the DCV is Law 18,876 (*"Establishing the Legal Framework for the Constitution and Operation of Private Securities Depository and Custody* Entities"). The DCV is regulated and supervised by the Chilean Financial Market Commission (CMF).

Because the DCV operates solely as a CSD, without acting as a securities settlement system in the strict sense, its systems are exposed to operational risk, custody risk, and general business risk, but it does not directly assume credit or liquidity risks.

II. SUMMARY OF THE MOST SIGNIFICANT CHANGES SINCE THE LAST DISCLOSURE

During 2024 and 2025, the DCV has driven a transformation agenda aimed at expanding its role beyond traditional custody and modernizing its technological infrastructure. In terms of services, the DCV has strengthened its approach to customer relationships and experience by creating the Commercial Department, organized around three pillars: transforming the commercial relationship into a strategic one, optimizing the efficiency of customer service, and developing management centered on customer experience.

It has also carried out the migration from ISO 15022 to ISO 20022 standards, in coordination with the Central Bank of Chile and international counterparts, which contributes to improving the interoperability, standardization, and efficiency of processes.

In terms of market integration and operations, the DCV has supported initiatives aimed at enabling new settlement methods, notably access to delivery-versus-payment (DVP) schemes in US dollars in coordination with Combanc. It has also made progress on agreements with the regional stock exchange holding company nuam exchange to centralize the custody of international securities currently held in the group's own central depositories. Operational integration with nuam also involves process standardization, technological interoperability, and improved access to markets in Chile, Colombia, and Peru.

In the area of innovation, the DCV has deepened its fintech strategy by developing digital issuance solutions for financial instruments, initially in conjunction with the Central Bank of Chile and later with BCI Bank, as well as by exploring the issuance and custody of digital financial instruments under tokenization schemes. This development is complemented by tools designed to manage the ownership of securities issued by emerging companies. Likewise, there is growing integration with digital platforms that provide financial services regulated under the 2023 Fintech Law.

Furthermore, the DCV has undertaken technological modernization processes to address obsolescence, such as in the case of recognition bonds, and has launched a new forward contract registration service, developed in collaboration with market participants and focused on the capture, standardization, and consolidation of information regarding these instruments.

Looking ahead to 2026, the DCV is developing initiatives with systemic scope. Of particular note is the design of a repo market, whose architecture has been the subject of an extensive analysis process involving authorities, technology providers, and international stakeholders, with its implementation planned in coordination with Combanc.

As part of Chile's recent pension reform, government debt instruments will be issued to participants in the system to supplement their future pensions. These instruments will be held in custody by the DCV, which will be responsible for their registration and administration task involving the management of approximately 6 million individual accounts, thereby consolidating its role as the operational backbone of the new system. Finally, the acquisition of RiskAmerica, a company specializing in financial instrument valuation and risk management, opens a new line of business in financial analysis and engineering, which is still in the strategic development phase.

III. GENERAL CONTEXT OF THE FMI

A. Overview of the DCV and the markets it serves

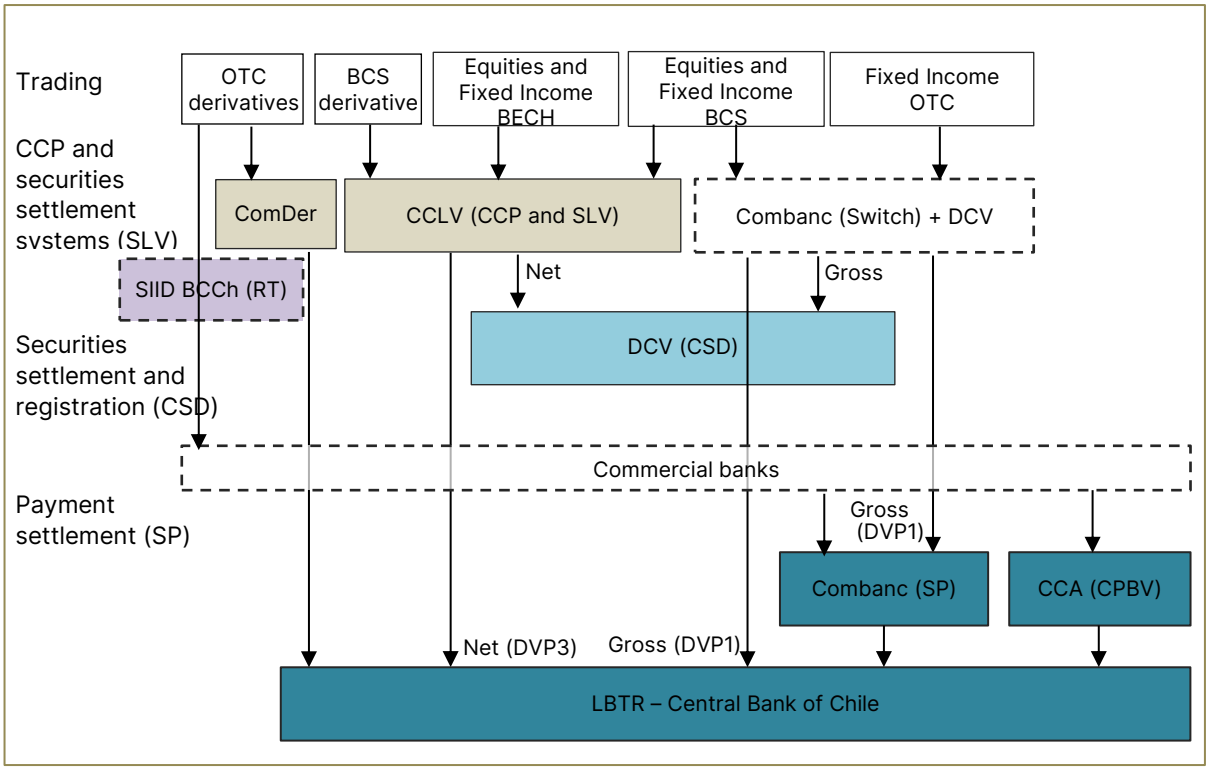
General description and the market it serves

The DCV holds publicly traded securities in custody, primarily those owned by institutional investors (insurance companies, banks, pension fund managers, and investment funds), as well as those held by brokerage firms, either on their own account or on behalf of their clients. In addition to providing securities custody, the DCV electronically records transactions and facilitates the transfer of ownership resulting from trading activities conducted by its depositors. These transactions originate in both the stock market and the over the counter (OTC) market.

In its capacity as a CSD, the DCV interacts with virtually all participants in the Chilean financial market, as shown in the following chart. Thus, it interacts with investors, in their capacity as DCV depositors, by offering custody services and executing instructions for the transfer of traded securities, originating either on the stock exchanges or in the OTC market. Likewise, in the task of securities settlement, it interacts operationally with payment systems and securities settlement systems. On the other hand, it interacts with issuers of publicly offered securities, as they conduct their securities offerings using DCV's services; and in the case of corporations, DCV's subsidiary, DCV Registros, manages the shareholder registries and corporate events for a large portion of Chilean companies. Finally, the DCV is subject to supervision by the Financial Market Commission (CMF) and, in turn, provides various authorities with information to support their regulatory work.

Figure 1 presents an overview of the securities clearing and settlement system in Chile. Securities clearing and settlement 21is carried out through multilateral and bilateral processes, depending on the origin of the transaction. In general, stock market transactions—that is, those carried out on the BCS and the BEC—are cleared through multilateral procedures by the central counterparty clearing house CCLV and settled in the DCV, and in the BCCh's LBTR System, for securities and payments, respectively. On the other hand, DVP transactions between AFPs and stockbrokers related to stock exchange transactions (referred to as "cycles" 1 and 3 of the AFP settlement process), as well as fixed-income transactions traded on OTC trading mechanisms, are settled through gross bilateral processes, through a bilateral DVP settlement service offered in coordination with the Combanc large value payment system (the latter using its "Switch" functionality), which also clears other payments initiated by banks, and which then, like CCA, the low-value payment clearinghouse, settles the resulting net balances in the LBTR System. Derivatives transactions are settled in the CCLV when traded on an exchange. In the case of over-the-counter transactions, these are settled through the Comder Central Counterparty Clearing House or recorded in the BCCh's derivatives transaction repository, known as the Integrated Derivatives Transaction Information System (SIID-TR).

Figure 1. Architecture of Securities Clearing and Settlement and Payments in Chile



Key statistics

Key statistics (December 2025)

Total amount under domestic custody	US$ 438.547 billion
Percentage held in fixed income (domestic custody)	53%
Percentage held in equities (domestic custody)	31%
Percentage held in financial intermediation (domestic custody)	16%
Percentage of dematerialized instruments	98.8%
Total amount transferred during 2025	US$ 3,285,309 million
Number of transfers in 2025	3,416,836
Total amount transferred in December 2025	US$ 496,782 million
Number of transfers in December 2025	308,338
Total amount under international custody	US$ 3.519 billion

Figure 2. Amounts under custody (millions of US$)

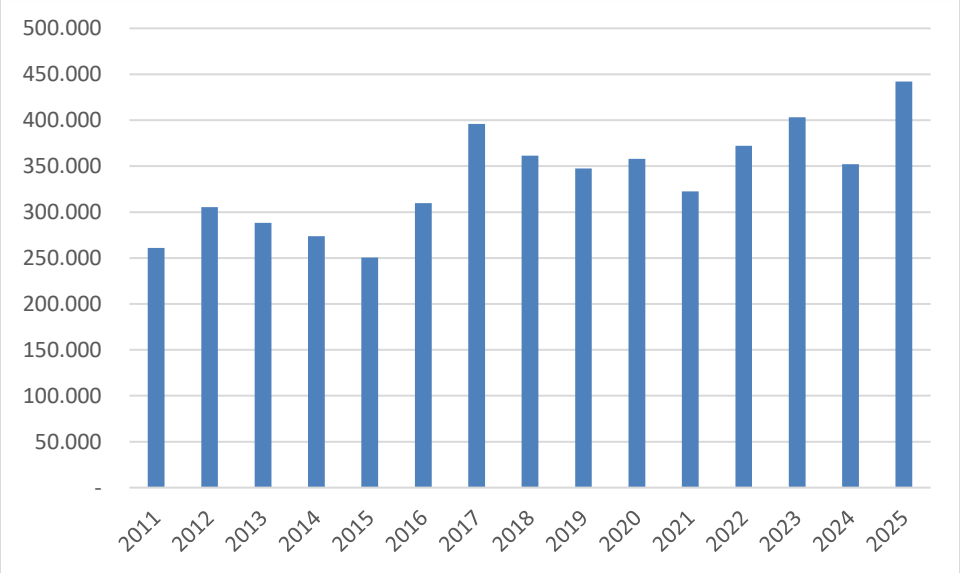
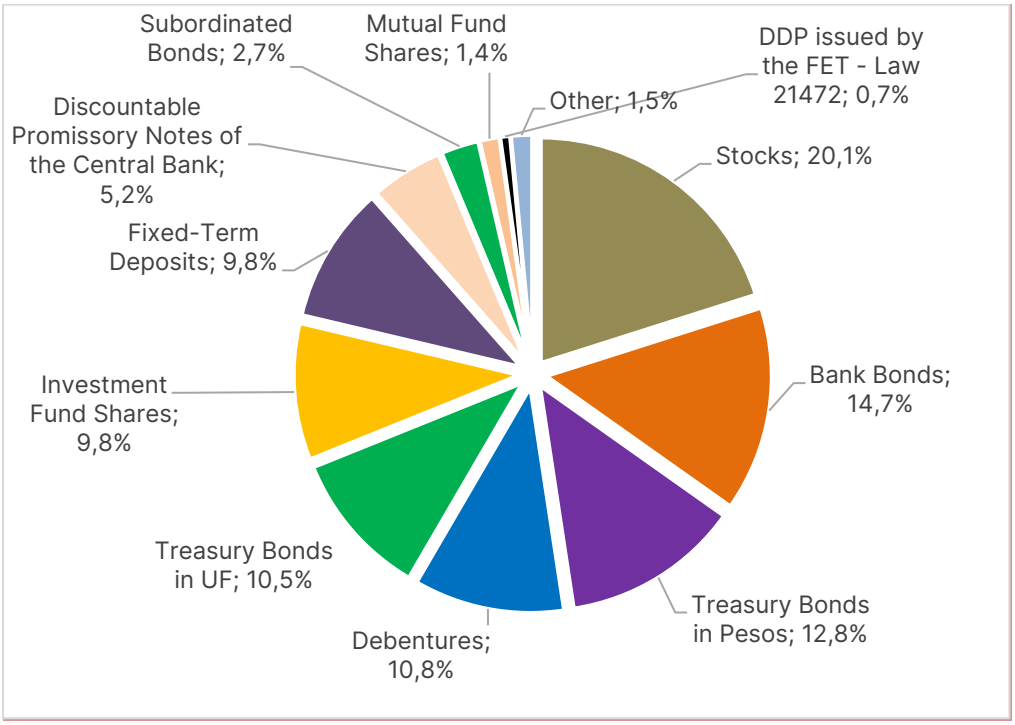


Figure 3. Types of instruments under custody



B. General Organization of the DCV

The DCV is a Chilean company and, as such, is organized and regulated under Chilean law. As a securities depository, it is legally incorporated under Law 18,876, which regulates "Private Securities Depository and Custody Entities." Its legal structure corresponds to that of a Chilean corporation, and therefore the provisions of Law 18,046 on Corporations also apply to it.

The ultimate shareholders of the DCV are domestic banks (30%), pension fund administrators (30%), Holding Bursátil Regional S.A. (nuam exchange, which acquired the BCS's stake) (23.14%), insurance companies (10%), the Electronic Stock Exchange (6.4%), and other shareholders (0.46%). DCV's corporate governance is based on a mutual ownership structure, under which its shareholders are, in turn, companies representing the various industries or market sectors in which the depositors operate.

At the shareholders' meeting, the shareholders appoint the DCV board of directors, composed of 10 members, who serve two-year terms and may be reelected indefinitely.

The board has five committees (Audit, Clients and Business Development, Risk Management and Cybersecurity, IT and Operational Efficiency, and People and Sustainability).

The **Audit Committee** oversees the internal audit, reviews reports from external auditors and the CMF, analyzes financial statements, related-party transactions, conflicts of interest, and fraud, and may order special audits. Composed of three directors; it meets at least eight times a year.

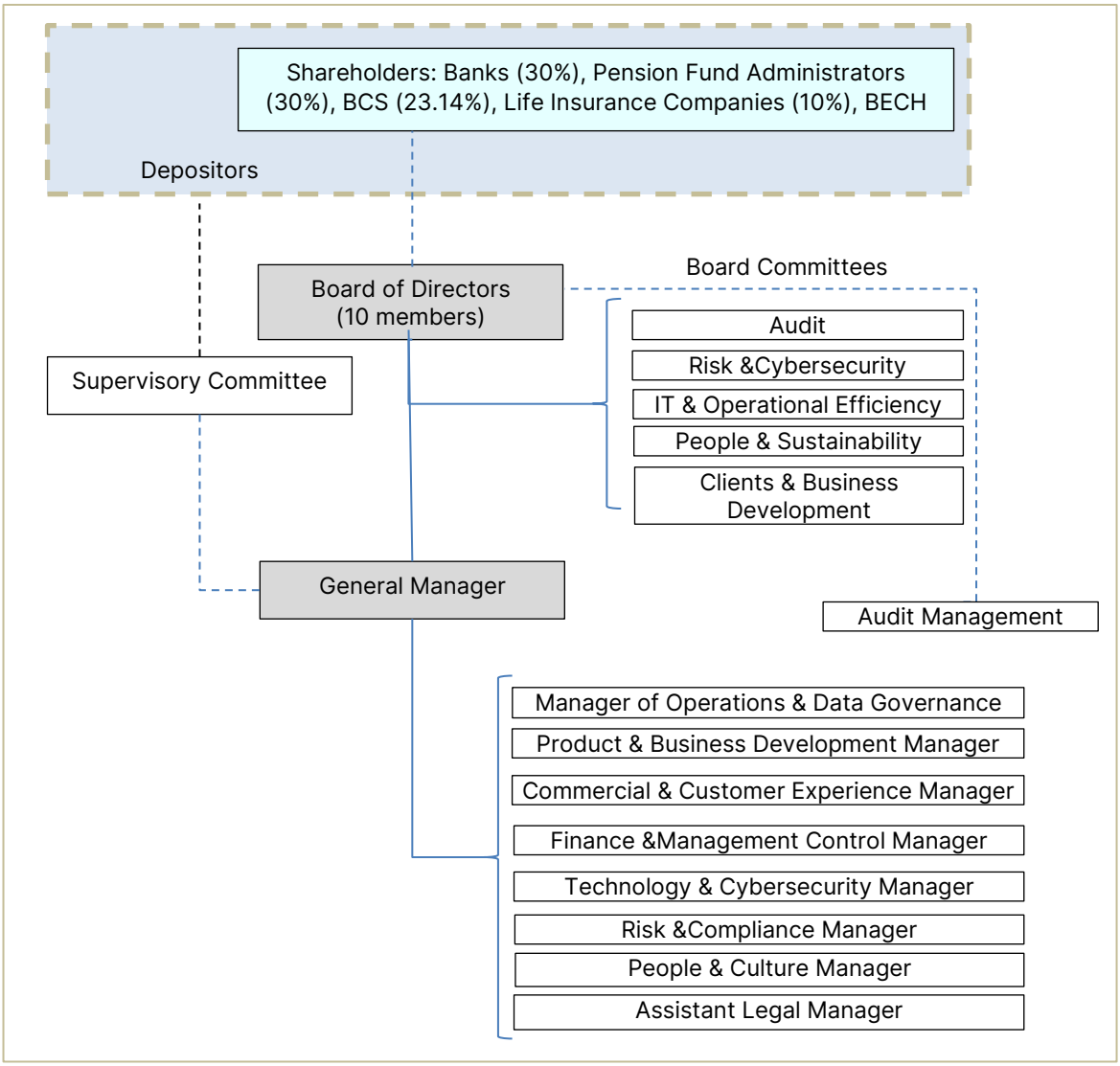
The Customers and Business Development Committee proposes strategic definitions (mission, vision, values), business initiatives, services, rates, and plans to the Board of Directors. It reviews projections, the strategic plan, and investments. Composed of three directors; it meets at least six times a year.

The Risk Management and Cybersecurity Committee supports the oversight of risk management, regulatory compliance, and the crime prevention model, in accordance with Board policies and agreements. Composed of three directors; meets at least six times a year.

The IT and Operational Efficiency Committee proposes the technology strategy, prioritizes projects and resources, and reviews operational and technology infrastructure performance. Composed of three directors; meets at least six times a year.

The People and Sustainability Committee defines compensation, benefits, and incentive policies, and sets compensation for the CEO and managers. Composed of three directors, it meets at least twice a year.

DCV's executive management is led by its General Manager, who in turn reports directly to the Board of Directors. In addition to the General Manager, there are nine senior managers, as shown in the box below.



DCV depositors meet in regular or special meetings. Regular meetings are held once a year to decide on matters within their purview. Special meetings may be held at any time as determined by the DCV, or upon request by the Oversight Committee or the depositors.

The Oversight Committee is a body created and regulated by Law 18,876, responsible for the internal oversight of the company's operations and those between the company and the depositors themselves. As provided by law, this committee is composed of five depositor representatives and is mandated with the following functions.

First, it must verify that custody, clearing, settlement, and transfer operations are carried out fully and in a timely manner. Additionally, it must conduct quarterly audits of the company and verify the accuracy and reconciliation of depositors' accounts.

Additionally, it is responsible for verifying that the information available to depositors is sufficient, accurate, and timely, as well as for ensuring that depositors fulfill their obligations in a timely and satisfactory manner, both with respect to other depositors and to the company itself.

It must also verify the quality of the facilities and security systems, along with the quality and amount of existing guarantees and insurance policies.

Furthermore, the Committee must report to the CMF any deficiencies, discrepancies, and irregularities it detects, suggesting the measures it deems appropriate to address them or prevent their recurrence. Similarly, it must inform the depositors' assembly of any situation that may affect their interests.

Finally, it is responsible for performing any other function necessary for the adequate security of the system.

C. Legal and Regulatory Framework

The main legal framework governing the DCV is Law 18,876 (*"Establishing the Legal Framework for the Formation and Operation of Private Securities Depository and Custody* Entities"). This law establishes the legal basis for the deposit contract, who may become participants in the company, the main relationships between the participant and the company, the legal implications of the company's actions—including transfers, the creation of pledges, ownership of securities, the finality of settlement, and the company's liabilities.

Law 18,876 also establishes operational requirements, including the existence of Internal Regulations governing the relationship between the company and depositors and the provision of a publicly available fee schedule supporting the fee structure. It also establishes the existence of a depositors' assembly, whose primary purpose is to appoint the Oversight Committee and determine its annual objectives, monitor the performance of these tasks, and oversee those duties imposed by law on the committee. The law further provides for procedures in the event of a capital deficit, including reorganization and orderly liquidation procedures.

On the other hand, Supreme Decree 734 (issued by the Ministry of Finance) establishes the procedure for approving the operation of companies, the content of the Internal Regulations, as well as the Deposit Agreement that the company must sign with each of its depositors. It also includes provisions regarding the deposit and withdrawal of securities, the opening and closing of accounts, and reporting and oversight obligations, such as the submission of financial statements and the requirement for an external audit with respect to the company's own operations and those related to the custody of securities.

The Financial Market Commission (CMF) is responsible for supervising the DCV. Its role is to supervise and regulate the insurance industry, the banking industry, and the securities market, including stock exchanges, fund managers, securities brokers, corporations, and financial market infrastructure.

Regarding regulations issued by the CMF, some of its most relevant rules are as follows:

General Rule 223. This regulation defines the information that deposit and custody institutions must make available to account holders with individual accounts, as referred to in Article 179 of Law 18,045.

General Rule 224. Given that Law 18,876 stipulates that a publicly available fee schedule must be provided to support the compensation structure, this regulation establishes minimum content requirements for the preparation of the fee schedule that securities deposit and custody firms must provide.

General Rule 509. This regulation establishes guidelines for risk management, internal control, and governance in entities supervised by the CMF, promoting the adoption of formal frameworks that enable the identification, assessment, and mitigation of risks relevant to their operations. It also reinforces the role of the board of directors and senior management in overseeing these risks, contributing to the stability and proper functioning of the entities and, consequently, to an adequate level of information and transparency toward the market.

General Rule 510. This regulation complements General Rule 509 by establishing specific requirements regarding operational risk, cybersecurity, and business continuity, requiring institutions to have adequate policies, procedures, and governance structures for managing these risks.

D. Design of the System and Activities of the FMI

DCV Services

The DCV organizes its services into an integrated set of offerings that cover both basic market operations and complementary support and administrative functions. At the core are custody and settlement services, both domestically and internationally, which include the administration of various types of accounts—proprietary, third-party, and client accounts—the custody of securities, and the execution of transactions such as purchases, sales, transfers, settlements, and the deposit and withdrawal of digital instruments. Internationally, the DCV maintains operational links with foreign CSDs—Euroclear (Belgium), DECEVAL (Colombia), and CAVALI (Peru)—and maintains a link with the global custodian Citibank, allowing DCV depositors to trade in markets across Latin America, Europe, and Asia.

In addition to the above, the DCV provides services related to the securities lifecycle, which include the issuance of financial instruments—such as fixed-income securities, equities, financial intermediation, digital issuance, and digital financial assets—along with the assignment of ISIN codes. Furthermore, the DCV manages capital events, such as shareholder meetings, dividend payments, corporate or debt restructurings, and other corporate events that affect the instruments and their holders.

The DCV also provides operational and legal support services, including the creation and registration of guarantees, liens, and judicial measures, such as special liens, electronic lien registries, notarial liens, mining guarantees, attachments, and other judicial measures, in addition to the registration of forward-type derivative contracts. In parallel, it offers information and compliance services, which include the issuance of statistical reports, certificates—

including tax-related ones—tax annexes, and document validation, along with tax-related functions such as acting as a responsible agent and managing tax returns.

Finally, the DCV provides services related to the administration of shareholder registries for corporations and investment fund contributors, as well as digital subscription and redemption processes for shares and services for shareholders. This suite is complemented by solutions focused on new technologies, such as fintech services, which include tools like cap tables and the custody of financial instruments in digital environments, creating a comprehensive offering that addresses the diverse needs of the securities market.

Key Risks

The DCV is exposed to operational risk and custody risk, as well as general business risk. However, it does not assume credit or liquidity risks. Operational risk management is focused on assessing the risks associated with the following categories:

People. This refers to the risk of losses, whether intentional or unintentional, caused by or involving employees. This type of risk causes internal organizational problems and losses.

Third-Party Relationships. This refers to losses incurred by the company that arise from the firm's relationships or interactions with its customers, shareholders, third parties, regulators, and stakeholders.

Processes. This refers to risks related to the execution and maintenance of operations and various aspects of business execution, including products and services.

Technological. This refers to risks of loss caused by piracy, theft, failures, interruptions, or other disruptions in technology, data, or information; it also includes technology that does not contribute to achieving business objectives.

External. Refers to risks of loss due to damage to tangible property or intangible assets caused by natural or non-natural causes. This risk category also includes actions caused by external agents, such as the commission of fraud. In the case of regulators, this includes the enactment or amendment of regulations that could disrupt the firm's ability to continue operating in a particular market.

IV. SUMMARY DISCLOSURE PRINCIPLE BY PRINCIPLE

Principle 1: Legal Basis

An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

Key consideration 1: The legal basis should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions.

Material Aspects and Relevant Jurisdictions

The essential aspects of the DCV's activities that require a high degree of legal certainty are: 1) Book-entry and dematerialization of securities, 2) Final settlement, and 3) Protection of depositors' assets, including the segregation of the securities of the depositor and its clients.

The relevant jurisdiction for each material aspect of an FMI's activities is Chile, with the exception of the international custody service, where the jurisdiction of issuance of the financial instruments held in custody is also relevant.

Legal basis for each key aspect

Dematerialization and book-entry

Article 11 of Law 18,876 permits securities to be issued in dematerialized form—that is, without physical certificates—through book entries at a deposit and custody firm. These entries replace the physical document and have full legal validity to prove the existence and ownership of the securities. Additionally, Article 7 establishes the validity of the mechanism of debits and credits to accounts for transfers of ownership, equating them to the physical delivery of securities with full enforceability against third parties upon execution. For its part, Article 14 bis grants full probative value to the certificates issued by the company acknowledging ownership.

Final Settlement

In the event of a participant's insolvency, Article 5 of Law 18,876 protects already settled positions through the automatic segregation of deposited securities from the insolvent party's assets, ensuring that registered transfers cannot be reversed by creditors or bankruptcy trustees.

Protection and Segregation of Depositors' Assets

Regarding the protection and segregation of assets, Articles 4, 5, 18, and 19 of Law 18,876 establish that deposited securities must be kept separate from the DCV's own assets and those of third-party participants, including custodians and financial intermediaries. This segregation ensures that depositors' assets are not commingled with other assets and remain identifiable and available at all times, even in the event of the insolvency of intermediaries or the entity itself. The regulation also ensures that the assets cannot be claimed by creditors of the custodians, providing a high level of legal and operational protection. Furthermore, Article 15 of the aforementioned law establishes that the securities acquired shall be deemed free of encumbrances, prohibitions, or attachments.

Key consideration 2: An FMI should have rules, procedures, and contracts that are clear, understandable, and consistent with relevant laws and regulations.

Clear, understandable, and consistent rules, procedures, and contracts

The DCV has demonstrated that its rules, procedures, and contracts are understandable by formalizing them in a comprehensive and structured set of documents, which includes its Internal Regulations, 47 manuals, 10 operational guides, 7 procedures, and more than 366 circulars currently in effect. This documentation systematically describes the processes, the rights and obligations of participants, as well as the main operational and control mechanisms, and is applied uniformly in daily operations. As of the date of the evaluation, no relevant incidents attributable to regulatory ambiguities or divergent interpretations of the system's rules have been identified.

Amendments to the rules and procedures follow a formal process; in the case of amendments to the Internal Regulations, these are approved by the Board of Directors in a formal meeting, authorizing their submission to the CMF along with an explanatory memorandum, and they enter into force once the CMF issues the express resolution approving them, which is communicated to participants via a circular.

The Internal Regulations and the deposit contract must be approved by the CMF and, in accordance with Supreme Decree 734, which approves the Regulations of Law 18,876, may only be amended with prior authorization from this authority. Furthermore, this legal instrument reinforces this requirement by specifying the minimum content that must be included in the central depository's internal rules and its deposit contract.

Key consideration 3: An FMI should be able to articulate the legal basis for its activities to relevant authorities, participants, and, where relevant, participants' customers, in a clear and understandable way.

The DCV communicates the legal basis for its activities to the relevant authorities and participants through formal communications addressed to depositors and by disclosing its applicable internal regulations on its website. Furthermore, the laws and regulations governing its operations are public and available for consultation on the relevant official websites, allowing participants and, where applicable, their clients, to access the legal framework underpinning its activities in a transparent manner.

Key consideration 4: An FMI should have rules, procedures, and contracts that are enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken by the FMI under such rules and procedures will not be voided, reversed, or subject to stays.

Enforceability of Rules, Procedures, and Contracts

The IMF derives a high degree of confidence in the enforceability of its rules, procedures, and contracts from a robust legal framework—public in nature and hierarchically clear—that provides legal certainty regarding the validity and enforceability of its provisions. Additionally, in the exercise of its functions, the DCV has periodically obtained independent legal opinions from law firms to verify the legal strength and consistency of its internal regulatory framework. As of the date of the assessment, no regulatory inconsistencies or interpretive discrepancies have been detected that would compromise the proper application of the DCV's legal and regulatory framework. Furthermore, there is no record of legal actions, claims, or disputes related to transactions processed in the system, nor any challenges regarding the legal validity or enforceability of the DCV's internal rules.

Degree of certainty regarding rules and procedures

The DCV's securities deposit and custody activities are expressly regulated by Law 18,876 and its supplementary regulations, and its internal rules and contracts with participants are structured in accordance with that framework, explicitly defining the rights, obligations, and legal effects of transactions registered and settled in the system. Regarding the possibility of invalidity, reversal, or suspension, the measures adopted by the DCV could only be affected under exceptional circumstances beyond its control, such as a judicial ruling invalidating an act due to a serious legal violation, or legislative or regulatory changes that expressly provide for the suspension of the rule. However, as of the date of the assessment, there is no record of judicial, administrative, or regulatory decisions that have challenged or invalidated the validity or enforceability of the rules, procedures, contracts, or transactions processed through the DCV.

Key consideration 5: An FMI conducting business in multiple jurisdictions should identify and mitigate the risks arising from any potential conflict of laws across jurisdictions.

The DCV has entered into agreements to open securities accounts with the CSDs DECEVAL in Colombia, CAVALI in Peru, and Euroclear in Belgium, as well as with the global custodian Citibank in the United States (see Principle 20). In providing the international custody service, through which the DCV holds its depositors' foreign securities with the aforementioned custodians, the contracts that investors in Chile sign with the DCV for this purpose establish that, for transactions involving securities held with foreign CSDs, the applicable law is that of the foreign CSD or foreign custodian.

Principle 2: Governance

An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

Key consideration 1: An FMI should have objectives that place a high priority on the safety and efficiency of the FMI and explicitly support financial stability and other relevant public interest considerations.

The DCV's mission statement establishes "its commitment to providing the local and international capital markets with infrastructure solutions and complementary services, under the highest standards of transparency, security, and efficiency." For its part, the institutional vision expresses the aspiration to "be a leader in providing infrastructure for the capital markets, standing out for excellence in execution, risk management, and innovation."

DCV manages its strategic objectives through a Balanced Scorecard, focused on four Strategic Perspectives: Shareholders and Finance, Clients and Service Delivery, Organization, and Risk Management (see Principle 21). DCV's objectives place a high priority on security through the Risk Management perspective, including regulatory compliance, integrity of assets in custody, cybersecurity, and business continuity. Efficiency is prioritized through the cost-efficiency ratio, while objectives supporting financial stability and the public interest require high standards of technological platform availability to ensure continuous service to the securities market.

Key consideration 2: An FMI should have documented governance arrangements that provide clear and direct lines of responsibility and accountability. These arrangements should be disclosed to owners, relevant authorities, participants, and, at a more general level, the public.

Governance Mechanisms

The DCV is incorporated as a special public limited company. The corporate governance rules for public limited companies under Law 18,046 apply to it, supplemented by Law 18,876, which establishes specific requirements for central securities depositories.

The DCV's corporate governance is based on a mutual ownership structure, under which its shareholders are, in turn, companies representing the various industries or market sectors in which the depositors operate, and they hold a proportional share on the board of directors, ensuring a certain alignment between ownership and the intensity of service use. The ultimate shareholders of the DCV are national banks (30%), Pension Fund Administrators (30%), Holding Bursátil Regional SA, the parent company of the Santiago Stock Exchange (23.14%), life insurance companies (10%), the Electronic Stock Exchange (6.4%), and other shareholders (0.46%).

The DCV Board of Directors, as the highest governing body, defines the institutional strategy, oversees senior management, and approves key policies regarding risk, regulatory compliance, and business continuity. It is supported by five specialized committees: Audit; Risk Management and Cybersecurity; People and Sustainability; IT and Operational Efficiency; and Clients and Business Development, whose operating rules detail specific responsibilities.

The DCV's Internal Regulations stipulate that the Board of Directors must ensure the proper

functioning and stability of the Company, as well as strict compliance with legal and regulatory standards. The same Regulations also govern the Oversight Committee elected by depositors and the operation of the Depositors' Assemblies.

In accordance with Chile's Corporations Act, the Board of Directors exercises a role of control and oversight over management, being responsible for demanding and reviewing accountability from senior management, as well as for verifying compliance with the legal, statutory, and regulatory provisions applicable to the DCV. This function is primarily carried out through the review of financial and management reports, the evaluation of internal and external audits, and ongoing interaction with the CMF, within the framework of the information and oversight requirements established by current regulations.

In addition, the Oversight Committee, an independent body elected by the Depositors' Assembly, fulfills an additional oversight and accountability function, given that, in accordance with Law 18,876, the Oversight Committee, among other functions, must "oversee the DCV's compliance with the legal, regulatory, and statutory provisions applicable to it." The committee reports periodically to the Depositors' Assembly and to the CMF upon request, contributing to transparency and the confidence of market participants.

The accountability system is complemented by formal reporting and public disclosure processes, which include the publication of annual reports, corporate governance reports, risk management reports, and audited financial statements, all of which are made available to the competent authorities and the public. These mechanisms allow stakeholders to make an informed assessment of the DCV's performance, soundness, and institutional transparency.

Disclosure of Good Governance Mechanisms

DCV's Articles of Incorporation, which govern the structure and key corporate governance arrangements, are published on the DCV website. In addition, the company discloses other governance arrangements through its Internal Regulations and circulars. All this information is public, except for the minutes of Board meetings, which are available only to depositors. The website includes "Corporate Governance" and "Corporate Information" sections, with details on the composition of the Board of Directors, internal committees, and senior management, as well as key governance procedures and decisions.

Key consideration 3: The roles and responsibilities of an FMI's board of directors (or equivalent) should be clearly specified, and there should be documented procedures for its functioning, including procedures to identify, address, and manage member conflicts of interest. The board should review both its overall performance and the performance of its individual board members regularly.

Functions and Responsibilities of the Board

The roles and responsibilities of the DCV are defined and formally established within a legal and regulatory framework that combines general provisions applicable to corporations with specific rules for securities deposit and custody firms. This framework consists of Law 18,046 on Corporations and Law 18,876 "on Securities Depository and Custody Companies," and is supplemented by the Bylaws, the Internal Regulations, and other internal policies and rules.

In accordance with Law 18,046, the Board of Directors is the body responsible for the

administration and senior management of the company (Article 40) and must act with the diligence and care required by applicable regulations (Article 44). Its responsibilities include defining and overseeing the company's strategy, supervising the General Manager's performance, approving the financial statements and annual report, convening and conducting shareholder meetings, and bearing joint and several liability for damages arising from legal or statutory violations or negligent management (Article 44). Likewise, the Board of Directors must ensure compliance with the applicable regulatory framework, the proper organization of the company, and the transparency of relevant information.

These general powers are supplemented by the specific provisions established in Law 18,876, pursuant to which a securities deposit and custody firm is responsible for ensuring the proper custody and accurate registration of deposited securities, as well as for ensuring the secure and efficient operation of its infrastructure. In this context, it is responsible for guaranteeing the protection of depositors' rights over their securities, maintaining adequate internal control and risk management systems, and ensuring the segregation of assets between the company's own securities and those of clients and participants. Likewise, the Board of Directors must ensure compliance with current regulations and the instructions issued by the Financial Market Commission, as well as the existence of duly approved operating procedures and internal regulations.

The Board's responsibilities are further developed and specified in the Articles of Incorporation and the DCV's Internal Regulations, which assign it ultimate responsibility for the entity's operational and financial stability, the secure functioning of its systems, and compliance with the applicable regulatory framework. The Bylaws also regulate the composition of the Board of Directors, the term of office, the possibility of reelection, quorums, and the rules for adopting resolutions, providing clarity regarding the exercise of governance functions and decision-making.

The DCV Board of Directors is composed of ten members elected by the Shareholders' Meeting, who serve for a two-year term, with the possibility of reelection. Within the governance structure, the General Manager reports directly to the Board of Directors and is responsible for the entity's day-to-day management. The Internal Audit Manager reports functionally and hierarchically to the Board of Directors, which ensures the independence of the internal audit function, in line with the PFMI's expectations regarding governance and internal control.

Documented Procedures and Conflicts of Interest

The Board's procedures are governed by the provisions of Law 18,046 on Corporations and the company's Articles of Incorporation. This framework regulates the composition of the Board of Directors, the method of election, the term of office, the calling and conduct of meetings, quorums for holding meetings and adopting resolutions, as well as the obligation to document deliberations and decisions through minutes.

The identification, handling, and management of conflicts of interest involving Board members are directly regulated by Law 18,046, which establishes directors' duty of loyalty, the obligation to abstain from participating in deliberations and votes in which they have a personal interest, and the requirement to record such abstention in the respective minutes. The applicable procedures are documented in current legislation and in the Bylaws. These procedures are reviewed through legal amendments or changes to the Bylaws as determined by the Shareholders' Meeting.

Board Committees

The DCV Board of Directors has committees that support and facilitate its operations, acting as advisory bodies on matters of audit, risk management and cybersecurity, technology and operational efficiency, people and sustainability, and customers and business development.

The Risk Management and Cybersecurity Committee is composed of directors and executives responsible for risk and cybersecurity functions, and is responsible for assisting the Board in overseeing DCV's comprehensive risk management framework. In particular, it supports the definition and review of risk management policies, monitors exposure to operational, technological, and cybersecurity risks, assesses the resilience and operational continuity of critical systems, and reports periodically to the Board on the risk profile and the mitigation measures adopted.

The Audit Committee, composed of directors and executives from the audit and control departments, assists the Board of Directors in overseeing the internal control system, internal and external audit functions, and the integrity of financial information. This committee reviews the financial statements, analyzes audit reports, evaluates the effectiveness of internal controls and risk management, proposes the appointment of the external auditor, and addresses matters related to related-party transactions, conflicts of interest, fraud, or irregularities, reporting to the Board of Directors in a timely manner.

The Information Technology and Operational Efficiency Committee is composed of directors and executives responsible for technology and operations, and its purpose is to assist the Board of Directors in defining and overseeing the DCV's technology and operational strategy. Its functions include analyzing and proposing the medium- and long-term technology vision, prioritizing relevant technology projects, overseeing operational efficiency initiatives, and evaluating investments in infrastructure and systems critical to the continuity, security, and efficiency of services.

The People and Sustainability Committee, composed of directors and executives from the organization, advises the Board of Directors on matters related to people management and sustainability. This committee analyzes and proposes policies on remuneration, compensation, and incentives; reviews matters related to organizational development, workplace climate, and succession for key positions; and supports the Board of Directors in defining general guidelines regarding sustainability and corporate responsibility.

The Clients and Business Development Committee is composed of directors and executives responsible for the commercial and services areas, and supports the Board of Directors on strategic matters related to the development of DCV's services and business. Its functions include analyzing and proposing new services, modifications to existing services, business development initiatives, and proposals for fee structures, taking into account client needs and the development of the securities market.

Performance Review

Periodically, the DCV administers a questionnaire designed to gauge the directors' own perceptions regarding the practices and structure of the DCV Board of Directors, based on industry best practices and the corporate governance questionnaire established by Chilean regulations for publicly traded corporations. The questionnaire covers both the Board's operational functioning and the performance and qualifications of its members.

Key consideration 4: The board should contain suitable members with the appropriate skills and incentives to fulfill its multiple roles. This typically requires the inclusion of non-executive board member(s).

Board Members

The DCV has established a clear separation between the roles of Board Chair and Chief Executive Officer (CEO), positions held by different individuals. The Board has no executive members and performs exclusively strategic management and oversight functions, while the day-to-day management of the entity falls to the executive management.

Representation on the Board is structured, in general terms, in a manner consistent with the ownership structure, such that the various types of participating institutions (e.g. banks, stock exchanges, and other market entities) appoint directors based on their collective stake in the DCV. The Board of Directors is composed of professionals with extensive experience in the Chilean capital markets, primarily in the sectors represented in the company's ownership. Furthermore, directors typically serve as senior executives (such as general managers or presidents) in entities belonging to those sectors. No member of the Board of Directors performs executive functions within the DCV.

DCV, in accordance with its bylaws, compensates its directors in a manner consistent with its role as a financial market infrastructure and with long-term orientation. Its compensation structure seeks to attract and retain professionals with experience and a proven track record in the capital markets, without incorporating variable incentives linked to short-term results that could affect decision-making independence. Directors receive compensation for serving in their positions and an additional stipend for their participation in Board committees.

Furthermore, serving as a director at the DCV entails significant professional recognition and direct involvement in matters critical to the functioning of the Chilean securities market, such as the custody and settlement of securities, the management of operational and technological risks, and interaction with regulatory and supervisory authorities, particularly the CMF and other competent entities. These non-monetary elements complement the compensation package and help attract senior-level candidates with a comprehensive and systemic view of the market.

The DCV's ownership structure does not grant any single shareholder individual control. The DCV is not subject to the obligation to appoint at least one independent director under the terms of Article 50 BIS of Law 18,046 (not elected by votes of the controlling shareholder). However, in practice, these legal requirements are met. None of the directors perform executive functions at DCV, and, furthermore, all meet independence criteria in terms of having no commercial or business relationships with DCV.

Given DCV's ownership structure and the incompatibility between the positions of manager and director, as provided for in Article 44 of Law 18,046, the status of independent director is fully defined and safeguarded by these legal provisions.

Key consideration 5: The roles and responsibilities of management should be clearly specified. An FMI's management should have the appropriate experience, a mix of skills, and the integrity necessary to discharge their responsibilities for the operation and risk management of the FMI.

Roles and Responsibilities of Senior Management

The functions and responsibilities of DCV's management are established in Law 18,046 on Corporations and are further detailed in the Articles of Incorporation and the company's internal regulations, which define the organizational structure, the powers of executive management, and the levels of delegation of authority.

Pursuant to Law 18,046, the General Manager is the company's chief executive and acts as the Board of Directors' agent, being responsible for executing its resolutions and for the day-to-day management of the company within the delegated powers, while the other managers and executives validly represent the company vis-à-vis third parties when acting within the powers conferred upon them, being subject to duties of diligence and loyalty and to liability for negligence or willful misconduct in the performance of their duties (Articles 49, 41, and 50). The Bylaws provide for the position of General Manager as the chief executive, responsible for the day-to-day management and representation of the company within the delegated powers .

The functions and objectives of DCV's senior management are formally established through the internal document "Mission, Description, and Functions by Management Unit," which formally sets forth the mission, responsibilities, and specific functions of each management unit. Senior management performance is evaluated through periodic monitoring of management, financial, and operational indicators, compliance with strategic and action plans, and accountability to government authorities. For these purposes, primarily but not exclusively, the DCV uses the Balanced Scorecard ("Corporate BSC"), which translates the vision and strategy into objectives and indicators from four strategic perspectives: Shareholders and Finance, Customers and Service Delivery, Organization, and Risk Management (see Principle 21).

Experience, Skills, and Integrity

Senior management performance is monitored through management and performance indicators, including key performance indicators (KPIs), financial results, system availability levels, and other metrics relevant to operations. Critical success factors and specific performance indicators have been defined for certain senior management positions. Performance evaluations for senior management and staff are conducted annually.

Regarding the removal of senior management, the Articles of Incorporation specify that the CEO may be removed by a vote of at least seven directors. There is a policy approved by the board of directors that establishes the internal guidelines for the process of terminating and replacing the CEO and senior executives of DCV.

Key consideration 6: The board should establish a clear, documented risk-management framework) that includes the FMI's risk-tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies. Governance arrangements should ensure that the risk-management and internal control functions have sufficient authority, independence, resources, and access to the board.

Risk Management Framework

The DCV's Risk Management Framework is established and approved by its Board of Directors and is formally defined in the Risk Management Policy as a guiding document, supplemented by the Manual and associated specific policies. The Board of Directors defines the general guidelines and the acceptable risk level, and periodically monitors the entity's risk profile.

To support this function, DCV has a Risk Management and Cybersecurity Committee, which serves as a specialized body supporting the Board of Directors. The Committee is responsible for reviewing exposure to various relevant risks, evaluating the effectiveness of controls, and monitoring mitigation plans. The Committee meets periodically and reports its conclusions and recommendations to the Board of Directors.

Risk management is structured according to a clearly defined three-line-of-defense model. The first line of defense consists of the operational areas and process owners, who are responsible for managing the risks inherent in their activities. The second line is exercised by the specialized risk function, which defines methodologies and evaluation criteria and monitors the proper application of the framework. The third line corresponds to Internal Audit, which independently evaluates the effectiveness of the risk management system.

The risk management process is carried out continuously and comprehensively, encompassing the identification, assessment, prioritization, treatment, and monitoring of operational, technological, cybersecurity, business continuity, legal, and compliance risks, ensuring management consistent with the DCV's role as financial market infrastructure and with current regulations.

The DCV's Risk Management Framework explicitly addresses the risk tolerance policy by defining principles, criteria, and acceptable risk levels, which are approved by the Board of Directors and formalized in the Risk Management Policy. This policy establishes the DCV's risk appetite and tolerance, as well as the thresholds that trigger mitigation, escalation, or review actions, ensuring consistency with the DCV's systemic role as financial market infrastructure.

The assignment of responsibilities and lines of accountability are structured according to a clearly defined model. The Board of Directors is responsible for approving the risk policy, tolerance levels, and general guidelines, and for overseeing compliance. The Risk and Cybersecurity Committee acts as a support body to the Board of Directors, periodically reviewing risk exposure, compliance with defined limits, and the effectiveness of mitigation measures, and reporting its findings to the Board.

The operational management of risks falls to executive management and process owners, who are responsible for identifying, assessing, and managing risks within approved limits. The specialized risk function defines methodologies, monitors compliance with tolerance levels, consolidates risk information, and issues alerts and reports to senior management, the committee, and the Board of Directors when significant deviations occur. Internal Audit provides an independent assessment

of the framework's functioning and the effectiveness of controls.

In crisis and emergency situations, the framework includes specific escalation and decision-making procedures, defined in the business continuity and incident management policies (see Principle 17).

The DCV Risk Management Framework is defined based on the identification and analysis of risks relevant to its role as financial market infrastructure and is documented in the Risk Management Policy and associated internal regulations. The specialized risk function develops and updates the framework in coordination with senior management and process owners. The proposal is reviewed by the Risk and Cybersecurity Committee, which assesses its consistency and submits recommendations to the Board of Directors. The Board of Directors endorses the framework by approving the policy, risk appetite and tolerance levels, and escalation criteria. The framework is reviewed periodically and in response to significant changes in the operational, regulatory, or technological environment.

Authority and Independence of Audit and Risk Management Functions

Risk management and the internal control system are central elements of the oversight exercised by the DCV Board of Directors, which is primarily channeled through the Risk and Cybersecurity Committee and the Audit Committee. The responsibility for coordinating comprehensive risk management—including operational, technological, cybersecurity, and regulatory compliance risks—lies with the Risk and Compliance Department, which establishes and oversees the criteria, policies, and procedures.

The Internal Audit Department independently evaluates the effectiveness of the internal control system and reports directly to the Board of Directors, which safeguards the autonomy of its function. Its responsibilities include developing and executing an annual risk-based audit plan, evaluating the effectiveness of implemented controls, and issuing independent opinions on operational and management processes.

The rest of the executive management supports the operational implementation of controls, policies, and incident recovery, ensuring that processes and systems remain consistent with the defined risk management framework and with the DCV's institutional mission. Additionally, the DCV undergoes annual independent operational audits aimed at validating the robustness of operational controls. Furthermore, in accordance with best corporate governance practices, the DCV has a Oversight Committee, composed of depositor representatives, which exercises complementary external oversight functions over the entity's management.

The DCV Board of Directors ensures proper governance in the adoption and use of risk management models through a formal framework of policies, methodologies, and controls, the application of which is subject to periodic oversight. The Internal Audit function continuously and independently evaluates the effectiveness of risk management policies, procedures, and models, including operational, technological, cybersecurity, and continuity risks, and reports directly to the Board of Directors.

The independent validation of models and methodologies is reinforced through periodic external audits and the maintenance of certifications under international standards. In particular, DCV holds ISAE 3402 attestation reports (or their equivalent, AT 320) and ISO/IEC 27001:2022 (Information Security Management System) and ISO 22301:2019 (Business Continuity Management System),

subject to certification and follow-up audits, which allow for the periodic evaluation of the design, consistency, and effectiveness of the controls and models used.

Key consideration 7: The board should ensure that the FMI's design, rules, overall strategy, and major decisions reflect appropriately the legitimate interests of its direct and indirect participants and other relevant stakeholders. Major decisions should be clearly disclosed to relevant stakeholders and, where there is a broad market impact, the public.

Identification and consideration of stakeholder interests

Ownership of the DCV is distributed among companies whose shareholders are the depositors themselves, grouped by capital market sectors. For example, a company controlled by the major national banks holds 30% of the capital and the same proportion of votes for the election of directors. A similar structure applies to the AFPs and life insurance companies. For their part, the Santiago Stock Exchange and the Chilean Electronic Stock Exchange—composed mainly of stockbrokers—also hold ownership stakes. Thus, representation on the Board of Directors is proportional to the intensity of use of DCV services, although this correspondence is informal in nature.

Annually, the DCV conducts a Customer Satisfaction Survey, in which the evaluation is structured around five main areas: overall service quality, system availability, response times, operational continuity, and service provided by the Customer Service Desk (MAC), the results of which are used to make adjustments to services, processes, and service levels. (see Principle 21). Additionally, management holds regular meetings with client users to evaluate service delivery, plan developments, and exchange perspectives on operational needs, which provides systematic feedback to the decision-making process.

With regard to its direct relationship with system users, the DCV holds an annual Depositors' Assembly, which represents depositors' interests in certain matters established by Law 18,876. Additionally, the DCV has established a technical forum for interaction called the Depositors' Committee, through which the DCV presents its initiatives and gathers depositors' opinions and concerns.

Disclosure

The resolutions of the General Shareholders' Meeting are made public through the DCV's website. Meanwhile, the Board of Directors' decisions are reported monthly to the CMF through the respective minutes. Furthermore, a report is presented to shareholders at the Annual General Meeting. Relevant institutional information is published on the Company's website, while other resolutions are communicated to participants via newsletters or circulars.

Principle 3: Framework for Comprehensive Management of Risks

An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.

Key consideration 1: An FMI should have risk-management policies, procedures, and systems that enable it to identify, measure, monitor, and manage the range of risks that arise in or are borne by the FMI. Risk-management frameworks should be subject to periodic review.

Risks that arise in or are borne by the FMI

Various types of risks are generated and assumed within the DCV, the most significant being operational risk, associated with technological system failures, human error, business continuity disruptions, cyberattacks, and deficiencies in internal processes or controls. Added to this is general business risk, linked to events that may affect its financial sustainability, as well as risks arising from third parties and interdependencies with other financial market infrastructures, and systemic risk, to the extent that a failure in its operations could simultaneously impact multiple participants and markets. In addition to these, the DCV faces legal risk arising from regulatory ambiguities and inconsistencies between the law, internal regulations, and contracts with participants. Furthermore, there is a risk related to the custody or safeguarding of assets, linked to the loss, misuse, or incorrect recording of financial assets under its administration.

Risk Management Policies, Procedures, and Systems

The regulatory framework for risk management at the DCV is established by the Risk Management Policy, supplemented by the Information Security and Cybersecurity Policy, the Business Continuity Policy, and CMF General Rules 509 and 510, in addition to the provisions of Law 18,876 and its implementing regulations. This framework is based on international standards such as ISO 31000 (risk management), ISO 22301:2019 (business continuity), and ISO 27001:2022 (information security).

Risk governance is structured under a three-line-of-defense model: the first line consists of those responsible for operational processes and areas, who identify and manage risks in their daily work; the second line consists of the Risk and Compliance Management team, which defines methodologies, oversees management, and reports to the Board of Directors; and the third line corresponds to Internal Audit, which independently evaluates the effectiveness of controls and the management framework.

The management process is executed through a continuous six-phase cycle, defined in the operating model and supported by the GRC Platform: understanding the environment (context analysis), risk identification, risk analysis, risk assessment, risk treatment, and monitoring and communication. This process ensures that each risk is managed systematically and in alignment with the limits defined in the Risk Appetite Framework (MAR) approved by the Board of Directors.

The supporting infrastructure consists of the Risk Management Policy as the guiding document, the Operational Risk Management Manual detailing the methodology, and the GRC Platform, which centralizes the recording, analysis, and reporting of risks, ensuring traceability.

Risk Management Systems

The risk management process is supported by the GRC Platform, a comprehensive Governance, Risk, and Compliance (GRC) management platform that centralizes the recording, analysis, and reporting of risks, and automates these activities at DCV.

The GRC Platform facilitates the consistent quantification and aggregation of risk exposures through unified metrics and models, all centralized in a single, accessible registry.

Review of Risk Management Policies, Procedures, and Systems

The process for developing, approving, and maintaining risk management policies, procedures, and systems at DCV is governed by the Risk Management Policy and the General Risk Management Guidelines. The Risk and Compliance Department develops policies through analysis of the context and operational needs, and by proposing methodologies aligned with the ISO 31000 standard. The proposals are reviewed by specialized committees and finally approved by the Board of Directors, which is responsible for risk management and the institutional risk appetite.

DCV evaluates the effectiveness of its risk management policies, procedures, and systems through a comprehensive framework that combines internal and external verification processes. The Risk and Compliance Department applies measurement and monitoring methodologies, generating periodic reports for the Board of Directors and specialized committees. For its part, the Internal Audit function, accredited by the Institute of Internal Auditors (IIA Global) in accordance with international professional standards, plays an independent role in evaluating the effectiveness of controls, the adequacy of policies, and the consistency of the risk management model, recommending improvements where appropriate.

This process is complemented by international standards and certifications. In particular, the ISAE 3402 standard (or its equivalent, AT 320) is applied, ensuring that equity fund managers have internal controls that are audited and certified regarding their design (Type I) and operational effectiveness (Type II). Likewise, the DCV maintains ISO 27001:2022 certifications in information security management and ISO 22301:2019 in business continuity management, renewed on a three-year cycle and subject to annual follow-up audits conducted by the *British Standards Institution* (BSI), an international certification body that guarantees the validity and global recognition of these certifications.

Additionally, the DCV supplements its internal assessments and certifications with specific external audits focused on risk areas and the expectations of relevant third parties. Notable among these are the periodic assessments of the SWIFT Customer Security Controls Framework (CSCF), conducted by independent auditors, which verify compliance with international cybersecurity standards applicable to financial messaging. Finally, the DCV regularly responds to due diligence and risk assessment questionnaires submitted by Depositors, which address matters of operational security, continuity, risk management, and internal control, thereby reinforcing transparency and confidence in its management model.

The DCV maintains a periodic review schedule for its risk management policies and systems that varies depending on the nature of each document. Some strategic policies, such as those related to education and training, are reviewed every three years; compliance policies, every two years; and operational policies, such as the engagement of international custodians, on an annual basis.

Key consideration 2: An FMI should provide incentives to participants and, where relevant, their customers to manage and contain the risks they pose to the FMI.

The DCV provides depositors with training on the systems it operates and promptly communicates any changes to those systems. Depositors have access to online information regarding the settlement process for transfer instructions submitted by depositors.

The DCV's Customer Service Desk (MAC) identifies operational deficiencies or errors by depositors and determines when there is a need to retrain a specific operator or develop additional training needs.

In accordance with the Internal Regulations, depositors must assume responsibility for the due care and proper use of user profiles and credentials. Furthermore, penalties are established for violations of any DCV internal regulations. Such penalties include written warnings, fines, suspension, or expulsion.

In accordance with the General Risk Management Guidelines, the DCV designs its policies and systems to effectively enable Depositors—and, where applicable, their clients—to manage and contain their risks. This design is based on operational procedures that incorporate robust internal controls, continuous monitoring methodologies, and technological platforms that ensure traceability and transparency.

Key consideration 3: An FMI should regularly review the material risks it bears from and poses to other entities (such as other FMIs, settlement banks, liquidity providers, and service providers) as a result of interdependencies and develop appropriate risk-management tools to address these risks.

Significant Risks

With regard to risks originating from other FMIs, the DCV may be exposed to operational and reputational risk in the provision of its securities custody, administration, and transfer services, to the extent that failures in interconnected entities affect the efficiency, continuity, or reliability of such services. In its role as a central securities depository (CSD), the DCV faces risks associated with the proper administration, registration, and transfer of securities, which may be impacted by external events. In particular, the gross securities settlement service that the DCV provides to Depositors in conjunction with Combanc, and which is interconnected with the LBTR System of the Central Bank of Chile (BCCh), could be affected by a failure in any of these FMIs, hindering the timely settlement of transactions.

Likewise, the DCV identifies, assesses, and manages significant risks arising from its connection to other critical entities, including Participants and providers of essential services, such as the SWIFT network, communications services, and power supply, among others. Specific controls, service level agreements, and continuity plans have been implemented for each of these dependencies, taking into account scenarios of partial or total unavailability.

Given its central role in the Chilean financial market infrastructure, the DCV transmits operational risks to other financial market infrastructures, particularly CCA, ComDer, and CCLV. CCA is exposed in its capacity as a low-value payment system, while ComDer and CCLV are exposed in their capacity as central counterparties, with CCLV additionally serving as a

securities settlement system. Likewise, the LBTR system of the Central Bank of Chile is exposed to these interdependencies. In the event of a significant disruption in the DCV's operations, these entities could see their ability to operate normally compromised. In particular, CCA, the LBTR, ComDer, and CCLV would be unable to properly execute collateral management processes, and CCLV would be prevented from transferring ownership of securities within the framework of its functions as a securities settlement system and as a central counterparty.

In accordance with the DCV's risk management model, the identification of risks and their associated factors is the responsibility of the owners of processes, sub-processes, assets, or other elements subject to evaluation, who receive methodological support and oversight from the Risk and Compliance Department and the Audit Department. To this end, processes are formally documented through flowcharts and narrative descriptions, and specific techniques are applied for the identification, assessment, and treatment of risks, in accordance with international standards and best practices. Those responsible must record, among other aspects, the name of the risk, its description, the owner, the current and expected frequency, the magnitude and impact on the business—both current and potential—as well as the corresponding mitigation or elimination measures.

Risk Management Tools

The DCV risk management model establishes the guidelines and processes according to which the risk management macro-process must be managed. The technological tool used in risk management is the GRC Platform.

In accordance with the General Guidelines for Operational Risk Management, DCV's senior management must ensure that a review of the risk management system is conducted at least once a year to guarantee its continuous improvement, compliance, and effectiveness. This review is documented through audits, self-assessments, compliance verification, incident monitoring, and risk matrices. According to the Risk Management Policy, the review frequency is annual, or whenever significant changes occur, in compliance with CMF General Rule 510. The Policy Approval and Update Policy establishes that regulatory policies must be reviewed annually, while secondary policies are reviewed biennially and primary policies every two or three years, unless regulatory or strategic changes require an extraordinary review. Under the Business Continuity Policy, the review is annual and is conducted at planned intervals or when significant changes occur within the organization, in line with ISO 22301:2019. Finally, the Information Security and Cybersecurity Policy also establishes an annual review frequency, taking into account regulatory updates, audits, penetration tests, and lessons learned from incidents.

Key consideration 4: An FMI should identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern and assess the effectiveness of a full range of options for recovery or orderly wind-down. An FMI should prepare appropriate plans for its recovery or orderly wind-down based on the results of that assessment. Where applicable, an FMI should also provide relevant authorities with the information needed for purposes of resolution planning.

Scenarios that may prevent an FMI from providing critical operations and services

Within the framework of its Risk Management Policy and the General Guidelines for Operational Risk Management, the DCV identifies risks that could prevent the execution of its critical activities and the provision of essential services. These scenarios stem from two main sources: the disruption of operational continuity due to operational incidents and the loss of financial sustainability resulting from general business risk.

With regard to the disruption of operational continuity due to operational incidents, the DCV has a Business Continuity Policy, which provides the framework for identifying risk scenarios that may affect the organization and minimizing the probability of failure of critical operations and services.

Regarding scenarios associated with the loss of financial sustainability resulting from general business risk, the DCV has established provisions in its General Business Risk Policy and General Business Loss Management Protocol with the objective of maintaining net liquid assets equivalent to, at a minimum, six months of operating expenses, while the Finance and Management Control Department conducts 12-month financial sensitivity analyses, the results of which are reported monthly to the Board committees.

Independent threats (fires, floods, earthquakes, fraud, social unrest) are identified as isolated events in Business Impact Risk Analysis (RIA) and Business Impact Analysis (BIA) exercises, which allow for assessing the effect on individual critical resources and defining recovery time objectives (RTO, RPO, MTPD). Related risks are modeled using combined or cascading scenarios, where the simultaneous loss of multiple critical resources (systems, communications, power, strategic suppliers) causes major disruptions. These scenarios are assessed in the GRC Platform and in the integrated risk matrices, incorporating operational and financial dependencies to prioritize scaled recovery plans. Additionally, the DCV conducts 12-month financial sensitivity exercises on the IOSCO Fund, assessing the impacts of cost increases or revenue decreases, ensuring that both independent and related risks are managed in an integrated and preventive manner.

Recovery or Orderly Wind-Down Plans

The DCV has defined recovery strategies for its critical units through its Business Continuity Plan (BCP), based on the Risk Management Policy, the General Guidelines for Operational Risk Management, the Business Continuity Management Policy, and the BIA.

Regarding financial recovery, the General Business Loss Management Protocol and the IOSCO Reserve Fund Procedure establish the framework for maintaining sufficient net liquid assets and raising additional capital if necessary.

Regarding orderly liquidation, the framework is governed by Law No. 18,876 (Articles 37 through 46), the DCV's Internal Regulations, and the General Business Risk Policy, which define the regularization, dissolution, and liquidation of securities depository companies.

Through its BCP, the DCV has defined recovery strategies for its critical business units within a defined timeframe, based on the BIA. The focus of this plan is the recovery from disruptions caused by the materialization of operational risks.

Regarding financial recovery, the General Business Loss Management Protocol, approved by the Board of Directors, establishes the procedure for raising additional capital in the event that net equity falls below the minimum legal capital requirement. This mechanism allows for the restoration of solvency and ensures the operational continuity of essential services (see Principle 15).

With regard to orderly liquidation, the framework is directly governed by Articles 37 through 46 of Law 18,876, which regulate the reorganization, dissolution, and liquidation of securities depository firms. In the event of a capital shortfall or failure to meet guarantees, the Board of Directors must notify the CMF and take steps to reorganize the firm; if these efforts are unsuccessful, dissolution is ordered. The shareholders' meeting approves the orderly liquidation, which is administered by the Oversight Committee for six months, ensuring a minimum level of service continuity. Finally, rules are established to liquidate assets, meet obligations, and protect depositors (see Principle 15).

The Finance and Management Control Department reviews and projects the IOSCO Fund on a monthly basis, reporting the results to the Audit Committee and the Risk and Cybersecurity Committee. General Management reports quarterly to the Board of Directors on the adequacy of the fund and recovery strategies. Finally, on an annual basis, the Business Continuity Plan (BCP), the General Business Loss Management Protocol, and the General Business Risk Policy are reviewed and updated, including recovery tests and validation of orderly liquidation plans.

Principle 10: Physical Deliveries

An FMI should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor, and manage the risks associated with such physical deliveries.

Key consideration 1: An FMI's rules should clearly state its obligations with respect to the delivery of physical instruments or commodities.

Rules of the CSD

The DCV accepts, under the physical delivery modality, primarily securities issued in physical form, such as shares, bonds, promissory notes, and other paper-based instruments. These documents may be physically deposited at the DCV's facilities, where they are securely held and subsequently recorded in the electronic account management system. In this way, the physical securities are linked to participants' accounts, enabling their management and eventual transfer. Physical delivery remains in effect for certain traditional instruments or those with specific legal requirements, such as Affiliate Recognition Bonds (BRAA), which must be held in physical form.

The DCV holds a small volume of physical securities belonging to its depositors, representing 0.9% of the total value of deposited securities. These securities consist mainly of certain corporate bonds and time deposits. CMF General Rule 77 establishes that depositors may request withdrawals and physical delivery of securities that have been issued in the event of an increase in DCV service fees or the implementation of new fee-based services whose use is mandatory for the depositor.

Responsibilities regarding the delivery of physical instruments are established in Law 18,876 and in CMF regulations. The procedure for withdrawing physical securities is defined in Section 10.9.1 of the Internal Regulations, and the DCV's responsibility is limited to delivering the security in physical form to the owner or their representative. The DCV maintains communication with its depositors through training sessions, circulars, and regular bulletins, in order to ensure that they have a clear understanding of their obligations and the procedures for effecting the physical delivery of securities.

The DCV ensures that its participants understand their obligations and the procedures for physical delivery by clearly defining them in the Internal Regulations, operating manuals, and participation agreements, acceptance of which is a requirement for trading. This framework is reinforced through ongoing communications and operational support. To date, there have been no significant disputes or claims associated with a lack of understanding of these procedures.

Key consideration 2: An FMI should identify, monitor, and manage the risks and costs associated with the storage and delivery of physical instruments or commodities.

The DCV identifies the risks and costs associated with the maintenance and delivery of physical instruments through due diligence processes, internal controls, and periodic reviews defined in Law 18,876, CMF regulations, and its Internal Regulations. These processes address vault custody, the traceability of securities, and daily balance reconciliation, which allows for the detection of inconsistencies and the assessment of operational and financial exposure.

Recognized risks include the loss, theft, or damage of physical documents, the possibility of legal

disputes over the ownership or validity of securities, and exposure to participant insolvency. Operational continuity risks are also identified, given that physical infrastructure is more vulnerable than electronic records and requires greater security controls.

The associated costs relate to the maintenance of vaults and security systems, insurance coverage, specialized personnel for document handling, and administrative processes for withdrawal and delivery. The IMF has noted that these costs are high compared to the marginal benefit of holding physical securities, which represent less than 1% of the total held in custody, reinforcing the trend toward dematerialization.

The DCV has a framework of specific processes and controls to monitor and manage the risks and costs associated with the storage and delivery of physical instruments. First, custody processes are regulated by Law 18,876 and the Internal Regulations, which establish the receipt, registration, and storage of physical securities in high-security vaults. These processes include the traceability of each instrument, periodic reconciliations, and complementary electronic records (such as digitization) to ensure the reconstitution of securities in the event of a contingency.

Second, risk management procedures are integrated into the institutional risk matrix, which identifies operational risks (loss, theft, deterioration), legal risks (ownership disputes), reputational risks, and business continuity risks. Section 10.2.6 of the Internal Regulations specifies the procedures and controls for monitoring these risks, while Section 10.9.1 governs the physical withdrawal of securities.

Additionally, the DCV performs daily automatic position reconciliations with participants and issuers; there is a separation of duties between the handling of physical securities and recordkeeping; restricted access to vaults and areas where physical securities are stored; and periodic inventory counts and reconciliation processes. Finally, the controls implemented include physical security systems against theft and fire, insurance policies to cover losses, personnel specialized in document handling, and internal and external audits. The DCV complements these controls with ongoing communication to its depositors through circulars, bulletins, and training sessions, ensuring they understand the obligations and procedures related to physical delivery.

The DCV monitors its participants' delivery preferences through the records and accounts it maintains in its system, where each depositor specifies whether the securities are to be managed electronically or require custody and eventual physical delivery. These preferences are monitored through daily reconciliations, internal controls, and periodic reviews that ensure the correspondence between registered securities and those actually held in custody.

To ensure that participants have the necessary resources and systems, the DCV establishes standardized procedures in its Internal Regulations (sections on custody and physical withdrawal), which include requirements for infrastructure, authorized personnel, and valid documentation to request delivery. Additionally, it maintains ongoing communication with depositors through circulars, bulletins, and training sessions, where the obligations and processes associated with physical delivery are explained.

Principle 11: Central Securities Depositories

A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimize and manage the risks associated with the safekeeping and transfer of securities. A CSD should maintain securities in an immobilized or dematerialized form for their transfer by book entry.

Key consideration 1: A CSD should have appropriate rules, procedures, and controls, including robust accounting practices, to safeguard the rights of securities issuers and holders, prevent the unauthorized creation or deletion of securities, and conduct periodic and at least daily reconciliation of securities issues it maintains.

The DCV operates an indirect securities account system pursuant to the provisions of Law 18,876, which in Article 2 defines depositors as only certain legal entities, such as the Treasury, the Central Bank of Chile, banks, securities issuers, stockbrokers, and institutional investors in general. This means that non-institutional investors cannot become depositors directly and must have their securities held in custody through an authorized legal entity, generally a securities intermediary or a bank, which acts as their representative vis-à-vis the DCV and maintains the custody relationship.

Safeguarding the Rights of Issuers and Security Holders

The protection of the rights of issuers and security holders is primarily regulated by Article 5 of Law 18,876, which establishes that in the relationship between the DCV and the depositor, the latter is the owner of the securities. Although the DCV is considered the owner vis-à-vis the issuer and third parties, the law clarifies that this does not mean that the depositor or its principal loses ownership of the securities or their voting and property rights. Article 12 reinforces this protection by expressly recognizing the voting rights of holders at shareholder meetings and bondholder assemblies, unless they decide to delegate such rights to the DCV. Likewise, Articles 13 and 14 regulate the issuance of registered and non-transferable certificates evidencing ownership of securities, which are enforceable under Article 14 bis, thereby providing holders with a legal tool to demand the enforcement of their rights.

In the case of custody agreements in which the DCV acts as a direct participant with Euroclear and the central depositories of Colombia and Peru, or in the agreement between the DCV and the global custodian Citibank, it is specified that all securities held under such agreements belong to the respective clients of the DCV. This principle ensures that ownership of the securities remains with the end investors, even when custody is held in international infrastructures.

The DCV performs periodic reconciliations between its internal records and issuers' listings, as well as with the global custodian Citibank, Euroclear, and the CSDs of Colombia and Peru. These reconciliation processes ensure that the balances recorded in its systems match the securities actually issued and held in custody, reducing the risk of accounting errors or duplicate entries. The DCV also has procedures in place to prevent and detect unauthorized deletions of records or book entries. The book-entry system regulated in Article 11 stipulates that any modification must be supported by valid and verifiable instructions from depositors. Internal compliance and audit controls, together with the oversight of the Oversight Committee regulated in Articles 30 through 33, enable the identification of irregularities and their reporting to the CMF. This ensures that there are no improper deletions or alterations that could affect the integrity of holders' property rights.

Article 4 of Law 18,876 requires the opening of individual accounts for each depositor, recording homogeneous securities and those subject to liens or precautionary measures separately, which ensures traceability and accuracy in accounting. Article 11 regulates the book-entry system, establishing that entries in the DCV's books constitute full proof of ownership. Articles 13 and 14 require the issuance of registered and non-transferable certificates attesting to the quantity, type, and issuer of the securities, and Article 14 bis grants them enforceable status, reinforcing accounting certainty and the legal protection of holders.

Protection against risks associated with other services is provided for in Article 17, which establishes that securities held in custody cannot be seized or affected by the DCV's own obligations, ensuring they remain separate from the company's assets and any risks arising from its business activities.

The DCV ensures robust accounting practices through the application of IFRS standards and annual external audits required by the CMF. These audits verify that the securities held in custody correspond to clients' rights and that there are no unauthorized deletions in the records. In addition, the Oversight Committee, regulated by Articles 30 through 33 of Law 18,876, periodically reviews the DCV's books and procedures and reports any irregularities to the CMF. Together, the annual external audits, internal reviews, and oversight by the Oversight Committee ensure that securities are properly accounted for and protected against operational risks or risks associated with other services.

Prevention of Unauthorized Creation or Deletion of Securities

The DCV has strict internal procedures for authorizing the creation and maturity of securities, ensuring that these transactions are carried out only with legal backing and under robust internal controls. For the creation of securities, the issuer is required to provide the DCV with a formal authorization, signed by authorized personnel of the issuer. Individuals with power of representation must be previously registered with the DCV, which allows for verification of the validity of signatures and the legitimacy of the instruction. This document is reviewed by the DCV's legal department, which confirms its compliance with current regulations and the issuer's bylaws. Only after successfully completing these steps can the issue amount be entered into the DCV system.

It is not possible to remove a security at will, as its removal from the system must strictly follow formal withdrawal procedures, maturity of the instrument, or cancellation due to the issuer's liquidation under current regulations. In accordance with the Internal Regulations, once dematerialized issues registered with the DCV have matured, the DCV proceeds to reduce the corresponding amounts from the Depositors' accounts and simultaneously reflect this in the corresponding registry for each of the matured dematerialized securities. The DCV maintains an auxiliary registry to keep track of dematerialized securities that have matured while they were on deposit.

Internal controls include the verification of signatures against the registry of authorized representatives, the mandatory legal review of each instruction, the segregation of duties between the operational and legal areas, and periodic internal audits that review the operations related to the creation and maturity of securities issues.

Periodic reconciliation of securities issues

With regard to equity issuances, including shares and investment fund units, Article 26 of Law 18,876 stipulates that the DCV must provide issuers with a daily list of depositors and the quantities of securities each one holds in custody. This mechanism constitutes a continuous cross-check between the DCV's records and those of the issuer or its issuing agent, ensuring that the total number of securities recorded in the account matches the number actually issued.

Regarding fixed-income issues, there are specific controls—some of which are daily—based on reports of the securities issued and registered with the DCV. Additionally, differentiated control mechanisms are applied depending on the type of issue, distinguishing between one-time issues and recurring issuance programs.

Consistency between the total number of securities registered in the DCV for a given issue and the number recorded in the issuer's own books is ensured through a set of internal controls. These include document verification prior to the creation of securities, validation of signatures of the issuer's authorized representatives, mandatory legal review of each instruction, appropriate segregation of duties between operational and legal areas, as well as internal and external audits aimed at verifying the integrity of the records.

In cases where the DCV does not act as the official registrar for the issues maintained in its books—a function performed through its subsidiary DCV Registros—and particularly in the case of recurring issues by banks and the BCCh, the DCV maintains comprehensive control over the issues. This control is consolidated daily at the close of business and reported to issuers, supplemented by periodic circularization processes. In the case of one-time issuances, such as corporate bonds, it is verified that the amounts deposited do not exceed those authorized by the CMF. It is worth noting that Article 26 of Law 18,876 requires the DCV to send daily to issuers of shares and investment fund units information on each depositor's holdings, which allows for continuous reconciliation.

Key consideration 2: A CSD should prohibit overdrafts and debit balances in securities accounts.

Overdrafts and Debit Balances

The DCV prevents overdrafts and debit balances in securities accounts through operational rules that ensure that any transfer can only be executed if there are sufficient securities in the depositor's account. The principle of sequential processing and the priority of securities ensure that account entries are made in a logical and sequential order, so that no transfer can precede the actual availability of the securities. Article I of the DCV's Internal Regulations expressly states that securities transfers may only be processed when the corresponding deposit account holds the necessary securities. This prevents the creation of negative balances or overdrafts in any type of transfer order.

Additionally, Article 28 of the law establishes that securities surpluses do not affect the continuity of operations. In the event of an unattributable or uncovered deficit, depositors may continue to trade with adjustments proportional to the loss. The depository must immediately report these situations and any recovery that allows for the full or partial restoration of positions.

Key consideration 3: A CSD should maintain securities in an immobilized or dematerialized form for their transfer by book entry. Where appropriate, a CSD should provide incentives to immobilize or dematerialize securities.

Immobilization or Dematerialization of Securities

The DCV holds the vast majority of securities in dematerialized form. As of the evaluation date, 99.1% of the total value in pesos of deposited securities is dematerialized, while the remainder remains in physical form. In operational terms, approximately 99% of the total transaction volume involves dematerialized securities, reflecting the predominance of this format in the market. For securities still held in physical form, the Internal Regulations (Article 7.2.2) provide for the possibility of immobilizing them, allowing their holding and transfer through the book-entry system. Additionally, the DCV charges higher fees for the deposit of physical securities, which serves as an incentive for immobilization and dematerialization, reinforcing the trend toward a safer and more efficient system.

When securities are issued in the form of physical certificates, the DCV may immobilize them and allow their maintenance and transfer through the book-entry system, in accordance with Article 7.2.2 of its Internal Regulations. This means that, although the physical security continues to exist, its circulation and transfer are carried out exclusively through electronic records at the DCV. 99.1% of the total value in pesos of the securities held in the DCV is dematerialized. The remainder consists of physical securities, a portion of which is immobilized and traded through book-entry transactions. Approximately 99% of the total transaction volume involves dematerialized securities, while the percentage of transactions involving immobilized securities is marginal.

The higher fees applicable to the deposit of physical securities provide an incentive for issuers and depositors to opt for immobilization and, ultimately, for complete dematerialization. Furthermore, by opting for the immobilization and dematerialization of securities, depositors can trade with

greater efficiency, security, and speed, avoiding the physical handling of certificates and facilitating electronic transfer through book entries.

Key consideration 4: A CSD should protect assets against custody risk through appropriate rules and procedures consistent with its legal framework.

Protection of assets against custody risk

Article 27 of Law 18,876 establishes the DCV's liability for custody risk, including negligence, fraud, misappropriation of assets, mismanagement, and inadequate records. In turn, the Internal Regulations (Art. 2.2.1) provide for specific measures to protect the authenticity and integrity of securities held in custody and safeguard depositors' interests. These mechanisms are complemented by internal controls, segregation of duties, periodic audits, and oversight by the CMF and the Oversight Committee. Additionally, the DCV maintains insurance policies covering misappropriation, destruction, and theft of securities, with a limit of up to 0.1% of the total amount on deposit.

The DCV has determined that its rules and procedures are consistent with the legal framework because all provisions of its Internal Regulations are drafted in accordance with Law 18,876 and require prior approval by the CMF. Each amendment is reviewed by the DCV's legal department and authorized by the CMF before taking effect, ensuring its regulatory validity. In addition, the application of these rules is subject to continuous supervision by the CMF and the Oversight Committee (Articles 30 to 33 of Law 18,876), along with annual external audits that verify their consistency.

The DCV supplements asset protection with additional mechanisms such as asset segregation, which keeps depositors' funds separate from the DCV's own assets; secure technological infrastructure with redundant systems and daily backups; and access controls with full traceability, which prevent tampering or misuse. It also has business continuity and disaster recovery plans, as well as internal and external audits that verify the effectiveness of controls. Together, these measures strengthen protection against embezzlement, destruction, or theft and reinforce participants' confidence in the system.

Key consideration 5: A CSD should employ a robust system that ensures segregation between the CSD's own assets and the securities of its participants and segregation among the securities of participants. Where supported by the legal framework, the CSD should also support operationally the segregation of securities belonging to a participant's customers on the participant's books and facilitate the transfer of customer holdings.

Mechanisms for Segregation of Assets

The DCV has segregation mechanisms that ensure a clear separation between its own assets and participants' securities, as well as between the securities of different clients. First, Article 19 of Law 18,876 authorizes the DCV to hold its own securities, but requires that these be identified separately in its accounting system to distinguish them from depositors' assets. In practice, the DCV does not hold any significant proprietary securities in custody, which reinforces its exclusive role as a custodian of third-party securities.

Regarding the segregation between depositors and their clients, the DCV allows for the existence of separate accounts that are used at the discretion of the depositors in accordance with

applicable regulations or their custody practices. Depositors maintain a Proprietary Securities Account and, additionally, Third-Party Securities Accounts, which can be of two types: omnibus or group client accounts, which group the securities of multiple clients under a single account; and individual client accounts, which separately reflect the securities of each of the depositor's clients.

On the other hand, Article 179 of Law 18,045 requires brokerage firms to maintain separate omnibus accounts and to offer custody in individual accounts as an option for their clients. In the case of banks and other financial institutions acting as depositories, the use of segregated accounts is optional, although common in practice. Currently, the DCV does not hold securities on its own account.

The DCV promotes the operational segregation of securities belonging to its participants' clients through a system of differentiated accounts managed directly on its central platform. This ensures that clients' securities are not recorded in the participants' own books, but rather in accounts maintained at the DCV, thereby avoiding any risk of commingling of assets and ensuring transparency and traceability.

To do so, depositors must maintain a Proprietary Securities Account, intended exclusively for their own holdings, and may also open Client Securities Accounts for the custody of third-party assets. The latter are divided into two types: the Group Client Account (an omnibus account), which groups the securities of multiple clients under a single account, and the Individual Client Account, which allows the securities of each client to be recorded separately. This framework, supported by Law 18,045 and Law 18,876, ensures that client assets are clearly distinguished from both the participant's assets and those of the DCV itself.

Regarding transfers from client accounts to another depositor, once instructions have been entered by the respective participants, the DCV validates the availability of the securities in the seller's client account and proceeds to execute the electronic transfer to the buyer's client account.

Key consideration 6: A CSD should identify, measure, monitor, and manage its risks from other activities that it may perform; additional tools may be necessary in order to address these risks.

Other Activities of the FMI

The DCV offers services complementary to its custody and settlement services, which are provided both directly and through its subsidiary DCV Asesorías y Servicios S.A., established in 2020 to develop new services and assume some that were previously offered by the DCV itself.

Among the DCV's direct services are the issuance and administration of securities, including the registration of instruments in the local market and support for digital issuance processes; the management of corporate events, such as dividend payments and corporate or debt restructuring processes; and the administration of collateral and judicial measures, through the management of special pledges and the Electronic Pledge Registry (REP), in addition to the custody of securities subject to judicial measures. Likewise, the DCV provides international custody services, facilitating the settlement of foreign securities and participating in the Latin American Integrated Market (MILA).

The DCV also administers financial derivatives, such as forward contracts and other instruments, and offers tax services, including the issuance of certificates and annexes, as well as the

management of tax returns in its capacity as a tax agent. Through DCV Registros, it provides services for the administration of shareholder and fund contributor registries, the organization of shareholder meetings and contributor assemblies, and the management of information and certifications for issuers and investors. Finally, through DCV Digital, a platform based on Nasdaq technology and distributed ledger technology, it drives innovation in the issuance and custody of digital financial instruments.

For its part, DCV Asesorías y Servicios S.A. offers specialized services such as the DTCC Transaction Comparison Service, which allows for the validation of transactions with foreign investors; the preparation of Statistical Reports to provide information to the market; the Administration of Active Affiliate Recognition Bonds (BRAA), which adds value to the management of these instruments; and the role of Tax Agent, representing foreign investors for tax purposes. Additionally, DCV directly maintains the forward contract registration service for institutional investors.

The risks identified for the DCV's additional activities are essentially operational risks, arising from the administration of registries, corporate events, tax services, international custody, and other processes that require continuity and precision. These risks are managed as part of the DCV's operational risk management policy, in accordance with the requirements of General Rule 510 on Operational Risk Management from 2024, and General Rule 509 on corporate governance and comprehensive risk management.

Principle 13: Participant-Default Rules and Procedures

An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

Principle 13 does not apply to DCV, as it operates exclusively as a central securities depository, acting solely on the basis of instructions received. Consequently, it assumes no liability for any defaults arising from delays or failures in the delivery of securities or funds associated with settlement. The DCV participates in the DVP gross settlement process, which is carried out in coordination with Combanc. However, in Chile there is no single operator responsible for this process (see Section III).

Principle 15: General business risk

An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialize. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

Key consideration 1: An FMI should have robust management and control systems to identify, monitor, and manage general business risks, including losses from poor execution of business strategy, negative cash flows, or unexpected and excessively large operating expenses.

Management of General Business Risks

DCV has established a General Business Risk Policy that defines the framework for managing this type of risk at the corporate level. Primary responsibility lies with Risk and Compliance Management, with support from Finance and Management Control, ensuring cross-functional coordination in identifying and addressing risks that may affect business continuity.

In addition, the General Business Loss Management Protocol details the processes and activities necessary for the proper management, governance, and monitoring of these risks. This protocol ensures that control and mitigation measures are applied in a systematic and documented manner, guaranteeing traceability and effectiveness in management.

In this context, the DCV has developed a general business risk model that includes the identification of risk factors, the assignment of specific controls, and the documentation of each scenario. This model is based on the identification of two major sources of risk: one-off scenarios, which correspond to unexpected events requiring immediate liquidity for mitigation, such as internal or external fraud and failures in strategy execution; and structural scenarios, which refer to situations that generate a permanent increase in costs or a significant decrease in revenue, with a significant impact when they reach 20% of the EBITDA/Sales ratio.

To manage these risks, DCV uses a risk matrix that assigns probabilities to each scenario and establishes the corresponding controls. This tool allows the institution to anticipate potential

losses and define timely mitigation actions, thereby strengthening its operational and financial resilience.

The DCV continuously manages its general business risks as part of its comprehensive risk management framework, led by Risk and Compliance Management together with Finance and Management Control. The General Business Risk Policy and the General Business Loss Management Protocol establish processes for identification, control, and ongoing monitoring, ensuring traceability and consistency. The assessment explicitly incorporates the effects on cash flows, given that certain events may require immediate resources, and on capital, considering that DCV is a private entity that must safeguard its solvency.

Key consideration 2: An FMI should hold liquid net assets funded by equity (such as common stock, disclosed reserves, or other retained earnings) so that it can continue operations and services as a going concern if it incurs general business losses. The amount of liquid net assets funded by equity an FMI should hold should be determined by its general business risk profile and the length of time required to achieve a recovery or orderly wind-down, as appropriate, of its critical operations and services if such action is taken.

Net Liquid Assets

As of December 31, 2025, DCV maintains net liquid assets within its equity intended to cover general business losses, in accordance with the provisions of its General Business Loss Management Protocol. This protocol requires maintaining a specific fund equivalent to six months of operations, calculated as the difference between current assets and current liabilities and projected over twelve months with sensitivity analyses for scenarios of increased costs and decreased revenue, in order to ensure that liquid assets never fall below the defined minimum.

As of the same date, the amount of total net liquid assets, defined in accordance with the procedure established in the General Business Loss Management Protocol, amounted to approximately $14.5 million, equivalent to 8.3 months of operating expenses. As of the same date, the minimum required total net liquid assets (6 months of operations) amounted to approximately $10.5 million.

The DCV calculates the amount of net liquid assets in its net equity in accordance with the General Business Loss Management Protocol. The procedure consists of determining the difference between current assets and liabilities, projecting net liquid assets over a 12-month horizon. Sensitivity analyses are applied to this projection, considering scenarios of increased costs, decreased revenue, or both combined, with the aim of ensuring that liquid assets never fall below the defined minimum, equivalent to six months of operations. This forward-looking approach allows for the proactive assessment of the resources needed to address general business losses.

The time required and the operating costs for an orderly recovery or liquidation are determined based on that same six-month operating standard. The calculation is based on the institution’s average operating expenses, so the general business loss fund must cover at least that period. The methodology considers six months to be the prudent timeframe for implementing recovery, restructuring, or, in extreme cases, an orderly liquidation of essential activities and services, ensuring operational continuity while contingency plans are executed.

Key consideration 3: An FMI should maintain a viable recovery or orderly wind-down plan and should hold sufficient liquid net assets funded by equity to implement this plan. At a minimum, an FMI should hold liquid net assets funded by equity equal to at least six months of current operating expenses. These assets are in addition to resources held to cover participant defaults or other risks covered under the financial resources principles. However, equity held under international risk- based capital standards can be included where relevant and appropriate to avoid duplicate capital requirements.

Recovery or Orderly Wind-Down Plan

Regarding financial recovery, the General Business Loss Management Protocol, approved by the Board of Directors, establishes the procedure for raising additional capital in the event that net equity falls below the required minimum statutory capital. This mechanism allows for the restoration of solvency and ensures the operational continuity of essential services.

Regarding orderly liquidation, the framework is directly regulated by Articles 37 through 46 of Law 18,876, which establish the provisions applicable to the regularization, dissolution, and liquidation of securities depository firms. In the event of a capital shortfall or failure to meet guarantees, the board of directors must notify the CMF and adopt regularization measures; if these are unsuccessful, dissolution is ordered. The shareholders' meeting approves the orderly liquidation, which is administered by the Oversight Committee for six months, ensuring minimal continuity of services. Finally, rules are established for liquidating assets, covering obligations, and protecting depositors.

Resources

The DCV maintains sufficient liquid assets in its net worth to implement the General Business Loss Management Protocol and the General Business Loss Fund Procedure, which stipulate that the fund's amount must be equivalent, at a minimum, to the resources necessary to cover six months of operations. This calculation is performed in accordance with the IOSCO Reserve Fund, which requires that net liquid assets be projected over a twelve-month period and subjected to sensitivity analyses for scenarios involving increased costs, decreased revenues, or both combined, in order to ensure that they never fall below the defined standard.

The adequacy of these resources is determined by comparing the level of net liquid assets with the institution's current operating expenses. If the amount exceeds the six-month threshold, coverage is considered adequate to sustain the continuity of essential services in the event of general business losses. At the end of each fiscal year, the DCV verifies that available liquid assets exceed the required minimum, which guarantees an additional safety margin against adverse scenarios and confirms the capacity for recovery or, in extreme cases, orderly liquidation.

The DCV does not maintain associated resources to cover participant defaults or other financial risks, as the DCV acts solely as a central securities depository, whose primary function is the custody, administration, and registration of securities, and not as an administrator of securities settlement systems.

Key consideration 4: Assets held to cover general business risk should be of high quality and sufficiently liquid in order to allow the FMI to meet its current and projected operating expenses under a range of scenarios, including in adverse market conditions.

Composition of Net Liquid Assets

The DCV's net liquid assets are defined in the current Policy on the Investment of Own Resources in Financial Instruments, which stipulates that such resources must be concentrated in low-risk, highly liquid fixed-income instruments, such as time deposits and sovereign or bank debt securities with high credit ratings (see Principle 16). The management of these assets is entrusted to an external entity designated as the "Portfolio Management Company", which must be a bank or a banking subsidiary, in accordance with the provisions of the DCV's Policy on the Investment of Own Resources in Financial Instruments.

The composition of these assets allows them to be converted into cash quickly and efficiently, if necessary, with minimal or no loss of value even under adverse market conditions, given their high liquidity and low credit risk. This framework is complemented by the provisions of the General Business Loss Management Protocol and the General Loss Fund Procedure, which require maintaining net liquid assets equivalent to at least six months of operating expenses.

The DCV periodically assesses the quality and liquidity of the net liquid assets in its equity in accordance with the provisions of the Policy on the Investment of Own Resources in Financial Instruments and the General Business Loss Management Protocol. The Policy on Investment of Own Resources in Financial Instruments stipulates that resources must be concentrated in low-risk, highly liquid fixed-income instruments, and, in accordance with the provisions of said policy, their management and periodic assessment of quality and liquidity is the responsibility of an external entity designated as a Portfolio Management Company.

Key consideration 5: An FMI should maintain a viable plan for raising additional equity should its equity fall close to or below the amount needed. This plan should be approved by the board of directors and updated regularly.

Additional Capital

DCV has a formal procedure for raising additional capital, which replicates the provisions of Articles 36 and 37 of Law 18,876, which set a minimum legal equity requirement of UF 30,000 (approximately USD 1.1 million). This procedure stipulates that if, 30 business days after the detection of an equity deficit, the deficit has not been resolved, the board of directors must call an extraordinary shareholders' meeting to approve a capital increase, which must be held within the following 60 business days. If the increase is approved, it must be paid in within a maximum of 30 business days from the date of the resolution. If the capital increase is not achieved within that period, the CMF will revoke the DCV's operating authorization, initiating the orderly liquidation procedure regulated in Articles 41 through 46 of the same law.

The plan also provides for the responsibility of the Finance and Management Control Department to monitor and periodically report on compliance with the minimum legal capital requirement, ensuring early detection of any deviation. Finally, given the DCV's ownership structure, where depositors are also shareholders, there is a strong incentive for them to contribute additional capital, considering the DCV's essential role in the continuity of their own businesses.

In practice, the review of the formal procedure for raising additional capital is conducted as part of regular corporate governance processes, which means that the Board of Directors must verify its validity and adequacy at least once a year, or more frequently if there are significant changes in the financial situation, applicable regulations, or market conditions.

Principle 16: Custody and Investment Risks

An FMI should safeguard its own and its participants' assets and minimize the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

Key consideration 1: An FMI should hold its own and its participants' assets at supervised and regulated entities that have robust accounting practices, safekeeping procedures, and internal controls that fully protect these assets.

Secure Custody of Assets

The DCV does not hold collateral on behalf of its participants and, in accordance with its Policy on the Investment of Own Resources in Financial Instruments, manages its liquid resources through a Portfolio Management Company (SAC), which must necessarily be a bank or banking subsidiary subject to regulation and supervision by the Financial Market Commission. The selection of the SAC is based on criteria of solvency, capital adequacy, regulatory compliance, and experience in managing low-risk, highly liquid fixed-income portfolios, ensuring that the resources are protected under prudential standards. Additionally, aspects of corporate governance, internal controls, and the ability to provide periodic reports are considered, allowing the DCV to continuously monitor the composition, quality, and liquidity of the managed assets. Compliance with these criteria is monitored through periodic performance reviews, contractual and operational monitoring, and regular reports to the Finance and Management Control Department, ensuring traceability, transparency, and immediate availability of funds.

Verification that these entities have robust accounting practices, secure custody procedures, and adequate internal controls is carried out through regulatory supervision by the CMF, contractual and operational review of the relationship with the SAC, and ongoing monitoring by the Finance and Management Control Department.

Key consideration 2: An FMI should have prompt access to its assets and the assets provided by participants, when required.

Solid Legal Foundation

The legal strength of depositors' rights in Chilean banks rests on three central pillars. First, the legal framework established in the General Banking Law (DFL 3 of 1997), which recognizes deposits as enforceable contractual obligations, in which the depositor holds the status of a creditor entitled to the return of their funds, along with the corresponding interest. Second, the dual supervision and regulation exercised by the CMF and the BCCh, aimed at safeguarding the stability of the financial system. Finally, preferential protection, which grants deposits legal priority over other creditors in the event of bank liquidation, further ensuring their immediate contractual enforceability, backed by Chilean civil and commercial law.

Regarding financial instruments held in the DCV, depositors have three fundamental protection mechanisms at their disposal. Asset segregation ensures that deposited securities are kept separate from the DCV's assets and cannot be subject to claims by its creditors in the event of financial difficulties. Added to this is the regulatory oversight of the CMF, which continuously monitors compliance with the rules applicable to the custody and protection of assets.

Quick access to assets

The DCV's assets are invested exclusively in Chile. Cash and cash equivalents are kept permanently available in electronic form, allowing for immediate access to liquidity.

Key consideration 3: An FMI should evaluate and understand its exposures to its custodian banks, taking into account the full scope of its relationships with each.

DCV assesses and manages its exposures to custodian banks by taking a comprehensive view of the scope of its financial and operational relationships. It maintains checking accounts at various banks and has engaged a limited number of banks as managers of surplus funds, all of which have a credit rating of A+ or higher and recognized experience in managing investment portfolios, in accordance with the provisions of the Policy on the Investment of Own Funds in Financial Instruments.

Key consideration 4: An FMI's investment strategy should be consistent with its overall risk-management strategy and fully disclosed to its participants, and investments should be secured by, or be claims on, high-quality obligors. These investments should allow for quick liquidation with little, if any, adverse price effect.

Investment Strategy

DCV ensures consistency between its investment strategy and its overall risk management strategy through the Policy on Investment of Own Funds in Financial Instruments, approved by the board of directors and reviewed annually, which operationalizes the institutional risk appetite defined as conservative in terms of liquidity, credit, and market risk.

The Policy on Investment of Own Resources in Financial Instruments restricts investments to highly liquid, low-volatility fixed-income instruments (time deposits, sovereign or bank debt, shares in fixed-income mutual funds), requires a minimum rating of BBB+, as well as duration and diversification criteria; these parameters are calibrated to maintain the coverage capacity of at least six months of operations required by the general business loss management protocol.

It also incorporates maximum limits on investments in securities or issuers rated A-/AA (30%) and BBB+ (15%). Other limits are established based on the size of the liquid funds the company has available for financial investments. These limits pertain to the type of instrument, its duration, and diversification.

Risk Characteristics of Investments

The DCV establishes concentration limits to mitigate the credit risk associated with a single issuer. Specifically, the policy stipulates that maximum exposure may not exceed 30% for instruments issued by entities rated A-/AA and 15% for instruments issued by entities rated BBB+.

The DCV ensures the rapid liquidation of its investments by prioritizing highly liquid, low-risk

instruments, such as short-term registered time deposits, shares in open-end mutual funds with a duration not exceeding 90 days, and securities issued by the Central Bank of Chile and the General Treasury of the Republic, all of which have deep secondary markets that allow for their timely sale or redemption. The investment policy further stipulates that the average duration of the portfolio must be maintained between 1.5 and 3 years, favoring short-term instruments that reduce sensitivity to interest rate fluctuations and facilitate liquidation without significant losses. Additionally, the fund is required to maintain a minimum available balance of at least 20,000 UF in bank accounts or easily liquidated instruments.

Principle 17: Operational Risk

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfillment of the FMI's obligations, including in the event of a wide-scale or major disruption.

Key consideration 1: An FMI should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.

Identification of Operational Risk

The DCV uses the Risk Management Policy as its guiding framework, supplemented by the Business Continuity Policy, the Information Security and Cybersecurity Policy, and the General Guidelines for Operational Risk Management, all in compliance with Law 18,876, its regulations, and CMF General Standards 509 and 510. This framework is based on international standards such as ISO 31000 (risk management), ISO 22301:2019 (business continuity), and ISO 27001:2022 (information security).

The identification of plausible sources of operational risk is carried out through a continuous six-phase cycle: context analysis, identification, analysis, assessment, treatment, and monitoring, supported by the GRC Platform, which centralizes risk recording and analysis. The DCV's processes identify internal risks linked to system failures, human error, control deficiencies, and cyberattacks; risks arising from participants, such as operational errors or non-compliance; and external risks, such as failures in critical suppliers, interdependencies with other FMIs (CCA, CCLV, ComDer, LBTR System), as well as environmental events such as natural disasters.

The DCV, as an FMI, has identified various sources of operational risk that may affect its critical operations. These include failures in technological systems, human errors in process execution, business continuity disruptions, cyberattacks, and deficiencies in internal controls. Risks arising from third parties are also considered, such as strategic providers of communications, energy, or technology services, as well as risks associated with interdependencies with other financial market infrastructures, such as CCA, CCLV, ComDer, and the LBTR system of the Central Bank of Chile (BCCh).

Regarding specific elements that could cause failures, the DCV has identified the possibility of loss

or misuse of assets in custody, incorrect records in securities administration systems, regulatory ambiguities that create legal risk, failures in the SWIFT network, unavailability of critical energy or telecommunications services, and external events such as natural disasters or social unrest that could disrupt operations. These elements are managed through risk policies, continuity plans, periodic testing, and internal controls aligned with international standards such as ISO 31000, ISO 22301:2019, and ISO 27001:2022.

Management of Operational Risk

DCV monitors and manages identified operational risks through a continuous six-phase cycle (context analysis, identification, analysis, assessment, treatment, and monitoring), supported by the GRC Platform, which centralizes the recording, analysis, and reporting of risks, ensuring traceability and aggregation of exposures. In addition, continuous monitoring methodologies, continuity testing, and internal and external audits are applied, aligned with international standards such as ISO 31000 and ISO 22301:2019.

These systems, policies, procedures, and controls are documented in the Risk Management Policy, the Business Continuity Policy, the Information Security and Cybersecurity Policy, the Operational Risk Management Manual, the General Risk Management Guidelines, and in CMF regulations (General Standards 509 and 510), in addition to external certifications such as ISAE 3402 (or its equivalent AT 320), and various ISO standards.

Policies, Processes, and Controls

DCV ensures the timely implementation of its procedures through a comprehensive risk management framework based on the Risk Management Policy, the Business Continuity Policy, the Information Security and Cybersecurity Policy, and the General Operational Risk Management Guidelines. These documents establish clear methodologies for the identification, assessment, treatment, and monitoring of risks, and are complemented by robust internal controls, standardized operating procedures, and technological platforms such as the GRC Platform, which centralizes the recording and tracking of risks, ensuring traceability and the timely implementation of defined measures.

The implementation of these policies and processes is organized under a three-lines-of-defense model, where operational managers manage risks in their daily work, the Risk and Compliance Department supervises and reports to the Board of Directors, and Internal Audit independently evaluates the effectiveness of controls.

Regarding the incorporation of international, national, and sector-specific standards, DCV aligns its management with Law 18,876, CMF General Rules 509 and 510, and international standards such as ISO 31000 (risk management), ISO 22301:2019 (business continuity), and ISO 27001:2022 (information security). Additionally, it complements this framework with external certifications such as ISAE 3402 and specific assessments such as the SWIFT CSCF.

With regard to human resources, the DCV Human Resources Policy covers topics such as staff selection criteria, initial and ongoing staff training, and promotion, to ensure that employees are satisfied with their overall professional development, with the aim of reducing staff turnover. Both individual performance and teamwork are evaluated. All applicants must pass screening tests and background checks. The Policy also emphasizes avoiding conflicts of interest and situations that could lead to weak controls or potential fraud.

Regarding change management, when the DCV is implementing software changes, updates, code improvements, and/or bug fixes, specific procedures are followed to ensure that no service interruptions occur as a result of the changes made. Procedures based on international standards and formalized in policies, such as the Software Development Policy, guide the development and renewal of systems and the risk assessment for new technology projects.

Key consideration 2: An FMI's board of directors should clearly define the roles and responsibilities for addressing operational risk and should endorse the FMI's operational risk-management framework. Systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes.

Functions, Responsibilities, and Framework

The regulatory framework for risk management at DCV is established by the Risk Management Policy, supplemented by the Information Security and Cybersecurity Policy, the Business Continuity Policy, and CMF General Rules 509 and 510, in addition to the provisions of Law 18,876 and its implementing regulations. This framework is based on international standards such as ISO 31000 (risk management), ISO 22301:2019 (business continuity), and ISO 27001:2022 (information security).

Risk governance is structured under a three-line-of-defense model: the first line consists of those responsible for operational processes and areas, who identify and manage risks in their daily work; the second line consists of the Risk and Compliance Management team, which defines methodologies, oversees management, and reports to the Board of Directors; and the third line corresponds to Internal Audit, which independently evaluates the effectiveness of controls and the management framework.

The management process is executed through a continuous six-phase cycle, defined in the operating model and supported by the GRC Platform: understanding the environment (context analysis), risk identification, risk analysis, risk assessment, risk treatment, and monitoring and communication. This process ensures that each risk is managed systematically and in alignment with the limits defined in the Risk Appetite Framework (MAR) approved by the Board of Directors.

The supporting infrastructure consists of the Risk Management Policy as the guiding document, the Operational Risk Management Model that details the methodology, and the GRC Platform, which centralizes the recording, analysis, and reporting of risks, ensuring traceability.

Risk management and internal control occupy a central place in the work of the DCV Board of Directors, which explicitly supports the operational risk management framework through two specialized bodies: the Risk and Cybersecurity Committee and the Audit Committee. The Risk and Compliance Department has overall responsibility for risk management and regulatory compliance, while the Internal Audit Department reports directly to the Board on the effectiveness of controls.

The Board reviews and endorses the operational risk management framework on a quarterly basis through periodic reports and annually through the approval and updating of strategic policies, in compliance with CMF General Rule 510 and international standards such as ISO 31000 and ISO 22301:2019.

Review, Audit, and Verification

DCV reviews, audits, and verifies its systems, policies, procedures, and controls—including

operational risk management mechanisms—through a comprehensive framework that combines internal and external verification processes. The Risk and Compliance Department applies continuous measurement and monitoring methodologies, generating periodic reports for the Board of Directors and specialized committees. The Internal Audit Department, accredited in accordance with international standards (IIA Global), is responsible for internal audit processes, the scope of which includes the availability and reliability of information regarding risk management and compliance with organizational processes, procedures, and practices. In addition, it proposes corrective and preventive action plans from the perspective of efficiency, the proper use of resources, fraud prevention, and compliance with the current regulatory framework.

The internal audit team reviews critical processes and procedures and monitors risks in key areas at least once every six months, while non-critical processes are reviewed every two years.

The frequency of these reviews and verifications is quarterly for reports to the Board of Directors, annual for the updating of strategic policies and continuity plans, and monthly for the supervision of the IOSCO Fund and financial literacy initiatives, in addition to annual follow-up audits by international certification bodies and special reviews when regulatory changes or significant incidents occur.

Since 2009, the DCV has presented its participants with the independent ISAE 3402/SOC 1 Type II report, prepared and evaluated by an external audit firm. This report verifies the DCV's internal control structure as an organization providing services to third parties, with an emphasis on the processes that directly impact the internal control structure of user entities. The scope includes both the certification of the controls implemented and tests of their operational effectiveness, conducted over a period of no less than 11 months, which allows for the conclusion with reasonable assurance that these controls have functioned adequately over time.

These activities are complemented by specific external audits, international certifications such as ISO 27001:2022 and ISO 22301:2019, as well as periodic assessments of the SWIFT Customer Security Controls Framework (CSCF). Likewise, the Internal Audit Department reviews critical processes at least every six months and non-critical processes every two years, proposing corrective and preventive action plans. Additionally, the DCV systematically addresses the requirements of its depositors, who periodically request information and verification regarding risk management, business continuity, information security, and internal control.

Key consideration 3: An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.

Operational Reliability Objectives

The DCV, as a financial market infrastructure, establishes qualitative operational reliability objectives aimed at ensuring the continuous availability of its critical services, resilience against operational incidents, the integrity and accuracy of recorded information, and the security of its technological infrastructure against cyberattacks or unauthorized access. These qualitative objectives aim to maintain the trust of participants and authorities, ensure regulatory compliance, and enhance transparency in management.

On the quantitative level, the objectives are defined in the corporate Balanced Scorecard (BSC), which periodically measures performance indicators. Notable among these are: ensuring that in

98.8% or more of cases, application response time is less than two seconds; achieving 99.80% or more compliance with service level agreements (SLAs) with the BCCh; maintaining 99.97% or higher availability of technology platforms; ensuring 98.50% or higher compliance with SLAs agreed upon with CCLV; and limiting critical operational incidents to a maximum of two per year, with a trend toward zero. Likewise, business continuity plans establish recovery objectives such as a 2-hour RTO for critical services and an RPO in minutes for data recovery.

These objectives are formally documented in the Business Continuity Policy, the Information Security and Cybersecurity Policy, the Operational Risk Management Manual, and the Risk Management Policy. Furthermore, they are reflected in the corporate Balanced Scorecard (BSC), which consolidates indicators for availability, response times, critical incidents, and SLA compliance (see Principle 21), and are monitored by the Audit Committee and the Risk and Cybersecurity Committee.

The explicit definition of availability and performance indicators, together with their systematic monitoring in the BSC, allows for the timely identification of deviations, the initiation of corrective actions, and the assurance of accountability at both the management and corporate governance levels. In particular, an availability target of 99.97% implies that the maximum tolerated downtime is approximately 13 minutes per month, which significantly limits the probability of significant disruptions in the provision of critical services. This standard is complemented by response times of less than two seconds for most transactions, compliance with SLAs with the BCCh (≥ 99.80%) and CCLV (≥ 98.50%), as well as continuous monitoring of critical operational incidents. These parameters ensure that operations remain at high levels of reliability and resilience, aligned with international best practices in operational risk management and business continuity.

The DCV's operational reliability objectives are based on the Business Continuity Policy (BCP/DRP), the Information Security and Cybersecurity Policy, the Risk Management Policy, the Operational Risk Management Manual, the Internal Audit Policy, the Policy on Reporting to the Board of Directors, the Operating Rules of the Audit Committee, the Operating Rules of the Risk and Cybersecurity Committee, the IT Environment Management Policy, and the Software Development Policy.

Key consideration 4: An FMI should ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service-level objectives.

Scalable Capacity

The DCV reviews, audits, and verifies the flexibility and adequacy of its technological capacity through the IT Infrastructure Usage Policy, the scope of which includes the management of technological resources, processing times, current business volumes, and the impact of new services. This policy establishes preventive parameters, such as that average utilization of installed capacity must not exceed 35%, that batch processing must be capable of running at least twice within the allocated period, and that on non-critical systems, utilization must not exceed between 60% and 70% of installed capacity. Capacity utilization is assessed monthly, ensuring systematic and timely monitoring.

Additionally, DCV subjects its systems to market stress tests at least once a year, simulating extreme conditions to verify the infrastructure's resilience and responsiveness. The results of these tests are reported to the management team, the internal auditor, the external auditor, and

the Board of Directors, ensuring transparency and accountability. These reviews are complemented by periodic audits and the application of control frameworks such as COBIT, which ensure alignment with international best practices in IT management and corporate governance.

It is worth noting that, with the launch of DCV Evolución, processing capacity increased fivefold compared to the pre-2022 infrastructure, representing a qualitative leap in the robustness and versatility of the systems. Currently, the DCV is conducting studies to adapt and update the Capacity Policy, in order to reflect this new technological reality and maintain consistency with the operational reliability standards required by regulation and international best practices.

When the volume of operations approaches or exceeds the operational capacity limit, the DCV applies a set of preventive and corrective measures defined in its Capacity Management Policy and IT Infrastructure Usage Policy.

First, continuous monitoring of technology infrastructure utilization levels is performed, with early warnings that allow for the anticipation of stress scenarios. If it is detected that installed capacity is approaching defined thresholds (for example, 35% average usage in critical systems or 60–70% in non-critical systems), adjustment plans are activated that include load redistribution, process optimization, and resource expansion.

Second, the DCV has controlled intervention windows and escalation procedures that allow for real-time reinforcement of operational capacity. This includes enabling additional servers, prioritizing critical processes, and coordinating with business units to defer non-essential operations.

Key consideration 5: An FMI should have comprehensive physical and information security policies that address all potential vulnerabilities and threats.

Physical Security

The DCV continuously addresses plausible sources of physical vulnerabilities and threats through an integrated set of corporate policies and operational processes that form part of its Risk Management Framework. These include the Business Continuity Policy, the Information Security and Cybersecurity Policy, the IT Environment Management Policy, the Software Development Policy, the Risk Management Policy, and the Change Management and Project Management procedures, which ensure that any technological or organizational change incorporates physical and operational risk assessments.

Security plans include specific procedures to prevent, mitigate, contain, and manage events such as fires, floods, earthquakes, terrorist attacks, fraud, theft, social unrest, war, and violent conflict. These plans are approved by the Board of Directors and reviewed at least once a year, ensuring they are updated in light of new threats.

Physical protection measures include access controls through building security, guards, and ID cards, as well as infrastructure designed to withstand natural disasters. The DCV has vaults for the safekeeping of valuables, earthquake-resistant construction, gas-based fire suppression systems, fire extinguishers, and water sprinklers, in addition to evacuation plans and emergency protocols.

The DCV applies guidelines derived from ISO/IEC 27001:2022, ISO/IEC 27002, and ISO/IEC 22301:2019, which establish best practices in information security and physical and environmental

security, including access controls, protection of critical assets, business continuity, and incident management.

Information Security

The DCV continuously manages vulnerabilities and threats to information security through a robust regulatory framework, the cornerstone of which is the General Information Security Policy, complemented by internal procedures and technical and organizational controls aligned with international standards. This approach allows for the systematic safeguarding of the confidentiality, integrity, and availability of the critical information that underpins its operations.

As part of this framework, the DCV conducts penetration tests and vulnerability assessments at least annually; the results are analyzed by the IT Operations and Cybersecurity Management team, reviewed by specialized governance bodies, and reported to the Board of Directors. Likewise, change management and project management processes incorporate security risk assessments from early stages, requiring testing in segregated environments and approval by competent committees prior to production deployment, which allows for the preventive identification and mitigation of potential vulnerabilities.

In terms of controls, the DCV implements logical security and cybersecurity measures that include individual credentials, role-based access control, segregation of duties, and restrictions on remote access. At the technological infrastructure level, it has perimeter and endpoint protection solutions, intrusion detection and prevention, continuous monitoring, and structured incident management, strengthening protection against internal and external threats. These capabilities are integrated under the permanent supervision of the IT Operations and Cybersecurity Management, which is responsible for coordinating incident response and strengthening operational resilience.

In 2025, the DCV obtained recertification under the ISO/IEC 27001:2022 standard, the international benchmark for information security management, which validates the effectiveness of a comprehensive set of controls aimed at protecting against cybersecurity risks. The certification is valid for three years, with annual follow-up audits, and is complemented by the implementation of the ISO/IEC 27002 standard, which establishes specific best practices in areas such as access control, asset management, physical and environmental security, and business continuity.

The DCV ensures that its information security policies and controls take into account international, national, and sector-specific standards. It maintains ISO/IEC 27001:2022 certification and applies ISO/IEC 27002 as a framework for best practices, while also complying with the requirements of the CMF and the BCCh.

Key consideration 6: An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.

Objectives of the Business Continuity Plan

The DCV Business Continuity Plan establishes objectives, policies, and procedures for the

recovery and resumption of critical operations in the event of incidents affecting their continuity, defining the Target Recovery Time Objective (TRTO), the Recovery Point Objective (RPO), the minimum business continuity objective (MBCO), and the maximum tolerable period of disruption (MTPD), in accordance with standards such as ISO 22301:2019 and ISO/IEC 27001; it also considers technological redundancy, alternate sites, and communication protocols with authorities and stakeholders, along with the conduct of periodic tests and crisis exercises, the results of which are reviewed by management and the Board of Directors.

Design of the Service Continuity Plan

The DCV Business Continuity Plan stipulates that critical IT systems must resume operations within a maximum of two hours following a significant disruption, while also ensuring that settlements are completed before the end of the business day. To this end, the design provides for the ability to transfer operations from the primary site to the secondary site in less than one hour. In the event of simultaneous loss of both sites, the third disaster recovery site guarantees a Target Recovery Time of two hours.

The availability thresholds are set forth in the document "Business Continuity Strategies," approved by the Board of Directors. The RPO is defined as zero seconds, which implies no data loss between the primary and secondary systems, achieved through real-time replication between both processing environments, ensuring the integrity and availability of the recorded information. Likewise, the DCV sets a TRTO of 2 hours from the occurrence of an outage, in line with international expectations applicable to financial market infrastructures, which require the ability to resume operations within that timeframe and ensure the completion of processing within the same business day. Additionally, an MBCO is defined as the minimum acceptable service level under contingency conditions, which is considered achieved when the system is capable of processing at least 80% of transactions in 2 seconds or less, thereby ensuring market operability even in degraded scenarios. For its part, the MTPD corresponds to the maximum downtime limit for critical services, beyond which unacceptable impacts arise for the operational continuity of the DCV and the proper functioning of the market; in this context, this limit is set at a maximum of the start of the next operating day following the occurrence of the event when the impact is limited exclusively to the DCV, while, in scenarios of systemic impact, it is adjusted to the time required for the resumption of market operations, taking into account the clearing and settlement cycles.

The plan is coordinated with complementary policies that reinforce technological resilience. The Production Rollout Policy requires rollback plans and controlled intervention windows to minimize risks in production environments. Likewise, the Application Support Policy regulates the management of critical incidents in accordance with CMF regulations, including escalation protocols and immediate activation of the continuity plan.

The General Corrective Maintenance Policy ensures that defects posing extreme or high risk are prioritized and validated in separate environments, reducing the likelihood of production failures. Meanwhile, the IT Environment Management Policy establishes strict segregation between production and pre-production environments, with continuous monitoring and service level agreements that support continuity.

Data Loss

If there is a possibility of data loss, the plan includes verification and reconciliation procedures with

relevant participants and third parties. These processes include reviewing transaction records, comparing balances and positions, and obtaining bilateral confirmation from affected counterparties. This ensures the complete reconstruction of information and the continuity of critical market operations.

The DCV has formalized crisis management procedures in the Business Continuity Policy and the Information Security and Cybersecurity Policy. Both documents establish the requirement to have internal and external communication protocols in place during the activation of contingency plans.

Internally, the IT Environment Management Policy and the Application Support Policy define escalation processes and immediate notification to critical areas, including continuity, security, and senior management.

Externally, the Information and Communications Technology Policy and the Business Continuity Policy establish the obligation to inform regulatory authorities (CMF, BCCh) and market participants through formal channels, ensuring traceability and consistency in messaging.

Communication is tested in business continuity simulation exercises, as outlined in the Business Continuity Policy, with the aim of validating response times and the effectiveness of the defined channels.

Secondary Site

The DCV has two alternative processing sites, both TIER III certified by the Uptime Institute. This certification ensures that the data centers are concurrently maintainable, with 99.982% availability, redundant components, and the ability to perform maintenance without affecting service continuity.

The secondary sites feature redundant critical infrastructure for power and cooling, gas-based fire suppression systems, fire extinguishers, and earthquake-resistant buildings. These measures protect equipment against risks of fire, flooding, or natural disasters.

In terms of location, DCV operates two data centers in Santiago separated by 14 km and a third recovery center more than 1,000 km from the primary site. This geographic distribution ensures distinct risk profiles and reduces the likelihood of simultaneous impact from a single event.

Production can be transferred from the primary site to the secondary site within 60 to 119 minutes, meeting the recovery objectives defined in the continuity plan. Additionally, the DCV can sustain its operations from the alternative sites for up to two months, ensuring continuity even in prolonged crisis scenarios.

Access to the secondary sites is primarily structured through remote connection mechanisms, with protocols for the redistribution of critical functions and personnel. This ensures adequate staffing to maintain operations during a contingency.

Since the services offered by the DCV to its users are defined as inconceivable without the availability of the computer systems built for that purpose, manual responses are not contemplated, given the complexity of the business and the risk involved.

Review and Testing

The DCV maintains a Business Continuity Management System certified under ISO 22301:2019. This certification requires periodic review of contingency and continuity plans, with tests

conducted at least once a year. Depositors and other financial market infrastructures participate in these exercises, verifying connectivity and operability from both the primary and alternative sites.

The processing sites are rotated periodically to validate the ability to operate from any of them. Additionally, the DCV conducts weekly remote access tests, ensuring that critical personnel can operate the systems during a contingency without interruption.

The DCV participates in the Business Continuity Committee led by the BCCh, a body that brings together the country's FMIs. In this context, joint continuity tests and partial crisis simulations have been conducted to validate the coordinated response to specific failures. The committee is currently working on an inter-FMI and BCCh crisis management protocol.

In addition, the DCV has conducted specific tests with Combanc to validate alternative messaging channels in the DVP service, ensuring operational continuity in the event of SWIFT network unavailability.

The DCV involves, where appropriate, its participants, essential service providers, and financial market infrastructures with which it maintains operational links in the review and testing of its contingency and service continuity mechanisms. This approach is aligned with international best practices in incident management and operational continuity, particularly with the provisions of ISO 22302:2021, which emphasizes the need to coordinate, test, and validate response and recovery procedures with all critical stakeholders that have relevant interdependencies.

Within this framework, the DCV participates in inter-FMI coordination efforts and with the BCCh to conduct testing exercises that include simulations of critical operational incidents and business continuity tests, aimed at verifying the effectiveness of communication channels, escalation protocols, alternative operating procedures, and the compatibility of target recovery times among interconnected entities. The results of these exercises are documented and evaluated, and serve as input for updating contingency and continuity plans, as well as for defining improvement actions.

Regarding frequency, the participation of essential service providers and, where applicable, Depositors, takes place at least annually, without prejudice to additional tests that may be conducted in the event of significant changes to the technological infrastructure, critical processes, or the DCV's risk profile. For their part, the FMIs with which the DCV maintains links participate in periodic coordinated tests, aligned with the schedules defined by the competent authority or by the relevant inter-FMI bodies.

Finally, interaction with critical providers and FMIs with operational interdependencies is supported by the Business Continuity Plan and service contracts that require joint testing at least annually or in the event of significant changes, aligning with the periodic review requirements established in both the local regulatory framework and ISO 22301:2019.

Key consideration 7: An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

Risks to the FMI's Own Operations

The DCV may be exposed to operational and reputational risk in the provision of its securities custody, administration, and transfer services, to the extent that failures in interconnected entities affect the efficiency, continuity, or reliability of such services. In its role as a central securities depository, the DCV faces risks associated with the proper administration, registration, and transfer of securities, which may be impacted by external events. In particular, the gross securities settlement service that the DCV provides to Depositors in conjunction with Combanc, and which is interconnected with the BCCh's LBTR System, could be affected by a failure at any of these FMIs, hindering the timely settlement of transactions.

Likewise, the DCV identifies, assesses, and manages significant risks arising from its connection to other critical entities, including Participants and providers of essential services, such as the SWIFT network, communications services, and power supply, among others. For each of these entities, specific controls, service level agreements, and continuity plans have been implemented, taking into account scenarios of partial or total unavailability.

To monitor risk exposures generated by other parties, the DCV uses alerts, automated controls, and feedback from participants. The DCV also continuously monitors these risks and reviews its risk management tools once a year.

The DCV has established that the outsourcing of essential services must meet the same reliability, security, and continuity requirements as internal services. This requirement is formalized in the Information and Communications Technology Policy, the IT Environment Management Policy, the Production Release Policy, the General Corrective Maintenance Policy, and the Application Support Policy.

Contracts with critical suppliers include service level agreements (SLAs) and operational level agreements (OLAs), with clauses regarding availability, recovery times, and contingency mechanisms equivalent to those required internally. Evidence of compliance with international standards such as ISO 22301:2019 and ISO/IEC 27001 is also required, as well as infrastructure certifications such as the Uptime Institute's TIER III for data center services.

The DCV conducts periodic audits and due diligence processes on its strategic suppliers, verifying the existence of technological redundancy, data replication, and crisis communication protocols. These processes include connectivity tests and joint simulations to validate the suppliers' ability to sustain operations in scenarios of significant disruptions.

Outsourcing governance is reinforced by the Software Development Policy (SGSI-INT-I-POLI-GTC-1.5), which regulates the participation of external suppliers in projects and maintenance, establishing requirements for security, quality, and code traceability.

Risks to Other Financial Market Infrastructures

Given its central role in the Chilean financial market infrastructure, the DCV transmits operational risks to other financial market infrastructures, particularly CCA, ComDer, and CCLV. CCA is

exposed in its capacity as a low-value payment system, while ComDer and CCLV are exposed in their capacity as central counterparties, with CCLV additionally serving as a securities settlement system. Likewise, the BCCh's LBTR system is exposed to these interdependencies. In the event of a significant disruption in the DCV's operations, these entities could see their ability to operate normally compromised. In particular, CCA, the LBTR, ComDer, and CCLV would be unable to properly execute collateral management processes, and CCLV would be prevented from transferring ownership of securities within the framework of its functions as a securities settlement system and as a central counterparty.

The DCV identifies and monitors risks that could affect other financial market infrastructures through a Risk Management Framework formalized in the Information and Communications Technology Policy, the IT Environment Management Policy, the Production Release Policy, the General Corrective Maintenance Policy, and the Application Support Policy. These policies establish controls for operational continuity, critical incident management, and the traceability of changes in production and pre-production environments.

The identification of new inter-FMI risks is carried out through continuous monitoring of critical operational incidents in accordance with CMF regulations and DCV policies, impact assessments of changes and maintenance on shared services, and participation in the Business Continuity Committee led by the BCCh.

Risk mitigation toward other FMIs is articulated in coordinated contingency plans that include operational reconciliation and alternative messaging channels, inter-FMI communication protocols that ensure timely and consistent information to the BCCh and counterparties, and rollback plans and controlled exception mechanisms established in the Production Release Policy.

Coordination of Service Continuity Mechanisms

The DCV has implemented an operational resilience framework that integrates its business continuity plans with the functioning of the financial system as a whole. This coordination is based on the provisions of the BCCh and the CMF, particularly the BCCh's CNF (Chapter III.H.2), which establishes operational continuity obligations, contingency protocols, and inter-FMI coordination to mitigate systemic risks and ensure the stability of payment and settlement systems. The CMF, through NCG 509 and NCG 510, regulates the management of critical incidents, information security, and the technological resilience of supervised entities.

In this context, planned exercises are conducted with the IMF, in coordination with Combanc and the BCCh, aimed at validating the availability of contingency channels, including the SWIFT channel, and at evaluating the consistency of escalation schemes, recovery times, and the operational capacity of participating institutions. Coordination is reinforced through formal governance bodies, such as the Business Continuity Committee led by the BCCh and the DCV Security Committee, which ensure ongoing technical oversight and operational alignment among interdependent financial infrastructures.

Principle 18: Access and Participation Requirements

An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

Key consideration 1: An FMI should allow for fair and open access to its services, including by direct and, where relevant, indirect participants and other FMIs, based on reasonable risk-related participation requirements.

Participation Criteria and Requirements

The regulatory framework applicable to the DCV establishes legal, operational, and technological criteria for the admission of depositors. Pursuant to Article 2 of Law 18,876 and Chapter 4 of its Internal Regulations, various financial and non-financial entities may be established as depositors, including banks, issuers of publicly offered securities, government agencies acting as issuers, other financial market infrastructures (FMIs), and such additional entities as the DCV expressly approves.

At the operational level, participation requirements focus on ensuring robust and continuous connectivity with the DCV's technology platform. Participants must maintain an active connection to the primary and secondary processing sites and ensure access to the backup site (SRAD) via the Internet. This requirement aims to ensure the system's operational continuity and technological resilience in the face of contingencies.

Access to the DCV is based on objective criteria proportional to risk. Law 18,876 determines who may be depositors, including banks, issuers of publicly offered securities, public issuing agencies, and other entities approved by the DCV. The DCV's Internal Regulations supplement the law and detail the specific conditions for participation. The admission of entities is governed by clear regulatory requirements and by the ability to meet operational and technological standards that ensure continuity and resilience. These parameters establish minimum connectivity conditions, applied uniformly, avoiding barriers to entry and ensuring equal obligations among participants.

Key consideration 2: An FMI's participation requirements should be justified in terms of the safety and efficiency of the FMI and the markets it serves, be tailored to and commensurate with the FMI's specific risks and be publicly disclosed. Subject to maintaining acceptable risk control standards, an FMI should endeavor to set requirements that have the least-restrictive impact on access that circumstances permit.

Justification and rationale for participation criteria

The DCV's participation criteria are justified in terms of security and efficiency, as they require only conditions essential for integration with its technological infrastructure. This framework is governed by Law 18,876, which defines who may be depositors, and by the DCV's Internal Regulations, which detail the conditions for participation and operational requirements.

The non-risk-based participation requirements pertain exclusively to determining the type of entity that may qualify as a depositor, in accordance with the provisions of Article 2 of Law 18,876. Thus, the securities depository must accept as depositors those identified in subparagraphs (a) through (m) of Article 2 of said law. As for subparagraph n), which includes "other [entities] authorized by the company" and covers, for example, fintech service providers regulated by Law 21,521, their

admission requires prior authorization from the securities depository. In this regard, the DCV's Internal Regulations provide that such authorization may be granted by a resolution adopted by at least seven of its directors.

Participants acting as depositors (banks, brokerage firms, fund managers, issuers of publicly offered securities, and public-sector issuers) must comply with the regulatory requirements set forth in Law 18,876 and the Internal Regulations, which include legal authorization and technological connectivity with processing and backup systems.

Similarly, participants acting as securities issuers and paying agents are subject to operational conditions tailored to their specific role within the payments and benefits chain. These criteria aim to ensure the proper execution of dividends, coupons, and other investor rights. For other FMIs or indirect participants, requirements may include additional conditions regarding operational coordination and custody standards, given that they act on behalf of third parties and concentrate distinct risks.

Less restrictive access

The requirements for participation in the DCV are limited to ensuring adequate connectivity, security, and integration with its systems, provided that applicants are established as entities authorized under Law 18,876 and the Internal Regulations. Thus, these requirements represent the least restrictive impact possible on access for new participants and are subject to continuous review to maintain their proportionality and relevance.

Disclosure of Criteria

Article 2 of Law 18.876 defines the categories of entities eligible to become depositors. In practice, this means that access to the system is contingent, first and foremost, on the participant's legal and institutional nature—as is the case, for example, with banks, stockbrokers, fund managers, or insurance companies—rather than on a specific assessment of their risk profile. For its part, the Internal Regulations, in accordance with the provisions of Article 24 of the Regulations of Law 18,876, specify the conditions, requirements, and specific procedures for admission, including the signing of the respective contracts, operational requirements, and applicable evaluation mechanisms.

Key consideration 3: An FMI should monitor compliance with its participation requirements on an ongoing basis and have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participation requirements.

Compliance Monitoring

The DCV continuously monitors its participants' compliance with the access criteria through formal oversight mechanisms that involve ongoing monitoring of the legal and operational requirements established in Law 18,876 and the Internal Regulations.

The DCV intensifies its monitoring in the event of deteriorating risk through enhanced monitoring, requests for additional information, operational restrictions, coordination with the CMF, and, in critical cases, suspension or exclusion.

Suspension and Orderly Exit

Title 20 of the Internal Regulations establishes that a repeat offender may be suspended for 15 days and, in the event of further violations or serious offenses, permanently excluded. The procedures for the suspension and orderly exit of participants are made public in the DCV's Internal Regulations.

Principle 19: Tiered Participation Arrangements

An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.

Principle 19 does not apply to the DCV because there is no multi-tiered participation in the DCV. DCV depositors hold their own securities and those of their clients in separate accounts, which are easily identifiable by the DCV.

Principle 20: FMI LInks

An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

Key consideration 1: Before entering into a link arrangement and on an ongoing basis once the link is established, an FMI should identify, monitor, and manage all potential sources of risk arising from the link arrangement. Link arrangements should be designed such that each FMI is able to observe the other principles in this report.

Potential sources of risk arising from such a linkage mechanism

In addition to the links it maintains with the other Chilean FMIs—CCLV, ComDer, Combanc, CCA, and the BCCh—the DCV maintains operational links with the foreign CSDs Euroclear (Belgium), DECEVAL (Colombia), and CAVALI (Peru). It also maintains a link with the global custodian Citibank, allowing DCV depositors to trade in markets across Latin America, Europe, and Asia, thereby expanding their international access and settlement capabilities. These links are structured through the DCV's participation in foreign deposit or custodian accounts, enabling the DCV to offer foreign securities custody services to its depositors and local investors.

To establish any international link, the DCV applies a formal due diligence process designed to identify and assess potential sources of risk associated with the relationship, including legal, credit, liquidity, custody, and operational risks. This process is defined in the Supplier Management Policy (specifically in Section 7.3), as well as in the International Custodian Contracting Policy and its Annex, and in the PFMI, particularly Principle 20 on IMF–IMF links. The legal assessment considers the regulatory authorization of the link, compatibility between jurisdictions, the validity of powers of attorney, and the corporate structure of the third party, in accordance with the requirements set forth in the Annex to the Supplier Management Policy and the legal criteria of the International Custodian Engagement Policy. The financial assessment includes a review of audited financial statements, tax compliance, and solvency, including the requirement for minimum credit ratings for international custodians, as established in the International Custodians Annex. With regard to custody, the DCV reviews asset segregation, protection against creditors, the transferability of securities, and account handling, following criteria 4 through 7 of the International Custodians Annex and PFMI Principle 16. Finally, the liquidity risk assessment considers dependencies on

payment systems and potential impacts on settlement capacity, in line with PFMI Principles 7 and 20.

The outcome of these assessments directly determines the DCV's decision regarding whether or not to establish the link. Both the Supplier Management Policy and the International Custodian Contracting Policy stipulate that a contract may only be entered into when all review conclusions are positive or recommendatory. If any assessment is negative or non-recommendatory, the case must be referred to the Finance and Investment Committee, which decides whether the link proceeds or is rejected, a decision that must be documented. This approach is fully consistent with PFMI Principle 20, which requires FMIs to establish links only when the associated risks are identified, assessed, and manageable. Consequently, the risk analysis not only identifies sources of exposure but also serves as the determining criterion for approving, conditioning, or rejecting the establishment of a relationship.

The DCV ensures that its link agreements do not affect compliance with the other principles through a prior review and ongoing monitoring as defined in the Supplier Management Policy, the International Custodian Engagement Policy, and the PFMI, particularly Principle 20. Before establishing a link, the DCV verifies that there are no legal, financial, operational, custody, or liquidity risks that could compromise its regulatory framework, operational continuity, or asset protection, and that the third party complies with equivalent standards in security, continuity, and governance.

Once implemented, the relationship is evaluated periodically using the critical supplier model: annual reviews covering financial, legal, business continuity, information security, and compliance matters, and semi-annual reviews covering SLAs, incidents, reputation, and flexibility. For international custodians, an annual review of compliance with applicable IOSCO Principles is also required. Any material deviation is reported to the responsible manager and the Finance and Investment Committee, which may direct corrective actions or review the continuity of the link.

Key consideration 2: A link should have a well-founded legal basis, in all relevant jurisdictions, that supports its design and provides adequate protection to the FMIs involved in the link.

Legal Basis

The legal framework underpinning the operational links is found in Law 18,876, whose Articles 2 and 3 define the purpose of securities depository companies and authorize them to carry out the acts necessary for their operation. This framework is supplemented by its Regulations, contained in Supreme Decree 734 of the Ministry of Finance, particularly Article 5, which expressly authorizes the holding of securities in domestic and foreign entities. Together, these provisions empower the DCV to establish and maintain links with other international infrastructures and custodians in the performance of its custody functions.

Internally, Title 15 of the DCV's Internal Regulations, approved by the CMF, expressly regulates interaction with foreign CSDs and global custodians to offer foreign securities custody services to local residents. Likewise, the Supplier Management Policy and the International Custodian Contracting Policy establish the legal, financial, operational, and custody requirements that third parties must meet before being approved.

The DCV ensures that its relationships have a well-founded legal basis, primarily through bilateral contracts with each foreign CSD or global custodian. These contracts precisely define the applicable law and establish that essential principles such as purpose, irrevocability, and the protection of rights shall be governed by the regulations of the issuing CSD, ensuring legal certainty in all jurisdictions involved.

To maintain these protections over time, the DCV applies due diligence and continuous monitoring processes, periodically reviewing the validity of powers of attorney, corporate changes, international certifications, and contractual terms. In addition, international custodians are classified as critical providers and are subject to regular assessments in financial, legal, operational, and security dimensions, which allows for the timely detection of any changes that may affect the legal soundness of the link and enables the adoption of corrective measures or a review of its continuity.

Key consideration 3: Linked CSDs should measure, monitor, and manage the credit and liquidity risks arising from each other. Any credit extensions between CSDs should be covered fully with high quality collateral and be subject to limits.

Credit and Liquidity Risks in Linkages

The DCV does not extend credit or provide liquidity to participants or other CSDs within the framework of links, and does not allow overdrafts or debit balances in securities accounts. All transfers are executed on a best-availability basis, meaning they are settled only when the securities (and, where applicable, funds) are actually available and transferable. Consequently, no open credit exposures are generated. Furthermore, the DCV's operational model prevents liquidity mismatches, as settlement does not occur if there is no actual availability, thereby eliminating the need for the DCV to advance its own or third-party funds. Consequently, it assumes no payment or delivery obligations contingent on a counterparty's future performance.

Key consideration 4: Provisional transfers of securities between linked CSDs should be prohibited or, at a minimum, the retransfer of provisionally transferred securities should be prohibited prior to the transfer becoming final.

Credit extensions, securities overdrafts, and cash overdrafts are not permitted in any contracts with other CSDs. Transactions are executed only when securities and funds are available and transferable.

Key consideration 5: An investor CSD should only establish a link with an issuer CSD if the arrangement provides a high level of protection for the rights of the investor CSD's participants.

Protection of the rights of participants in the investor CSD

When the DCV acts as an investor CSD, it maintains an account with the issuer CSD where securities are registered or recorded, and it is listed as the holder in that registry. The agreements underpinning each link explicitly state that ownership of the securities belongs to the DCV's clients and that these securities may not be used to back obligations of either the DCV or the issuer CSD.

To reinforce this protection, the DCV performs daily reconciliations between the balances recorded in the names of its depositors holding foreign securities and the total positions held in

the accounts of foreign CSDs, ensuring full correspondence and traceability.

As an investor CSD, the DCV protects the rights of its participants by segregating accounts by type of ownership, keeping the participant's own accounts separate from third-party (client) accounts within its system. This prevents commingling of assets and allows for the transfer of securities to another intermediary when appropriate. In the case of omnibus accounts, this protection is reinforced through contractual clauses and legal safeguards that exclude such securities from the assets of the participant and the DCV.

This framework is based on Law 18,876, which regulates central securities depositories in Chile and requires the separation of the depositor's own securities from third-party securities held in custody, and on the Internal Regulations, which operationalize this requirement through the opening and administration of segregated accounts by type of ownership (own accounts and third-party accounts).

Key consideration 6: An investor CSD that uses an intermediary to operate a link with an issuer CSD should measure, monitor, and manage the additional risks (including custody, credit, legal, and operational risks) arising from the use of the intermediary.

This key consideration does not apply to the DCV, as the DCV does not use intermediaries to operate links with issuer CSDs.

Key consideration 7: Before entering into a link with another CCP, a CCP should identify and manage the potential spill-over effects from the default of the linked CCP. If a link has three or more CCPs, each CCP should identify, assess, and manage the risks of the collective link arrangement.

This key consideration does not apply to the DCV, as it applies only to CCPs.

Key consideration 8: Each CCP in a CCP link arrangement should be able to cover, at least on a daily basis, its current and potential future exposures to the linked CCP and its participants, if any, fully with a high degree of confidence without reducing the CCP's ability to fulfil its obligations to its own participants at any time.

This key consideration does not apply to the DCV as it applies only to CCPs.

Key consideration 9: A TR should carefully assess the additional operational risks related to its links to ensure the scalability and reliability of IT and related resources.

This key consideration does not apply to the DCV, as it applies only to TRs.

Principle 21: Efficiency and Effectiveness

An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.

Key consideration 1: An FMI should be designed to meet the needs of its participants and the markets it serves, in particular, with regard to choice of a clearing and settlement arrangement; operating structure; scope of products cleared, settled, or recorded; and use of technology and procedures.

Design in accordance with the needs of participants and markets

The DCV ensures that the design of its services, systems, and processes meets the needs of its participants and the markets it serves through a structured framework of governance, consultation, and continuous feedback, in line with the PFMI.

The DCV's corporate governance is based on a mutual ownership structure, under which its shareholders are, in turn, companies representing the various industries or market sectors in which the depositors operate, and they hold a proportional stake on the board of directors, maintaining a certain alignment between ownership and the intensity of service use. This facilitates strategic decisions regarding operational design, clearing, settlement, and technology that directly incorporate the users' perspective (see Principle 2). This governance is complemented by the recommendations of the Oversight Committee.

Additionally, the DCV maintains formal and periodic channels of interaction with depositors, such as the General Assembly of Depositors, meetings with specific user groups, and the Depositors' Committee, where relevant initiatives are presented and comments and concerns are gathered prior to their implementation.

From an operational and continuous improvement perspective, the DCV conducts quarterly customer satisfaction surveys that measure participants' perceptions regarding overall service quality, system availability, response times, operational continuity, and service provided by the Customer Service Desk (MAC). The results are used to make adjustments to services, processes, and service levels.

Finally, the DCV has strengthened its approach to customer relationships and experience by creating the Commercial Division, organized around three complementary pillars: transforming the commercial relationship into a strategic one, optimizing the efficiency of customer service, and developing management centered on customer experience.

Together, these mechanisms allow the DCV to continuously verify that its operational and technological design remains aligned with the actual needs of the market.

Assessment of User Needs Satisfaction

The DCV has a formal process of quarterly customer satisfaction surveys, designed as a structural feedback tool to continuously evaluate the quality, timeliness, and suitability of its services in relation to participants' needs.

The surveys are periodically administered to depositors and consider quantitative and qualitative indicators, covering, among other aspects: the overall evaluation of DCV services; the availability, stability, and performance of systems; operational and response times; incident management and

operational continuity; and the quality, clarity, and timeliness of the service provided by the Customer Service Desk (MAC). Additionally, sections for open comments are included, allowing for the collection of specific observations, suggestions, and emerging needs from participants.

Survey results are consolidated, analyzed, and compared over time, enabling the identification of trends, recurring gaps, and opportunities for improvement. This information is reviewed by the relevant operational, technological, and commercial departments and translated into concrete action plans, such as process adjustments, improvements to technological platforms, strengthening communication with participants, and optimizing service levels.

Key consideration 2: An FMI should have clearly defined goals and objectives that are measurable and achievable, such as in the areas of minimum service levels, risk-management expectations, and business priorities.

Clearly defined goals and objectives

The DCV measures the effectiveness of its operations through a Corporate Balanced Scorecard, which constitutes the organization's primary strategic management system. This tool is ratified by the Board of Directors and formalized through a letter of commitment signed by the Chairman of the Board, ensuring its alignment with the institutional strategy and its endorsement at the highest level of corporate governance.

The Corporate BSC is structured around four perspectives:

The Strategic Shareholders/Finance Perspective (37%) focuses on the DCV's financial efficiency and sustainability and is measured using indicators related to expense control, information technology costs, compensation, staffing levels, and efficiency ratios, with the aim of ensuring responsible and consistent resource management.

The Customers/Service Delivery Strategic Perspective (57%), which carries the highest weighting in the BSC, evaluates the quality and operational continuity of DCV's services through indicators of customer satisfaction, compliance with service level agreements, platform availability, application response times, service revenue, and control of critical operational incidents.

The Organizational Strategic Perspective (6%) measures internal aspects of organizational management, such as employee engagement and compliance with the critical staff backup policy, recognizing that human capital is a key enabler of operational effectiveness.

The Risk Management Strategic Perspective acts as a multiplier of the BSC's overall result and incorporates indicators of regulatory compliance, operational risk management, cybersecurity, integrity of assets in custody, regulatory compliance, and execution of business continuity plans, ensuring that overall performance is achieved within a robust risk management and control framework.

The BSC breaks down overall performance into four weighted strategic perspectives: Shareholders/Finance (37%), Customers/Service Delivery (57%), Organization (6%), and Risk Management, the latter applied as a multiplier for the consolidated result. Each perspective consists of key performance indicators (KPIs) with quantifiable targets and predefined evaluation ranges (Below, Target, and Above), expressed through objective thresholds—including critical ranges below 80–90% and outstanding levels equal to or above 120%.

The BSC 2025 demonstrates solid performance across its most critical indicators. For example, in Risk Management, all parameters reached 100%. In the Customer perspective, satisfaction reached 85%, channel response capacity reached 95%, and the SLA for resolving requests stood at 90%, reflecting high service levels.

Key consideration 3: An FMI should have established mechanisms for the regular review of its efficiency and effectiveness

Periodic review of its efficiency and effectiveness

The DCV evaluates its efficiency and effectiveness through an integrated system of formal management and performance measurement processes, designed to ensure both the quality of operational results and adequate risk control. Daily operational monitoring allows for constant tracking of system availability, processing times, and compliance with service level agreements (SLAs).

Periodic business continuity (BCP) and disaster recovery (DRP) tests ensure the resilience of the infrastructure and the ability to respond to contingencies, reinforcing the stability of critical services.

Integrated risk management focuses on identifying, assessing, and controlling operational, technological, legal, and reputational risks, with the aim of keeping exposures under control and preventing impacts on operations.

Quarterly customer satisfaction surveys measure depositors' perceptions of service quality, response times, and the service received, providing input for continuous improvement.

Feedback mechanisms, such as the Depositors' Committee, the Depositors' Assembly, and regular meetings with depositor groups, provide formal forums for dialogue that strengthen transparency and participation in service design.

Finally, internal and external audits verify regulatory compliance, process efficiency, and the quality of controls, providing an independent perspective that contributes to continuous improvement and depositor confidence.

The KPIs defined in its BSC are measured monthly and allow for monitoring system availability, processing times, and compliance with service level agreements, feeding into both the quality assurance system and the internal control system to foster continuous process improvement. In addition, compliance with the goals and objectives established in the BSC is reviewed quarterly by the Board of Directors and its specialized committees. Customer satisfaction surveys are conducted quarterly. Finally, the effectiveness and efficiency of operations are evaluated annually by external professionals, auditors, regulators, and consultants, who verify regulatory compliance, process efficiency, and the quality of controls.

Principle 22: Communication Standards and Procedures

An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

Key consideration 1: An FMI should use, or at a minimum accommodate, internationally accepted communication procedures and standards.

Communication Procedures

Within the local ecosystem, the DCV maintains its communications with depositors through a proprietary web-based system, whose messaging standard is based on ISO 15022. For its interactions with other financial market infrastructures in Chile—Combanc, ComDer, CCA, and the Central Bank—the DCV uses SWIFT's international financial messaging services in accordance with the ISO 20022 (MX) standard, ensuring interoperability with national payment and settlement systems. Internationally, the DCV connects with foreign custodians, such as Euroclear and Citibank, also using SWIFT messaging under the ISO 20022 (MX) standard.

The DCV uses SWIFT's international financial messaging services in accordance with the ISO 20022 (MX) standard for the flow of financial transactions with foreign custodians.

Communication Standards

For communications with participants, the proprietary messaging standard is based on the ISO 15022 standard. Meanwhile, the ISO 20022 (MX) standard is the internationally accepted standard for financial communications.

The DCV uses SWIFT's international financial messaging services in accordance with the ISO 20022 (MX) standard for the flow of financial transactions with foreign custodians.

Principle 23: Disclosure of Rules, Key Procedures, and Market Data

An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.

Key consideration 1: An FMI should adopt clear and comprehensive rules and procedures that are fully disclosed to participants. Relevant rules and key procedures should also be publicly disclosed.

Rules, Procedures, and Disclosure

The primary document containing the DCV's rules and procedures is its Internal Regulations, approved by the CMF and available on the institutional website. These Bylaws govern the relationship between the DCV and its depositors, establishing the responsibilities of the company and the Board of Directors, the processes for depositing and withdrawing securities, the administration of custody accounts, ordinary and extraordinary settlement cycles, procedures for handling delays or contingencies, operational risk and business continuity management, as well as the sanctions regime applicable to participants.

The Internal Regulations are supplemented by circulars and operational instructions that enable their practical application and detail specific aspects of operations. The circulars communicate regulatory changes, adjustments to settlement deadlines, the introduction of new services, or reminders of depositors' obligations, and are official and binding. The operational instructions, on the other hand, provide technical details on how to execute transactions on the DCV platforms, describing workflows, validations, file formats, connection requirements, and security measures, serving as guides for participants' operational departments.

These documents are communicated through publication on the corporate website and the direct sending of circulars and electronic notifications to depositors.

The DCV ensures that its rules and procedures are clear and comprehensive through an internal and external validation process. The Internal Regulations and circulars are reviewed and approved by the Board of Directors and the CMF. Additionally, the DCV maintains a process of continuous feedback with depositors through the Depositors' Committee, the Oversight Committee, the General Assembly of Depositors, and periodic meetings, where comments are gathered and the documents are adjusted to ensure their practical understanding. In addition, the DCV conducts training sessions, workshops, and informational sessions to explain the rules and procedures, ensuring that users understand their application. Finally, internal and external audits, along with annual compliance reviews, confirm that the procedures comprehensively cover critical aspects of operations and risk management.

The regulations are widely disseminated and uniformly applied in daily operations, as evidenced by the fact that, to date, no incidents have been recorded resulting from ambiguities or divergent interpretations of the system's regulations.

Descriptions of the system's design and operations

The DCV's Internal Regulations establish specific provisions to address unusual, yet foreseeable, events with the aim of ensuring operational continuity and maintaining participant confidence. This

includes procedures for dealing with delays in settlement cycles, allowing, when necessary, for extraordinary settlements to be conducted to fulfill outstanding obligations and restore the system's normal operation.

The regulations also govern business continuity and disaster recovery plans for technological failures, disruptions to critical services, or external emergencies, including data backup and restoration protocols that ensure operations can continue under adverse conditions.

Finally, operational risk management standards are incorporated to identify, assess, and mitigate foreseeable contingencies, such as errors in information transmission, system unavailability, or connection failures.

Law 18,876 requires the adoption of Internal Regulations approved by the authority and stipulates that any amendment must be authorized in advance by the CMF. Supreme Decree 734 of 1991 supplements this law, detailing operational aspects and reinforcing the requirement for prior authorization for regulatory changes. In particular, the processes the DCV follows to change its rules and procedures are stipulated in the Internal Regulations, which are publicly available.

The DCV publicly discloses its rules and procedures primarily through its institutional website, where it publishes relevant regulations, manuals, instructions, and policies. It also communicates updates via circulars and press releases, supplementing this information with annual reports and direct channels with depositors.

Key consideration 2: An FMI should disclose clear descriptions of the system's design and operations, as well as the FMI's and participants' rights and obligations, so that participants can assess the risks they would incur by participating in the FMI.

Clear Descriptions of Design and Operations

The design and operations of the DCV system are described in three main documents. The Internal Regulations, approved by the CMF, constitute the central regulatory framework and detail the system's structure. DCV circulars supplement the Regulations and communicate operational changes. Third, the operational instructions and technical manuals provide practical details on the system's design and operation, including workflows, file formats, connection requirements, and security measures. These documents are available on the DCV website and are updated as operational needs arise.

First, the Internal Regulations explicitly establish the areas in which the DCV may exercise discretion, for example, in the administration of extraordinary settlement processes or in defining operational measures in response to contingencies. Second, official circulars inform depositors and clients how that discretion will be applied in practice, detailing procedures, deadlines, and conditions.

The DCV informs its participants, through its Internal Regulations, circulars, and instructions, of the rights (access to services, representation in formal proceedings), obligations (compliance with operational rules, maintenance of collateral, reporting of information), and risks assumed (operational, counterparty, liquidity, and technological) when participating in the system, and these are specified in greater detail in the contracts signed by DCV depositors.

Key consideration 3: An FMI should provide all necessary and appropriate documentation and training to facilitate participants' understanding of the FMI's rules and procedures and the risks they face from participating in the FMI.

Documentation and Training for Participants

Upon becoming a depositor in the DCV, participants are provided with the relevant rules and procedures, operational guidelines, and technical information regarding the DCV's technology platform, including a detailed user manual. These resources are generally sufficient for participants to understand the rules, procedures, and risks associated with their participation in the DCV. In addition, many of the depositors' operators have years of experience interacting with the system, which contributes to a solid understanding of its operation and the inherent risks.

The DCV also has a training program aimed at all users, especially when significant developments are implemented in its operational platforms. In this context, a certification process is being developed that includes training for new depositors, training in the operation of new services, and the creation of test environments to facilitate familiarization with the systems.

There have been no significant misinterpretations regarding the content, scope, and application of the rules and procedures, which demonstrates an adequate level of understanding among participants and the effectiveness of the communication and dissemination mechanisms implemented.

If the DCV identifies a participant committing operational errors in the system, indicating an insufficient understanding of the rules, procedures, or associated risks, corrective measures are applied in accordance with the Internal Regulations. These measures include providing additional training and guidance, participation in practical sessions in test environments, as indicated in the DCV user manuals, and monitoring the participant's operations until it is verified that the errors do not recur.

Key consideration 4: An FMI should publicly disclose its fees at the level of individual services it offers as well as its policies on any available discounts. The FMI should provide clear descriptions of priced services for comparability purposes.

Fee Disclosure

The DCV's fee structure is detailed in Title 19 of the Internal Regulations, which, as previously noted, is a public document. Additionally, participants and the general public can access the fee structure directly through the DCV's website.

Fee information is presented in a breakdown by service and includes both general expenses (such as the monthly fee and custody fees) and specific charges for deposit accounts, securities transfer services, inventory accounts, trade registration services, among others.

For each service, fees are detailed by instrument type and transaction type, thereby providing transparency and clarity to participants. Information on applicable discounts is also published and regulated in Section 20.10 of the Internal Regulations, ensuring that all terms and conditions are publicly available and verifiable.

Changes to fees or service conditions are reflected in Title 19 (Fees) or other relevant sections of the Internal Regulations, a document that is public and serves as the official reference for

depositors.

The DCV provides a detailed description of the prices for the services it offers. The fee structure and the description of the corresponding services specify service categories, charges, and applicable conditions, broken down by service type, financial instrument type, and transaction type.

Additionally, the DCV has conducted independent fee studies, prepared in compliance with CMF regulations and CMF General Rule 224, which support the rationale for service fees and explain their structure with the support of technical analyses and external experts.

The DCV discloses relevant information on the factors that impact the FMI's operating costs, including aspects related to technology and communication, through its fee studies. These studies detail the composition of the costs associated with the platform's operation, considering technological infrastructure, maintenance, IT security, and other elements that affect the provision of services.

Key consideration 5: An FMI should complete regularly and disclose publicly responses to the CPSS-IOSCO disclosure framework for financial market infrastructures. An FMI also should, at a minimum, disclose basic data on transaction volumes and values.

Disclosure Framework

The DCV has periodically prepared the CPMI-IOSCO Disclosure Framework for Financial Market Infrastructures, which is updated and published at least every two years.

Quantitative Information

The DCV publicly discloses relevant quantitative information regarding its operations, including the volume of processed transactions, balances of deposited securities, movements in deposit accounts, and aggregated data on settlement and custody. Some of this data is published daily through statistical reports, such as custody reports, which show the volumes and amounts of instruments held, and transaction reports, which detail the transactions recorded at the close of each trading day. Other indicators, such as monthly or annual aggregates, are updated monthly or annually, as applicable, in accordance with the provisions of the Internal Regulations.

In addition to quantitative information, the DCV discloses its fee and service charge structure; operational and technological procedures, including user guides and operating manuals; risk management and business continuity policies, which describe risk mitigation mechanisms and contingency plans; and regulatory or service changes or updates.

The DCV publicly discloses this information through its website, available in Spanish and English, and through circulars and official communications to participants. Key information, including fees, procedures, manuals, and risk policies, is published in Spanish, while certain key documents and sections are also available in English for international users.

V. LIST OF PUBLIC RESOURCES

DCV Website
www.dcv.cl

Financial Market Commission
www.cmfchile.cl

Central Bank of Chile
www.bcentral.cl

Library of the National Congress of Chile
www.bcn.cl