d

ISSA International Securities Services Association

Securities Services Risks 2025 Report

April 2025

DISCLAIMER

It is ISSA's intention that this report should be updated periodically. This document does not represent professional or legal advice and will be subject to changes in regulation, interpretation, or practice. None of the products, services, practices or standards referenced or set out in this report are intended to be prescriptive for Market Participants. Therefore, they should not be viewed as express or implied required market practice. Instead, they are meant to be informative reference points which may help Market Participants manage the challenges in today's securities services environment. Neither ISSA nor the members of ISSA's Working Group warrant the accuracy or completeness of the information or analysis contained in this report.

Table of Contents

Section 1: Executive Summary

Introduction

The International Securities Services Association (ISSA) is a global association that supports the Securities Services industry. ISSA's members include Central Securities Depositories (CSDs), custodians, technology companies and other firms who are actively involved in all aspects of the Securities Services value chain. By connecting its members and facilitating collaboration, ISSA provides the leadership necessary to drive change in the Securities Services industry. The focus is on finding progressive solutions to reduce risk and improve efficiency and effectiveness – from issuer through to investor – as well as on providing broader thought-leadership to help shape the future of the industry.

The ability to understand and mitigate risks is key to all participants in the Securities Services value chain. Mitigating risks can prevent organizations being impacted by unexpected events and from potentially suffering financial, operational and / or reputational loss. ISSA has therefore created the ISSA Securities Services Risk 2025 report which aims to provide those actively involved in the Securities Services industry with sufficient information to be able to both identify potential risks and implement actions to mitigate these risks. However, whilst looking to identify the key risks inherent in Securities Services, it should be noted that not all risks can be mitigated and are a necessary part of doing business. It is the responsibility of each organization to undertake their own research and assessment to ensure that they understand both the risks being taken and how best these can be managed.

Background

In 2017, ISSA published a 'Report on Inherent Risks within the Global Custody Chain' (Inherent Risks within the Global Custody Chain (issanet.org)) which refreshed the earlier 1992 publication 'Report on Global Custody Risks'. Both reports were designed as informational texts with an objective of improving the understanding of Securities Services, leading to a better appreciation of risks and therefore an outcome where risk mitigation across the Securities Services value chain was improved and losses and adverse outcomes were minimized.

Since the last report, the Securities Services industry has seen ongoing change with:

- New asset classes gaining investor popularity
- Significant developments in technology observed
- Fundamental operating model changes moving forward
- Regulations continuing to evolve
- The impact of geopolitical events having materialized

Given these developments, ISSA believes it is now appropriate to produce an updated Securities Services risk report.

ISSA Securities Services Risks 2025

The new ISSA report starts with a section that provides context, defining Securities Services, outlining Securities Services within the asset lifecycle and by explaining the role of the different participants and functions within the Securities Services value chain. The next section is then structured by the key risk types which are inherent within the provision of Securities Services and provides information on common approaches to risk mitigation.

These risks include:

- Operational Risk categories:
  - Regulatory, Legal and Compliance Risk
  - Client Risk
  - Third-Party Provider Risk
  - Asset Protection Risk
  - Execution, Delivery and Process Management Risk
  - Data Security Risk
  - Information Technology Risk
  - Digital Assets Risk

- Other key risk categories:
  - Credit Risk
  - Liquidity Risk
  - Systemic Risk
  - Geopolitical Risk

Key Points of Note

The following key points should be noted when reading this document:

- This report covers risks that are specific to the Securities Services value chain, which includes trade capture, clearing and settlement, safekeeping, asset servicing and related services. It does not look to address any risks outside of Securities Services in areas such as issuance and investment decisions
- Whilst the report is focused predominantly on the Securities Services functions and the risks for Securities Services participants, perspectives for other parties in the Securities Services value chain are also included where appropriate
- A glossary of high-level key terms and definitions is provided in the Appendices

Target Audience

This report is intended to introduce the processes and risks inherent in the Securities Services value chain. Its objective is to be a comprehensive overview that is educational in nature and provides a good introduction of Securities Services terminology, the participants, the functions and – of course - the risks. It will be of interest to the following:

- Asset lifecycle participants including Issuers, Asset Managers, Securities Services Providers (such as Custodians and Financial Market Infrastructures), Third-Party Providers (such as technology providers and outsourcers) and - potentially - industry associations and Regulators
- Those who are entering the Securities Services industry – as well as existing industry employees – who are seeking to broaden their understanding of the Securities Services environment

Acknowledgements

This report is the result of efforts by a team of experts drawn from ISSA, that participated in the Securities Services Risks 2025 Working Group (WG). This included Operating Committee members and other ISSA member firms. The names of the firms that have participated in creating this report are provided in the Appendices. The ISSA Executive Board wishes to thank the WG members for their contributions as well as their firms for having enabled their participation.

Section 2: Context

1. Introduction to Securities Services

1.1 Introduction

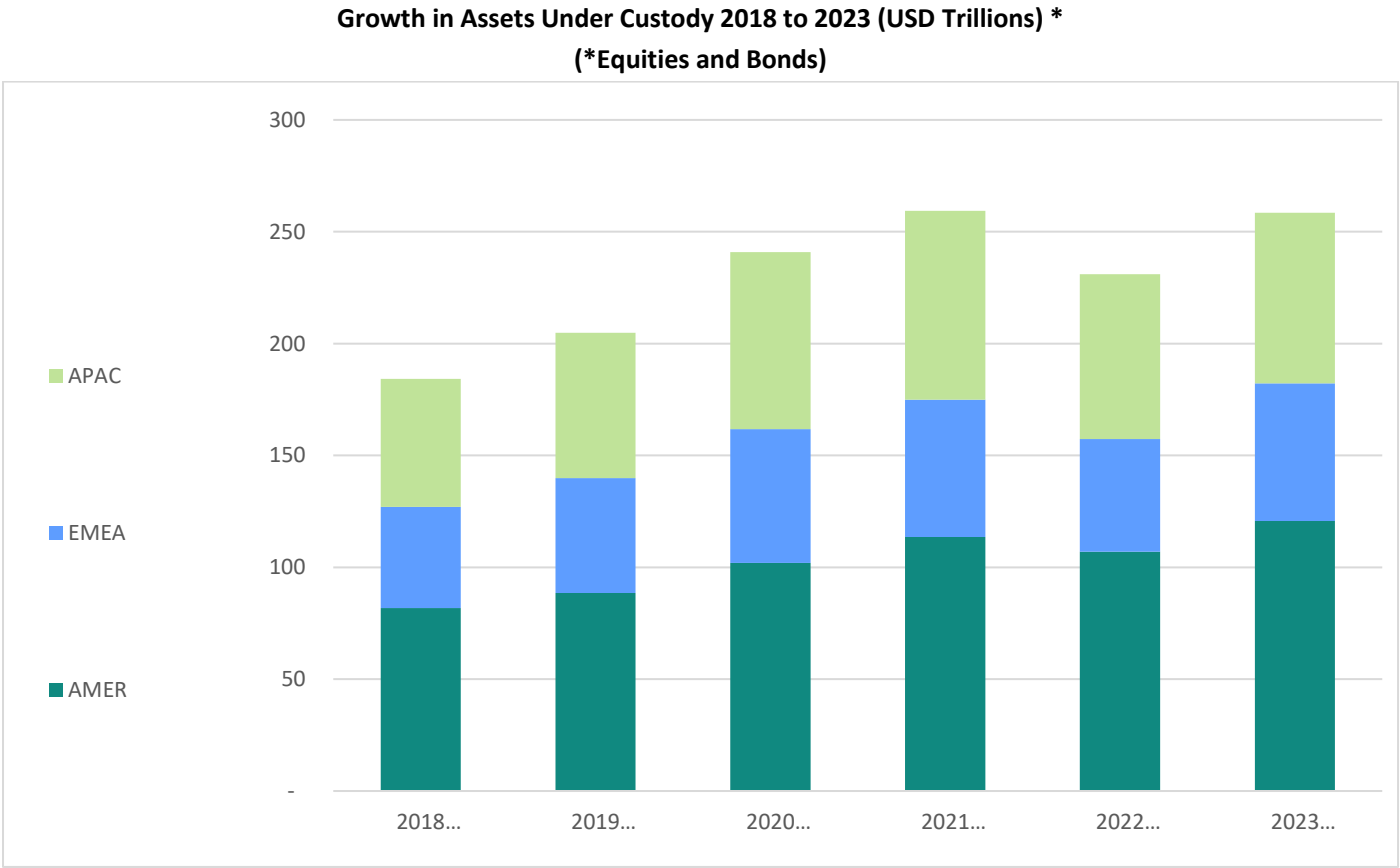
In this chapter, the term Securities Services is defined. The asset lifecycle is introduced and the Securities Services components highlighted. Additionally, the meaning of the term 'asset' is given.

1.2 Definition

Securities Services is a key component of the overall lifecycle of an asset. At its most basic, Securities Services (sometimes also referred to as post-execution or post-trade services) consists of trade capture, clearing and settlement as well as the safekeeping and administration of assets on behalf of Clients.

Securities Services has grown significantly in size and complexity, as financial markets themselves have grown. The following graph depicts the growth of Assets under Custody (AUC) from 2018 to 2023.

Illustration 1.2 Growth in Assets Under Custody Graph



Source: World Federation of Exchanges (WFE), Bank for International Settlements (BIS) and McKinsey analysis

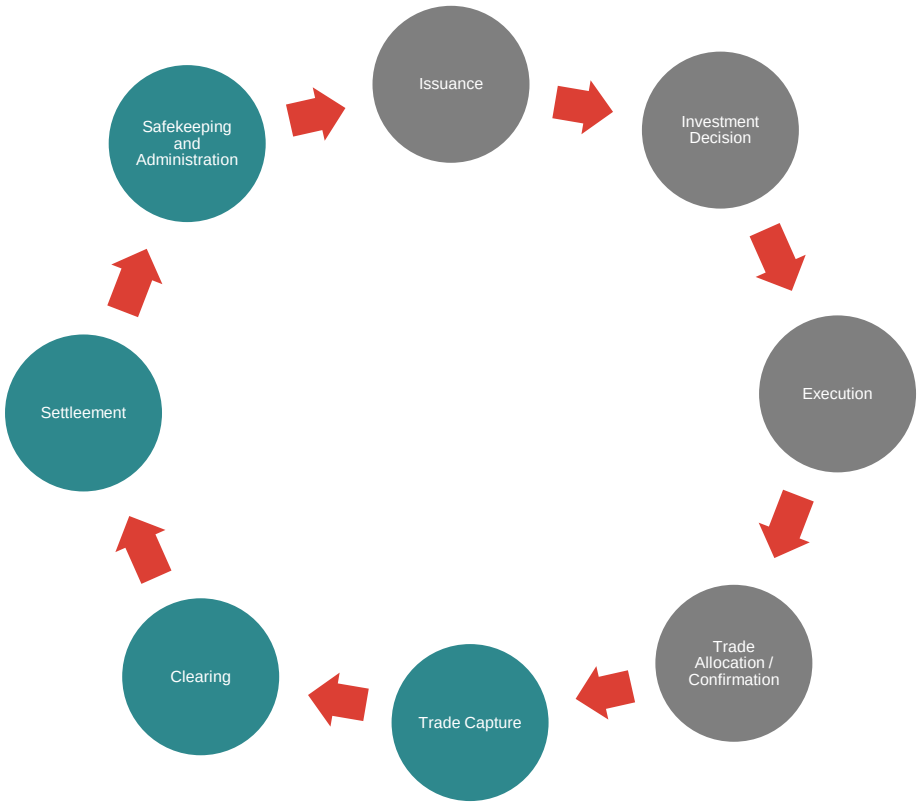
1.3 The Asset Lifecycle

The diagram below illustrates, at a high level, the lifecycle of an asset.

This document concentrates on the inherent risks within the Securities Services value chain. The Securities Services components of the lifecycle comprise the functions that are highlighted in green in the illustration below. These functions are trade capture, clearing, settlement and safekeeping and administration.

There are also additional components of the asset lifecycle - highlighted in grey in the illustration below. These are connected and provide information and support that are needed for the Securities Services components to operate but are not, themselves, Securities Services functions.

Illustration 1.3 Lifecycle of an Asset



1.4 Assets

An asset in the financial world (also known as a financial asset or financial instrument) is an asset that has value from a contractual claim or ownership right. There are many different types of financial assets and they can be held in various forms.

1.4.1 Asset Types

There are multiple asset types referred to throughout this document. The key categories, as defined by the Markets in Financial Instruments Directive (MiFID), include:

- Transferable securities (such as shares, depositary receipts and bonds)
- Money market instruments (such as certificates of deposit, commercial papers, treasury bills)
- Units in collective investment undertakings
- Derivatives (such as Futures, Options, Swaps, Forwards)

Note: This list is not exhaustive. Further information on financial assets, as defined under MiFID II, can be found at the following link: ANNEX I | European Securities and Markets Authority (europa.eu).

1.4.2 Asset Forms

Assets are held predominantly in electronic form but may also be held in different forms, such as physical certificates. The key forms are:

- Dematerialized Assets
  These are assets that are issued and held in electronic book-entry form only
- Assets that have been Immobilized
  These are assets that are issued in the form of paper certificates but have been immobilized (in a CSD) and therefore become available in electronic book-entry form
- Assets held as Certificates
  These are assets that are issued and remain in circulation as paper certificates. These assets are typically held by individual Investors or by Clients who will retain a Securities Services Provider to securely hold the assets in the vault of a Sub-custodian
- Tokenized Assets
  These are either a digital representation of the assets above or an asset that is only issued in a tokenized form (see Chapter on Digital Assets for more information)

In many markets, assets are now either completely dematerialized or immobilized. Dematerialization and immobilization improve efficiency and control, reducing the risk of loss, settlement failure and fraud.

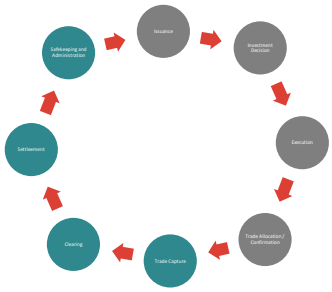
1.4.3 Asset Ownership

Asset ownership will be impacted depending on whether assets are registered or bearer securities:

- Registered Securities
  The ownership right / entitlement of the assets is maintained in the share or bond register of the Issuer company. Depending on the market, registration can be undertaken at nominee or at underlying Investor level.
- Bearer Securities
  There is no registration in the issuing company's books with the owner being whoever holds the bearer securities.

2. Asset Lifecycle Participants

2.1 Introduction



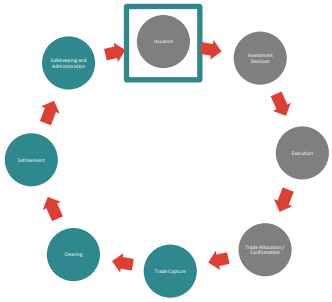
As can be seen in the illustration in Chapter I, there are many components to the lifecycle of an asset. In this chapter, the key participants are provided for each stage of the asset lifecycle and their roles and responsibilities are summarized.

2.2 Definition

Asset lifecycle participants are organizations or individuals that provide or utilize any of the components outlined in the lifecycle of an asset as outlined in the illustration in Chapter 1. These include the participants that are part of the Securities Services value chain as well as the participants that connect and interact with Securities Services participants.

The sections below outline the different asset lifecycle participants shown in the diagram above in sequential order. Sections 2.3, 2.4, 2.5 and 2.7 cover those participants that connect and interact with Securities Services participants whilst section 2.6 covers the Securities Services participants stage.

2.3 Issuer Services Participants



The first stage of the asset lifecycle is where the asset is created – known as issuance. The creation could be of a new asset or could be an addition to an existing asset. Participants in the issuance stage include the Issuer, Transfer Agent and Registrar.

2.3.1 Issuer

The creator of an asset is known as an Issuer. Issuers may be governments, companies or other parties who need to raise finance. The Issuer will look to sell the asset to Clients to raise the funds it needs. The Issuer is also responsible, on an ongoing basis, for ensuring that Investor disclosure rules are met.

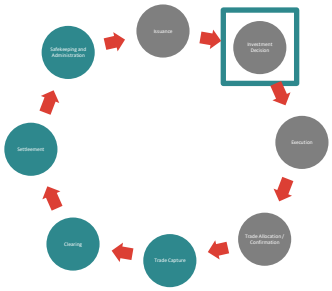
2.3.2 Transfer Agent

A Transfer Agent is a party appointed by a fund or the Issuer of an asset to issue and cancel fund units and securities in physical or dematerialized form, to reflect changes in ownership of the asset, to act as an intermediary for the Issuer and to handle interactions with its Investors regarding questions raised, such as lost or stolen securities and to process distributions.

2.3.3 Registrar

The Registrar is responsible for maintaining a registry of the Investors and number of securities held for a fund, bond or equity issuance and to ensure that the quantity of securities in circulation equates to the quantity issued. Registrar and Transfer Agency functions are often provided by the same entity.

2.4 Investment Decision Participants



The next stage in the asset lifecycle is the investment decision component. Investment decisions are made directly by an Investor or by an Asset Manager, that may be acting on their own behalf or on behalf of one or multiple Investors. For the purpose of this report, when an Investor or Asset Manager appoints a Trade Execution and / or Securities Services Provider, it is known as a Client.

2.4.1 Investor

An Investor is an individual or organization that invests in assets. An Investor may be the actual owner of the assets or be an intermediary holding assets on behalf of other Investors.

An Investor may be an institutional investor (e.g. a pension fund, a sovereign wealth fund, a hedge fund, a private equity fund or partnership, a bank (often holding assets for its underlying clients) or an insurance company) or it may be a retail investor. Where the Investor is the actual owner of the assets, it is known as the Ultimate Beneficial Owner (UBO). The term UBO has differing definitions according to different jurisdictions; for example, a UBO may be considered the party that has voting powers in certain markets.

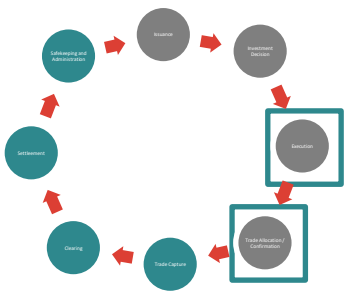
An Investor may make investment decisions itself or appoint an Asset Manager to manage its investment decisions - and become the Asset Manager's Client.

2.4.2 Asset Manager

An Asset Manager may be an Investment Manager (that focuses primarily on individual investments) or Fund Manager (that works with funds comprised of multiple assets which are often tailored to a particular market sector). An Asset Manager acts on behalf of an Investor and is appointed using an Investment Management Agreement (IMA) or similar arrangement. The IMA sets out the terms under which the Asset Manager is authorized to act on behalf of the Investor to manage the assets referred to in the Agreement. The IMA also establishes the extent to which the Asset Manager may act in a discretionary capacity to make investment decisions based on a prescribed strategy.

An Investor may appoint one or multiple Asset Managers depending on the assets under management and investment strategies. The Asset Manager(s) will interact with a Securities Services Provider on behalf of its Investors; for example by transmitting settlement instructions and receiving reports.

2.5 Trade Execution Participants



The next stage in the asset lifecycle is the trading of the asset. Assets can be traded on or off-exchange and by different trading - or Trade Execution - participants.

2.5.1 Broker Dealer

A Broker Dealer trades financial transactions on behalf of its Clients (Broker) or on its own behalf (Dealer). A Broker Dealer may be part of a firm that specializes in providing brokerage services or part of a larger

organization, such as a bank or Custodian. The Broker may provide Clients with access to trading platforms and, sometimes, Securities Lending services. Broker Dealers are authorized and supervised by local regulatory bodies.

2.5.2 Securities Broker or Prime Broker

Securities or Prime Brokers offer services to hedge funds and other professional Clients including securities lending, leveraged trade execution and cash management. A Prime Broker may also hold assets in custody on behalf of its Clients and act in the capacity of a Custodian. The Securities Broker may also provide Clients with access to trading platforms.

2.5.3 Stock Exchange

A Stock Exchange is a physical venue where Broker Dealers can buy and sell securities, such as stocks, bonds and other financial instruments. Most countries have a Stock Exchange (in some markets there are multiple exchanges). These exchanges are regulated by the local regulatory bodies.

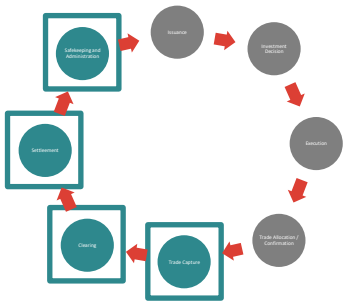
2.5.4 Other Market Utilities

There are multiple other market utilities including entities that provide industry trading and execution platforms. There are those that provide exchange data and connectivity as well as others providing securities reference and pricing data. Examples include:

- Electronic Communication Networks (ECNs)
- Alternative Trading Systems (ATSs)
- Multilateral Trading Facilities (MTFs)

2.6 Securities Services Participants

There are multiple participants involved in the next stage of the asset lifecycle which is referred to as Securities Services - or sometimes post-execution or post-trade services. These include Custodians, Financial Market Infrastructures (FMIs) as well as other participants that may be required depending on the services a Client needs. Throughout this document, these participants are referred to as Securities Services Providers.



2.6.1 Custodian

Whilst there are many ways in which an Investor / Asset Manager can hold assets, a common model adopted is one where a Custodian is appointed. The Investor / Asset Manager then becomes a Client of the Custodian, a term that is used throughout this report.

A Custodian is a financial institution which is authorized and supervised by the financial services / bank prudential regulator in its jurisdiction of establishment and / or where it offers its services. It is responsible for safeguarding the financial assets of a Client by holding the assets securely and, to the extent possible within its control, protecting the assets from loss whilst in custody. It is also responsible for processing and settling securities trades in all classes of financial instruments that are capable of being maintained in custody and servicing the associated portfolios whilst they are held in custody. In many ways the Custodian can be considered as an information intermediary, communicating between Issuers and Investors.

The relationship between a Custodian and a Client is governed by a custody agreement. This could be as simple as one bank appointing another bank as Custodian in one country or as complex as multiple fund managers acting on behalf of a Client covering services beyond traditional Securities Services. A Custodian may interact directly with a Client or take instructions on the Client's behalf from an Asset Manager. A Custodian's function, and scope of service, will depend on the Clients and markets which it covers.

To hold securities in a given market or jurisdiction on behalf of Clients, a Custodian must hold an account at the CSD or an International CSD (ICSD). This account is either held directly by a Global Custodian, where it has the capacity to do so, or by an appointed Sub-custodian. A Custodian, for the purpose of this report, refers to a Global Custodian and / or a Sub-custodian.

2.6.1.1 Global Custodian

A Global Custodian provides services with respect to securities traded in multiple markets or jurisdictions. It provides access to multiple markets to financial institutions such as banks, brokers and prime brokers as well as asset managers, fund managers, pension funds and other Clients. Global Custodians may provide services directly by holding an account at the (I)CSD or indirectly through using a number of Sub-custodians.

When portfolios are large, or diverse from a geographical or sector perspective, a Client may appoint a Global Custodian as agent and therefore benefit from having a single entity point of contact and expertise rather than having to liaise with multiple parties to provide the service (such as Sub-custodians, CSDs, tax agents, registrars, etc). By appointing a Global Custodian, a Client can take advantage of the Global Custodian's expertise and thereby ultimately reduce its Securities Services risk.

2.6.1.2 Sub-custodian

A Sub-custodian provides services with respect to securities traded in a particular market or jurisdiction. In addition to providing access to specific markets to financial institutions such as banks, brokers and prime brokers, a Sub-custodian may also provide services to a Global Custodian when the Global Custodian does not have an operation in a particular jurisdiction. A Sub-custodian is then sometimes referred to as an 'agent bank' and its relationship with the Global Custodian is governed by a Sub-Custody Agreement. In some instances, the Sub-custodian will be part of the same parent group of the Global Custodian.

2.6.2 Financial Market Infrastructure (also referred to as Financial Market Utility)

In the Securities Services industry, an FMI is a provider or operator which clears or settles securities between Securities Services participants. As an intermediary, a Custodian may access the FMIs directly through its own membership or indirectly through its Sub-custodian network. Further information on FMIs can be found via the Bank of International Settlements website: Principles for Financial Market Infrastructures (PFMI) (bis.org)

Examples of FMIs are CCPs, CSDs (see below for definition) and payment systems.

2.6.2.1 Central Counterparty

A Central Counterparty (CCP) - also called a Clearing House - exists in some markets and is able to operate cross-border in others. CCPs are typically used for stock exchange transactions, whereas 'over the counter' (OTC) transactions tend to route directly to the (I)CSDs via Custodians.

The CCP acts as the central counterparty for all clearing members. The CCP replaces one party's contract with another party by novation to a contract, with the CCP becoming the buyer to every seller and the seller to every buyer. The CCP is responsible for clearing (post-trade and pre-settlement), defining net-settlement obligations (where applicable) and assigning responsibility for undertaking settlement. Settlement occurs at the CSD following the clearing process at the CCP. In the event of a clearing member default, the CCP provides a performance guarantee for all obligations of the non-defaulting members by acting in the place of the defaulter.

2.6.2.2 Central Securities Depository

A Central Securities Depository (CSD) is a market infrastructure holding securities and enabling securities transactions to be processed by means of electronic book entry. The CSD typically operates a securities settlement system and provides central maintenance of securities accounts and/or notary functions. Depending on the market, a CSD may be privately owned or publicly listed. Some are operated by the national Central Bank. Others are part of a larger FMI group that may include Stock Exchanges and / or CCPs.

A CSD also provides central safekeeping and asset servicing (which may include the administration of corporate actions and redemptions) and plays an important role in ensuring the integrity of securities issues through reconciliation and similar controls which can also be mandated through local or regional regulations, such as the Central Securities Depository Regulation (CSDR) in the EEA. Securities can be held at the CSD either in physical (but immobilized) form or in dematerialized form (i.e. as electronic records).

The precise activities of a CSD can vary based on its jurisdiction and market practices (e.g. a CSD may be the official securities registrar and maintain the definitive record of legal ownership for a security in some cases but, in others, a different entity serves as the official securities registrar). Further, the activities of a CSD may vary depending on whether it operates in a jurisdiction with a direct, or indirect, holding arrangement or a combination of both.

At a high level, and regional differences aside, a CSD can act in different capacities:

- A Domestic CSD forms part of the national market infrastructure in the country where it is established and, depending on the market, can be both an Issuer CSD and an Investor CSD
- An Issuer CSD is the CSD in which securities are issued (or immobilized)
- An Investor CSD is a direct or indirect participant in the securities settlement system operated by another CSD in order to facilitate the transfer of securities between the participants of both CSDs
- An International CSD (ICSD) fulfils a dual role whereby it can be the Issuer CSD for international assets (e.g. Eurobonds) but can also settle eligible domestic instruments making it an Investor CSD

As FMIs, CSDs operate in a highly regulated environment. They are subject to national laws on securities issuance, settlement and safekeeping, while being supervised by the relevant authorities – typically the securities or banking regulator or national competence authority – and are generally subject to the oversight of the relevant central bank(s).

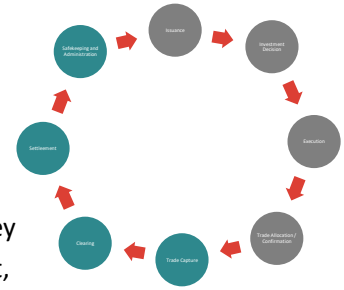
Notwithstanding this, CSDs are exposed to losses associated with their own errors/ omissions, fraud and costs associated with business interruptions. A CSD should therefore have clear and comprehensive standards, policies and procedures, and a similarly comprehensive and transparent governance and risk framework, to ensure that the securities it holds on behalf of its participants, and their clients, are appropriately accounted for on its books and protected from risks associated with the other services that the CSD may provide.

2.6.2.3 Central Bank

The Central Bank is the provider of Central Bank Money (CBM) for the settlement in the CSD. The CSD participants need to have an account either directly with the Central Bank or with a Settlement Bank that has such an account. In certain countries, the Central Bank may also act as, or operate directly, the national CSD for certain market segments (typically for government fixed income securities) and hold the record of ownership for these securities.

2.7 Other Asset Lifecycle Participants

Other participants, that are part of the asset lifecycle, include the Regulator, Third-Party Providers and Fund Services participants.



2.7.1 Regulator

A Regulator governs the operation of the financial market for the jurisdiction for which they are responsible. Whilst the remit and scope of a Regulator will vary from market to market, they often have a role to play in monitoring market conditions and stability and providing oversight. Within the Securities Services component of the lifecycle, Regulators set the rules by which market participants must operate, and may exercise their oversight responsibilities by, for example, taking feeds of data from CSDs and Custodians. In some markets, the entity acting as Regulator, such as a Central Bank, also plays a direct role in the operation of Financial Market Infrastructures (CCPs and CSDs).

2.7.2 Third-Party Provider

A Third-Party Provider is a specialist firm that offers external services to Securities Services Providers. Whist Third-Party Providers are an important part of the Securities Services landscape, it is imperative that there are contractual arrangements and service levels agreed to ensure that the service provision is clear and the risks are effectively managed.

Further information on the risks associated with Third-Party Providers can be found later in this report.

A specific example of a Third-Party Provider, in Europe, is the European Central Bank's Target 2 Securities (T2S) platform. The platform sits above multiple CSDs and Central Banks and provides a harmonizing layer to connect participants enabling cross-border settlement in central bank money.

2.7.3 Fund Services Participants

Funds Services describes the participants involved in providing services to a fund, which includes a Fund Administrator, Depositary / DepotBank and Transfer Agent (see Issuer Participant section).

2.7.3.1 Fund Administrator

A Fund Administrator is responsible for independently verifying the assets in a fund and valuing the fund on behalf of the Client (for a fund known as the Fund Manager). Its responsibilities include:

- Fund accounting
- Financial reporting
- Calculation of the Net Asset Value (NAV) of the fund
- Capital calls and distributions
- Oversight duties of certain operational functions to ensure the fund acts in accordance with applicable national law and fund rules

2.7.3.2 Depositary / DepotBank

A Depositary, or DepotBank, is appointed by certain types of EU domiciled fund to oversee the investments made into the fund. The funds requiring a DepotBank are Undertakings for the Collective Investment of Transferable Securities (UCITs) or Alternative Investment Funds (AIFs). The DepotBank has a strict restitution liability for lost assets subject to certain external event carve outs. Its responsibilities include, but are not limited to:

- Safekeeping and recordkeeping duties
- Cash flow monitoring
- Oversight duties of certain operational functions to ensure the fund acts in accordance with applicable national law and fund rules

3. Securities Services Functions

3.1 Introduction

To provide context and aid understanding of the Securities Services' component of the asset lifecycle outlined in Chapter 1, this chapter describes the core functions and utilities - as well as other additional services – that are Securities Services functions. Further detail about the risks involved in these functions is provided in the subsequent Risk Section.

3.2 Definition

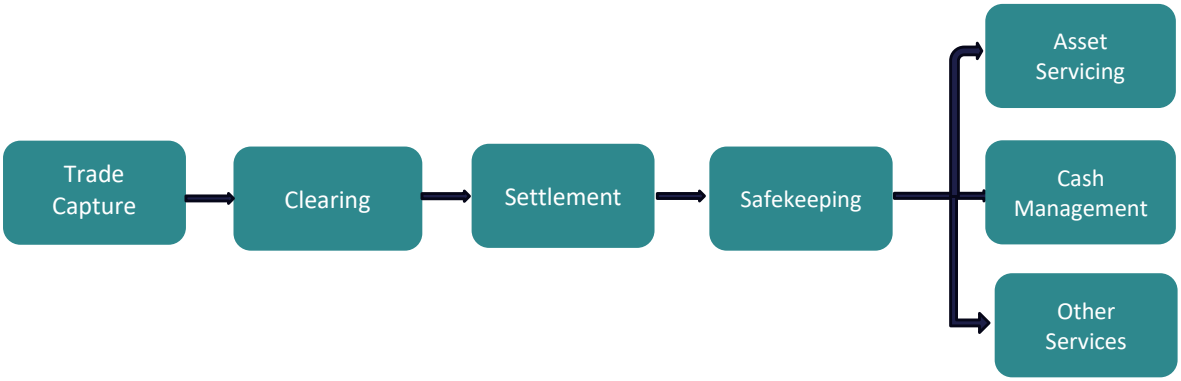
Securities Services functions are the different business areas of a Custodian, or other Securities Services Provider, that provide services to a Client. These comprise the core functions - which are utilized by most Clients utilizing a Securities Services Provider - as well as additional services which are optional but may also be of interest to a Client. There are also a number of utilities that are required to support the overall service offering.

3.3 Securities Services Functions

As shown in the asset lifecycle, the lifecycle of an asset comprises multiple components, a number of which are Securities Services related. The diagram below illustrates, at a high level, the core Securities Services functions. This diagram will be referenced throughout this report.

The Securities Services functions provide multiple layers of intermediation between the Issuer and the underlying Investor. Each layer constitutes a participant whose services and risk profile will very much be dependent on the Client base. The diagram should be considered from the perspective of both the purchase and sale of assets.

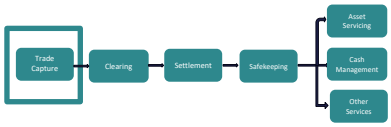
Illustration 3.3 Core Securities Services Functions Diagram



3.4 Core Securities Services Functions

Below are outlined the core functions that make up the Securities Services service offering.

3.4.1 Trade Capture

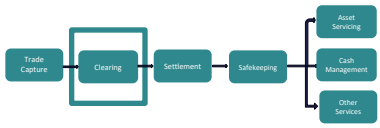


Trade, or instruction, capture is the first function in the Securities Services diagram and is the process whereby the Securities Services Provider receives an instruction from its Client (or Trade Execution participant)) to 'settle the trade' on their behalf.

As explained above, a Client typically accesses markets through a Broker, who helps a buyer find a seller and a seller find a buyer. For trades between a Client and a Trade Execution participant, a single transaction may be 'allocated' across multiple different accounts. This effectively results in multiple different transactions to be settled between both trading parties, both of which will instruct settlement instructions through the Securities Services Provider to the CSD for settlement.

The generation and transmission of the settlement instructions is a crucial 'first step' in the settlement process as it introduces the trade to the Securities Services Provider for matching and – ultimately - settlement.

3.4.2 Clearing



Clearing is an optional step - between trading and settlement - whereby certain transactions are processed together, typically on a clearing venue (although Over The Counter flows can also be committed for clearing). Clearing takes place at a CCP, which becomes the buyer to every seller and the seller to every buyer.

Clearing amalgamates multiple trades – a process referred to as 'netting' - to form one of the following:

- A single 'netted trade' i.e. the net of all purchase trades and all sale trades for a single security
- An aggregate of all purchases and an aggregate of all sales in a single security

Netting is an economical and efficient process but does require robust risk management.

Organizations that take part in the clearing process are known as clearing members. Clearing members act as the counterparty to any trades they clear. They can act in two different capacities:

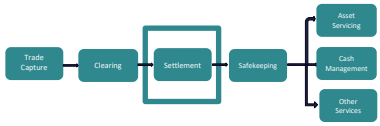
- on their own behalf for proprietary activity as a Direct Clearing Member (DCM)
- on behalf of a Client as a General Clearing Member (GCM)

In both cases, clearing members act as the counterparty to the trade. Therefore, when a Securities Services Provider is a clearing member and acting in a GCM capacity, it assumes the primary risk for the trade of its Client. As such, the Securities Services Provider is exposed to multiple risks associated with clearing including credit, market and operational risk and ultimately insolvency risk should the Client default. Sub-custodian network managers will have ongoing oversight of their CCP network.

The CCP protects itself by holding initial margin from both the buyer and the seller to ensure that downward changes in value are covered. It marks to market daily to ensure that both parties are able to fulfil their obligations. Additionally, the CCP can initiate buy-ins which is a mechanism to cover settlement fails. The CCP will source the security that is failing from another source, cancel the original trade and settle with the new security. Any costs of the buy-in are taken from collateral

provided by the GCM. Where the CCP holds securities as collateral it, would then appoint a Custodian to provide collateral management services.

3.4.3 Settlement



Settlement is the movement of securities between the receiving and delivering party. Most commonly associated with being the means to conclude a trade (i.e. the purchase and sale of securities), settlement can also be a movement effected between two different accounts held by the same account holder often referred to as inventory management. Whilst many Securities Services Providers facilitate the settlement process, settlement typically takes place in the securities settlement system of the (I)CSD where the transfer of title - and subsequent record of ownership - occurs through the central settlement of securities, either against or free of payment.

Settlement refers to the process of transferring the ownership of securities from the seller to the buyer. Settlement may be 'on exchange' or 'off exchange'. Settlement is usually against cash which is referred to as Delivery versus Payment (DVP) or Receipt versus Payment (RVP). However, the settlement may also be free of payment.

3.4.3.1 Settlement of On-Exchange Transactions

On-Exchange settlement benefits from the supervision and rules of the Stock Exchange and market transparency and is often supported by settlement in conjunction with a CCP. For CCP transactions, the Stock Exchange sends all orders for verification to the Client via a clearing member (usually either a Broker Dealer or Custodian). The clearing member is obliged to settle all trades at the end of each day on a net basis with the CCP and supports this obligation with appropriate levels of eligible collateral.

Organizations that are not clearing members need to find a Third-Party Provider to provide clearing services (usually a Custodian). The Third-Party Provider is responsible for clearing all on-exchange trades of their Clients and will ask for suitable collateral from their Clients to support their settlement obligations.

3.4.3.2 Settlement of Off-Exchange Transactions

Some securities are not suitable for on-exchange settlement, due to illiquidity or the level of credit risk they pose and are therefore settled off-exchange. Examples include illiquid stocks, hard to value transactions and some securities that are Issuer specific may not be eligible due to their perceived lack of market liquidity should a trade failure take place.

The settlement of Off-Exchange trade will normally take place between two Securities Services Providers using their accounts at the (I)CSD. This could be either on a delivery versus payment (DVP) or receipt versus payment (RVP) basis or may be free of payment (e.g. when the currency is not supported by the (I)CSD).

3.4.3.3 Delivery versus Payment Transactions

The Bank of International Settlement (BIS) wrote a paper on DVP settlement models which describes the three DVP models used by Securities Services providers Delivery versus payment in securities settlement systems - Oct 1992.

The three models are outlined below:

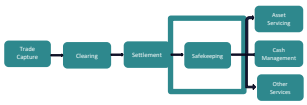
- Model 1: This refers to a system that settles transactions for both securities and cash on a trade-by-trade (gross) basis, with final (unconditional) transfer of securities from the seller to the buyer (delivery) occurring at the same time as final transfer of cash from the buyer to the seller (payment)
- Model 2: This is a system that settles securities transactions on a gross basis with final transfer of securities from the seller to the buyer (delivery) occurring throughout the processing cycle, but settles cash transactions on a net basis, with final transfer of cash from the buyer to the seller (payment) occurring at the end of the processing cycle
- Model 3: This is a system that settles transactions for both securities and funds on a net basis, with final transfers of both securities and cash occurring at the end of the processing cycle

Model 1 is preferred, from an Investor and European markets' basis, as it reduces the chance of any default impacting the settlement of a transaction. However, all three models exist within developed markets.

3.4.3.4 Free of Payment Transactions

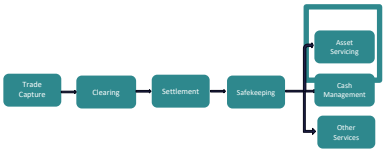
The most risk-intensive settlement is when securities are delivered to a counterparty 'free of payment'. This is a transfer of title without consideration. This type of settlement is kept to a minimum for obvious reasons but may be deployed in the issuance of new securities where payment takes place before delivery or when an account transfer from one provider to another needs to be executed. Extra caution needs to be exercised as any incorrect delivery may be hard to recover and will create full liability should the transaction be invalid. A delivery free of payment carries inherently higher risk of fraud as no value is exchanged in return for the securities.

3.4.4 Safekeeping



The holding of securities owned by a Client is referred to as Safekeeping. Assets are typically - although there are still exceptions - safekept in dematerialized electronic or immobilized form. They are held in the Issuer (I)CSD in the form of entries in the name of the Client or its nominee recorded in the Issuer's register. This service may be provided in a single market or across multiple markets. The assets are held, serviced and monitored under the asset protection regimes of the initial contracting Securities Services Provider's jurisdiction, the location of holding or of issuance, but also adhering to regional and global regulatory requirements.

3.4.5 Asset Servicing



The servicing of a Client's assets, commonly known as Asset Servicing, typically includes:

- Corporate actions (e.g. rights issues, stock splits)
- Proxy Voting
- Class Actions
- Income processing (e.g. dividends, interest /redemptions)
- Tax services (e.g. tax withholding and reclamation)

3.4.5.1 Corporate actions

A corporate action is an event initiated by the Issuer of a security, giving rise to a right in favour of the Client. For the Securities Services Provider, the corporate action servicing of a Clients' assets is often considered one of the highest risk processes due to the opportunity for error and the impact of the error given the market price differential often seen with corporate action events. As a consequence, the operating model is often designed to ensure that automation and Straight through Processing (STP) exists to ensure accuracy so reducing the risk of misinterpretation and failure to meet timelines.

A corporate action may be mandatory (e.g. such as stock splits, merger and acquisitions and cash dividends) or voluntary (e.g. tender offers, rights offers, buy-backs and conversions). A Securities Services Provider is exposed to increased operational risk where a corporate action is voluntary as an instruction is required from a Client.

- Mandatory Event
  For a mandatory corporate action, the Client does not have to take any action and has no choice whether to participate when the Issuer initiates the event.
- Voluntary Event
  Voluntary events are exercised at the discretion of the Client who has the option to elect their choice by sending an instruction, or to take no action, which will leave their securities unaffected. Mandatory events with options are also possible, whereby there are choices for the Investor to make by sending an instruction, but there will be a default option that will be applied if no choice is made.

3.4.5.2 Proxy Voting

Proxy voting services provide Investors with notification of situations advised by the Issuer whereby the Investor is requested to vote. A Securities Services Provider – either directly or through an agent - will ensure that the Investor's voting intentions are advised as required.

3.4.5.3 Class Actions

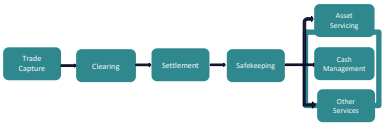
The class action service of a Securities Services Provider includes collecting proceeds of specific class actions and remitting these to a Client. As the results of class actions can often take a prolonged period to finalize, it is important the Securities Services Provider to has records of the Client's SSIs even if the custody agreement has lapsed. The Client should ensure that these are kept up to date as there is a likelihood that these will change over the often-extended period it takes for the class action to settle.

3.4.5.4 Income Processing

A Securities Services Provider may offer a tax service which facilitates a Client receiving a tax reduction on the corporate action and income received consistent with the applicable tax treaties and their tax status. Dependent on the market, the tax service may be provided through a tax relief at source model or via a tax reclaim process.

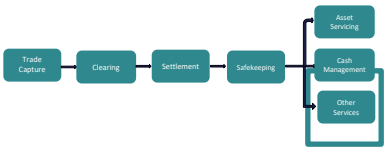
3.4.6 Cash Management

A Securities Services Provider often provides cash account facilities to support the movement of securities and asset servicing related monies. These services may include credit facilities to support intraday liquidity and Foreign Exchange (FX) capabilities.



FX services are often required to repatriate foreign currency proceeds (in relation to receipt of proceeds from the sale of securities, maturing redemption, income / dividend and tax reclaim) to the Client's base currency or to fund settlement of receipt of settled transactions or corporate actions. The ability to access FX currency can be restricted (currency controls) based on market rules and on occasion as a result of governmental actions. A Securities Services Provider's market intelligence can provide a Client with details of these as they become known.

3.5 Additional Services



In addition to the core Securities Services functions, a Client may also require additional services such as Securities Lending, Collateral Management, Investment Accounting and / or Fund Administration services. These services are typically offered from a menu of services by a Securities Services Provider, or a related entity, to the Client and are priced accordingly.

3.5.1 Securities Lending

The transfer, on a temporary basis, of assets owned by a Client to a borrower is known as Securities Lending. In return, the borrower either transfers other assets or cash to the Client as collateral or pays a fee.

3.5.2 Collateral Management

Collateral Management is where collateral is given from one counterparty to another as security for a credit exposure.

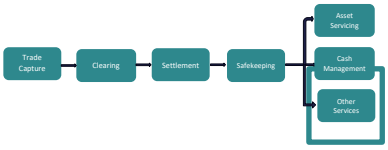
3.5.3 Investment Accounting

An Investment Accounting service, in its broadest sense, comprises the calculation of the portfolio's value (NAV), provision of compliance measurement, performance measurement, risk analytics and reporting services to a Client so that it can better understand and analyze how well its portfolios are performing.

3.5.4 Fund Administration

A Fund Administrator provides accounting services to Clients that are investment funds, such as mutual funds, hedge funds, pension funds and private equity funds. Fund Administration services include net asset value (NAV) calculations, investment compliance, regulatory and financial reporting. The Fund Administrator sits between the Asset Manager and the Investors in the fund and is responsible for independently verifying the assets and value of the fund.

3.6 Securities Services Utilities



As well as the core Securities Services functions, and additional services, that will be provided to a Client, a Securities Services Provider may also need to provide a number of utilities to support the different functions. These include the services outlined below.

3.6.1 Due Diligence

Due Diligence is core to the safe and efficient operation of the Securities Services lifecycle. As such it underpins all of the functions from the outset and is fundamental for transparency and asset protection. Further information on due diligence is provided in the Risk Section in the chapters on Client Risk and Third-Party Provider Risk.

3.6.2 Reconciliation and Reporting

Required at every stage of the Securities Services lifecycle, reconciliation is a fundamental control and effectively serves as a 'handshake' between the different participants. Reconciliation will occur at multiple stages during the Securities Services lifecycle, both pre- and post- settlement, including position and transaction level reconciliation.

The Securities Services Provider will also provide reporting to ensure that the Client has up to date information on both their transactions and positions. Ultimately a Securities Services Provider will ensure that the assets under custody (AUC) correspond to the required FMI records as a standard base-line business operation. This will, in the first instance, be at position level for each security and then, depending on the account structures applicable to particular holdings, at the Investor level.

3.6.3 Technology, Solutions and Interfaces

A Securities Services Provider will often provide the technical access to multiple FMIs, including CCPs and (I)CSDs. It will also frequently provide access to Trade Execution Participants (e.g. brokers) where execution services are offered. By connecting to a single Securities Services Provider, a Client will be able to reduce its system interface and development requirements by leveraging the Securities Services Provider's network and connectivity.

4. Account Structures

4.1 Introduction

Account structures for safekeeping assets – both securities and cash - vary throughout the Securities Services value chain. The structures are governed by factors such as mandatory requirements within the market and commercial or business onboarding decisions. In this chapter, an explanation of both securities and cash account structures that may be adopted by a Securities Services Provider is given. The different securities and cash account structure options are outlined, along with the key points that a Securities Services Provider – and potentially a Client – will need to consider when setting up an account structure.

4.2 Definition

An Account Structure is how an account is set up by a Securities Services Provider. Key securities account structures include omnibus accounts and segregated accounts (either at Sub-custodian and / or CSD level). Additionally, there are different naming conventions for accounts including the use of Nominees.

4.3 Securities Account Structures

Securities account structures vary globally and throughout the Securities Services chain. The variance can be due to a number of factors, such as:

- Regulation and / or law
- Market practice
- Commercial or operating preference of the intermediaries in the chain
- Investment markets
- Type of securities
- Domicile of the Investor

Common securities account structures offered by Custodians include:

- Omnibus account (where there are assets of multiple Investors together)
- Segregated account (where assets are split either at Sub-custodian or CSD level)
- Nominee account (where the assets may be held in an omnibus or segregated account but are registered in the name of a nominee)

Further information on the different securities account structures are provided below.

4.3.1 Omnibus Account Structure

An omnibus account is an account opened in the name of a Custodian either at Sub-custodian or CSD level. The positions held will belong to multiple Clients of the Custodian. In some jurisdictions, whilst omnibus accounts are permitted, regulations dictate that segregation of the Clients and the Custodian's propriety assets is required at the Sub-custodian and CSD. Even in jurisdictions where comingling of Client and proprietary assets is allowed, best practice should be to ensure they are segregated.

To ensure the safety of the assets, a Custodian will typically be obliged to maintain accounts in its own books recording the individual ownership interest of each Client in respect of the securities held in the Custodian's omnibus account.

Omnibus account naming conventions are also intended to ensure appropriate asset protections are maintained for Clients.

4.3.2 Segregated Account Structure

In some markets, regulation – or local market practice – means that segregated account structures are utilized. There are two different types of segregation that may be adopted:

- Segregated Account at Sub-custodian Level
  This account structure constitutes the holding of securities in the Ultimate Beneficial Owner (UBO)'s individual account at the Sub-custodian or, in some jurisdictions, in a trust account known as an Intermediate Beneficial Owner (IBO). Although accounts are segregated within the books of the Sub-custodian, segregation at the UBO or IBO level is not replicated or maintained at the CSD level where an omnibus account is still used (for example in the name of the Sub-custodian). This omnibus account will, however, be segregated from the Sub-custodian's proprietary assets.
- Segregated Account at CSD Level
  Under this type of segregation, securities are held in an individual account in the name of the UBO or IBO in the books of the Sub-custodian and the CSD. One of the main benefits of this type of structure include increased asset ownership transparency throughout the chain.

Different perspectives exist in respect to segregated account structures. Multiple and diverse market practice and laws exist which means there is no consistent global or regional model. Until further legal guidelines or revision of securities law exist, or further reform and regulation is mandated, segregation is often seen in some jurisdictions - and by certain actors including regulators - to be a good approach to mitigate legal risk. However, segregated accounts may be, operationally, less efficient.

4.3.3 Nominee Account Structure

A nominee is typically a company created for the purpose of holding securities on behalf of a Client. It holds the securities in trust for one or more Clients and often only the nominee company is identified on the shareholder register. A Custodian will establish one or more nominee companies to hold securities for their Securities Services Clients.

The use of nominee accounts provides the Custodian the opportunity to ease the operational burden of asset servicing. However, the use of a nominee will result in additional information requests to identify asset ownership.

Registering securities in the nominee's name segregates Client securities from the Custodian's assets, thus reducing the Client risk linked to insolvency of the Custodian (for example, a claim from the Custodian's creditors). However, the nominee account is not recognized in many markets, where the nominee would be seen as the legal owner and UBO of the securities held in the account.

4.4 Cash Account Structures

Cash account structures may also vary by market and currency. The structure may also be mandated by market requirements and / or regulations. Cash accounts may be provided to a Client by a Custodian and / or a CSD.

Where currencies are held on the balance sheet of the Custodian, either omnibus or segregated accounts may be possible. However, in markets where the currency is not held on the Custodian's balance sheet (e.g. for certain restricted currencies), segregated accounts may be a more common structure.

4.4.1 Custodian Cash Account Structures

Custodians provide Clients with cash accounts to support the movement, management and monitoring of cash positions associated with securities transactions (known as delivery versus payment or DVP transactions). In order to do so, the Custodian may hold the currencies on or off its balance sheet.

- On balance sheet

  The Custodian will open and operate, in its books and records, a cash account on behalf of the Client for each currency held on its balance sheet (sometimes known as an on-book currency).

  The Client is thereby taking on the risk for possible insolvency loss of the deposit. In this example the Client has credit counterparty risk to the Custodian.

- Off balance sheet

  In certain markets, the Custodian will maintain a currency off its balance sheet (known as an off-book currency). This may be because it is not possible to hold the currencies on balance sheet (i.e. for restricted currencies) or it is not desirable (e.g. for improved cut-off times or deadlines in the market).

  In these circumstances, the Global Custodian will open cash accounts with a Sub-custodian in the currency's local market on behalf of the Client. The risk for insolvency loss of the deposit will be with the Sub-custodian. In this example the Client has credit counterparty risk to the Sub-custodian which will be covered in the Client's contractual arrangement with the Global Custodian.

4.4.2 CSD Cash Account Structure

CSDs will operate with banks - including Central Banks - to perform the movement of cash related to CSD settlement activity and/or asset servicing. The CSD cash account structure should be designed to provide maximum certainty in relation to the finalization of the cash settlement of securities transactions.

Cash movements in a CSD can be either in central bank money or in commercial bank money.

- Central Bank Money

Central bank money refers to cash held in accounts at the Central Bank. When the cash leg is settled in central bank money, the transaction is recorded in the books of the Central Bank. This means the buyer's and seller's accounts at the Central Bank are debited and credited, respectively. Settling in Central bank money minimizes counterparty risk because the Central Bank is the ultimate guarantor of the cash. This ensures a high level of trust and stability in the financial system.

- Commercial Bank Money

Commercial bank money refers to cash held in accounts at commercial banks or CSDs with a banking license. This cash is essentially a deposit that can be used for securities transactions. When the cash leg is settled in commercial bank money,

the transaction is recorded in the books of a commercial bank or the CSD. This involves debiting and crediting the buyer's and seller's accounts at the commercial bank. Settling in commercial bank money carries higher counterparty risk compared to central bank money. This is because the commercial bank or the CSD, unlike the Central Bank, can potentially default.

CSDs generally operate central bank money accounts in the currency of their jurisdiction. Foreign currencies are generally operated through commercial bank money accounts.

Section 3: Securities Services Risks

5. Introduction to Securities Services Risks

5.1 Introduction

In this introductory chapter, a definition of risk is provided, along with an explanation of risk from a Securities Services perspective. Additionally, the key Securities Services risks are outlined and illustrated.

5.2 Definition

Risk, and more specifically financial risk, can be defined as the threat of loss or a negative impact.

The Basel Committee on Banking Supervision (BCBS) - the primary global standard setter for the prudential regulation of banks - considers Credit, Market and Operational risks to be the key risks for Banks to hold capital for. Of these prudential risks, Securities Services is predominantly exposed to Credit and Operational risk, with Credit risk largely intraday/short term in nature.

BCBS defines Operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. Within Operational risk, Basel guidelines recommend that every Operational risk is classified into one of seven categories (internal fraud; external fraud; employment practice and workplace safety; clients, products and business practices; losses to physical assets; business disruption; execution, delivery and process management).

The above taxonomy was adjusted to more clearly define how these risk categories apply to the Securities Services industry. The categories used in this report are as follows:

- Regulatory, Legal and Compliance Risk
- Client Risk
- Third-Party Provider Risk
- Asset Protection Risk
- Execution, Delivery and Process Management Risk
- Information Security Risk
- Information Technology Risk
- Digital Assets Risk

It is important to note, though, that the risk categories chosen are not exclusive; for example Third-Party Provider Risk covers business disruption and fraud risks. However, as these risks could occur at multiple junctures, it has been decided to include these within the different chapters where relevant rather than as a category of their own.

In addition to Operational and Credit Risk, Securities Services Providers also need to consider the following risk categories:

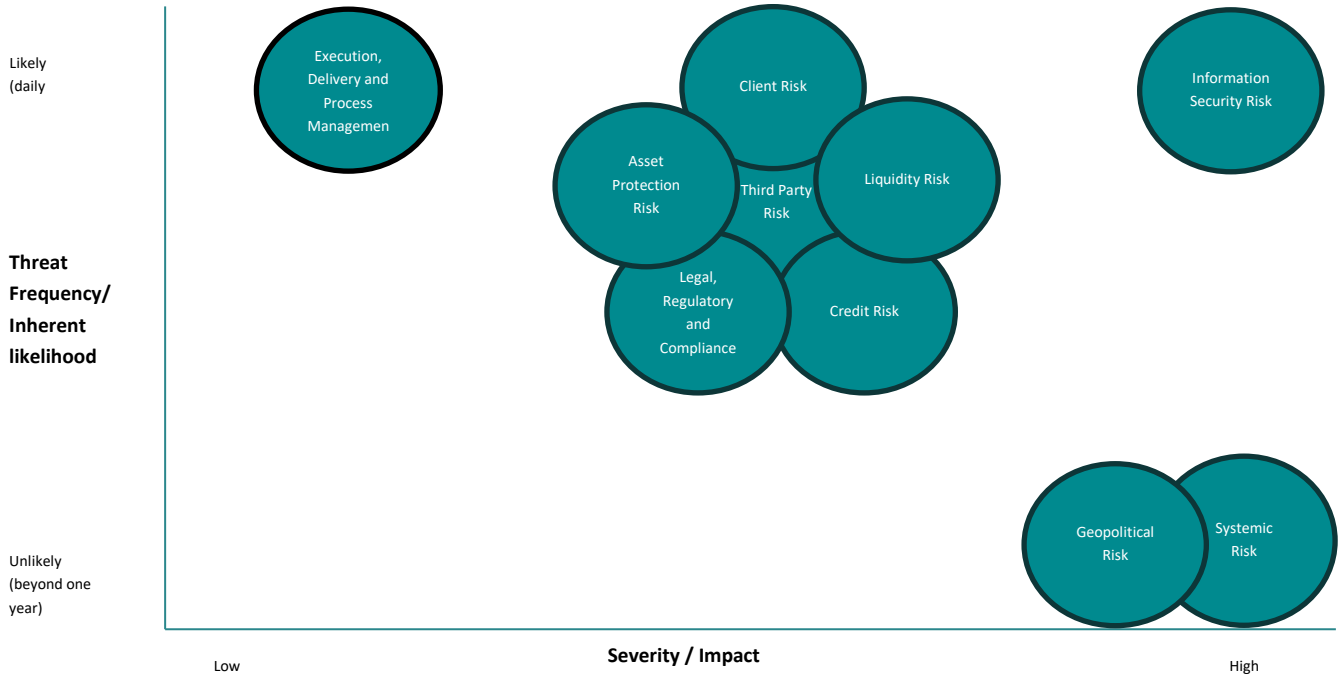
- Liquidity Risk
- Systemic Risk
- Geopolitical Risk

Within the Securities Services industry, market risk is largely a second order risk which may exist as a result of a first level risk such as operational risk materializing.

5.3 Key Risk Categories

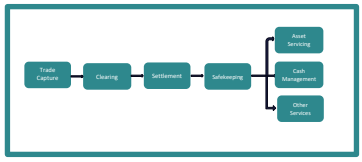
As outlined above, for participants in the Securities Services value chain, there are multiple risks to consider. The diagram below reflects the key risks categories from the perspective of threat frequency / inherent likelihood and severity / impact.

Illustration 5.3 Key Risk Categories Diagram



6. Regulatory, Legal and Compliance Risk

6.1 Introduction



Presenting itself at every stage of the asset lifecycle - and impacting all participants in the Securities Services value chain - the extent of regulatory, legal and compliance risks will vary. The risks may be based on several factors, including the participant's role, the types of assets held, the jurisdiction(s) and regulations in which participants and Clients are operating and the services involved.

This chapter looks to highlight key regulatory, legal and compliance themes and to discuss the risks and potential mitigants in the context of the Securities Services industry. It is, however, important that users of this report obtain up to date regulatory, legal and compliance advice relevant to their business.

6.2 Definitions

6.2.1 Regulatory Risk

Regulatory risk is the risk that a new, or change to existing, law and / or regulation will materially impact an organization. Regulatory risk may arise for a Securities Services Provider due to a failure to keep abreast of regulatory changes or by a failure to recognize the impact any new or change in law or regulation may have on its business and / or services. These failures could lead to strategic, reputational, financial, opportunity and operational issues and / or losses.

6.2.2 Legal Risk

Legal risk is the risk of legal action and / or losses occurring due to non-compliance with contractual-requirements. Legal risk may arise for a Securities Services Provider because of an unintentional or negligent failure to meet a contractual obligation. These failures could lead to litigation issues as well as financial and / or reputational losses.

6.2.3 Compliance Risk

Compliance risk is the legal, financial and criminal exposure as a result of non-compliance with existing applicable local, regional or international regulations and / or laws. Compliance failures can be institutional or arise from the actions of individuals. Compliance risk may arise for a Securities Services Provider leading to financial loss, legal issues and / or reputational damage.

6.3 Regulatory, Legal and Compliance Landscape

The Securities Services industry is subject to a complex regulatory, legal and compliance landscape. A Securities Services Provider must adhere to various regulations and guidelines to ensure that they are conducting their business in a safe and sound manner, complying with local, regional and global regulations and laws and protecting the interests of their Clients.

Below are highlighted the key factors that a Securities Services Provider should consider when looking at the regulatory, legal and compliance landscape as well as a table outlining the key legal protection and regulatory oversight regimes and standards.

6.3.1 Strategic Direction

A new, or change to a, regulation / law, may cause regulatory risk to arise, it may also impact the strategic direction that an organization takes. Regulatory change may offer an opportunity to innovate with market and product development. Conversely, a regulatory change may increase the costs of operating a business, reduce the attractiveness of investment and / or change the competitive landscape for Securities Service Providers.

6.3.2 Conduct

Conduct is a key area of regulatory focus throughout the Securities Services lifecycle and organizations need to have the appropriate processes in place to ensure compliance. Whilst there are many definitions, most conduct focus is on the behaviours and culture of an organization and its employees. Inappropriate conduct (for example due to improper execution of business activities, fraud or other such breaches of professional conduct) can impact Clients, the market or the firm itself.

6.3.3 Legal Agreements

The services that a Securities Services Provider performs are described in a contractual agreement which is entered into between a Securities Services Provider and its Client. A well-written legal agreement helps prevent potential disputes and legal issues. It can also establish trust between a Securities Services Provider and its Client, strengthen the relationship and may lead to additional business.

Contractual agreements must be in place and clearly define the parameters of the services offered and the expectations of each party. Such agreements are – for the most part - standard. They may be supplemented by Addenda - which further fulfil operating, legal and market practices of any given markets and/or services (e.g. settlement finality, collateral management, securities lending and insolvency definitions) as well as by a service level agreement (SLA) or similar document.

A Securities Services Provider and its Client may require the provision of certain protection clauses which would be inserted in accordance with local law and subject to the Securities Services Provider's risk appetite. Strict liability provisions, such as those required under UCITS and AIFMD, may also need to be considered and included in legal language to ensure regulatory conformance and transparency as well as definitions of liability.

It is vital in agreeing legal language that fair consideration is given as to where liability should lie, either with a Securities Services Provider, a Client or an external party. A Securities Services Provider should not be expected to bear all risks and losses and - as such - clear definitions of liability are required. Examples include not taking liability for the actions of Third-

Party Providers (third party choice may be limited by the investment choice of the Client rather than driven by the Securities Services Provider) and losses down to force majeure.

As Securities Services Providers are generally banking entities, capital adequacy assessments (and cost of capital) form part of the risk appetite and risk acceptance decision particularly in relation to liabilities and indemnities. Securities Services Providers must perform impact / probability vs revenue / reward assessments to influence risk acceptance or rejection decisions.

6.3.4 Asset Protection

Many jurisdictions have regulations and laws governing asset protection with the aim of preventing the loss of assets due to fraud, misappropriation, inadequate controls or insolvency. A critical factor in mitigating the risk of loss of assets is in understanding the law governing each agreement between different Securities Services Providers or between a Securities Services Provider and a Client as well as the current regulations / laws in the country where the Client activity is contracted. Interoperability and equivalence arrangements can ensure that protection levels in one jurisdiction are upheld in another to ensure that the cross-border transfer of ownership of securities does not result in unintended consequences.

6.3.5 Jurisdiction of Operations

Regulations and the implementation of regulations into local law vary from jurisdiction to jurisdiction and the regulatory environment is constantly changing. As such, it is vital that both Securities Services Providers and Clients are aware of the applicable rules in any given jurisdiction, to ensure that existing business models comply with current regimes, to keep abreast of changes to such rules, and to understand how these rules impact liability when operating in that jurisdiction.

For global organizations, understanding how the various regulations work together is also imperative. Each component of a product needs to be assessed looking at where and how it is delivered, breaking it down to component elements and then identifying where each element is delivered from.

6.3.6 Information Security

Data privacy and cybersecurity regulations and laws, require Securities Services Providers to implement measures to protect their Clients' personal information and assets from unauthorised access, theft or destruction.

6.3.7 Digital Assets

With the increased interest in digital assets, different regulatory, legal and compliance factors need to be considered. Regulators are adapting existing regulations to incorporate legal language covering digital assets as well as creating new frameworks and guidelines.

6.3.8 Sustainability

Sustainability - also known as Environmental, Social and Governance (ESG) - has become increasingly important to Clients over recent years. Securities Services Providers must be aware of, and address, this need. New ESG regulations require organizations to comply with applicable regulations and laws which may require integrating ESG factors into their investment decision-making processes to meet their clients' ESG objectives. Securities Services Providers may need to disclose information about their ESG policies and practices to Clients in order to promote transparency and accountability and Clients are often required to provide their Securities Services Provider with their ESG policies.

6.4 Legal Protection and Regulatory Oversight

Financial authorities are responsible for developing rules, guidance and other regulatory texts that provide minimum control requirements to manage the risks of their covered entities. In addition, these authorities also perform oversight of covered entities through their supervisory functions to measure adherence to these control obligations. Given the potential market impacts that may result from a Securities Services Provider's control failure, financial authorities provide stringent supervision of financial institutions that safekeep and manage client assets.

The following table summarizes prominent themes within the Securities Services value chain with examples of the key applicable regional and global regulations, laws and market standards as at the date of this report. (Note: This table is not exhaustive and national, as well as some regional, regulations are not shown).

Illustration 6.4 Legal Protection and Regulatory Oversight Table

Regulation Addressing	Regulations / Standards	Regulatory Requirements	Implementation Requirements
Conduct	▪ Basel Regulations ▪ EU Capital Requirements Directive (CRD)) VI and Capital Requirements Regulations (CRR) III ▪ EU Central Securities Depository Regulation (CSDR) ▪ US Volcker Rule ▪ UK Financial Conduct Authority (FCA) Conduct Rules ▪ US Securities and Exchange Commission (SEC) Business Conduct Rules ▪ Swiss Bank's Recovery and Resolution Directive ▪ IOSCO Client Asset Principles ▪ US Dodd Frank	▪ New rules for transacting with certain funds (inability to extend credit / segregation) ▪ Identify & manage critical economic functions ▪ Bail in / Stay protocols ▪ Cost of Business- capital requirements ▪ Central Governance and Supervision	▪ Enhanced Intra-day Liquidity management ▪ Enhanced credit monitoring processes ▪ Enhanced capital / stree test requirements. ▪ Supporting measures for Bail - in liabilities and obligations ▪ Enhanced risk and governance regime in segregation of duties ▪ Legal review
Asset Protection	▪ EU Undertakings for the Collective Investment in Transferable Securities UCITS ▪ Alternative Investment Fund Managers Directive (AIFMD) ▪ European Market Infrastructure Regulation (EMIR) ▪ CSDR ▪ EU Markets in Financial Instruments Directive (MiFID) ▪ UK Client Assets Sourcebook (CASS) ▪ SEC Safeguarding Rule ▪ IOSCO ▪ German Safe-Custody Act	▪ Laws governing client agreements ▪ Interoperability and equivalence arrangements	▪ Legal review of regulations / laws in different jurisdictions ▪ Operational requirements such as reconciliation, reporting and account segregation

Regulation Addressing	Regulations / Standards	Regulatory Requirements	Implementation Requirements
Client Due Diligence and AML / AFC	▪ Funds Transfer Regulation ▪ Anti Money Laundering (AML) Directive ▪ EU Market Abuse Directive ▪ US Foreign Account Tax Compliance Act (FATCA) ▪ Common Reporting Standard (CRS) ▪ ISSA Financial Crime Principles	▪ Enhanced KYC due diligence and ongoing client monitoring ▪ Enhanced controls for Omnibus accounts ▪ Third-country Equivalence	▪ Enhancements to message screening technology ▪ Additional messaging parameters to Identify beneficial owner ▪ Enhanced KYC controls/product & client suitability risk assessment
Operational Resilience	▪ EU MiFID ▪ EU Digital Operational Resilience Act (DORA) ▪ UK Operational Resilience Regulation ▪ CPMI-IOSCO Guidance on Cyber Resilience for FMIs ▪ Monetary Authority of Sginapore's Business Continuity Management ▪ Hong Kong Monetary Authority Supervisory Policy Manual OR-2 ▪ US Regulators FRB / OCC / FDIC Sound Practices to Strengthen Operational Resilience	▪ Increased due diligence and oversight of ICT (Technology) third party providers ▪ Minimum cyber controls and risk assessment activities ▪ Identification and mapping of the financial institution's critical operations and supporting third parties ▪ Defining Tolerance For Disruption (Impact Tolerance) for critical operations	▪ Review of contractual arrangements with internal and external ICT third party providers ▪ Review of current cyber programs used to assess ICT environment with minimum DORA control requirements ▪ Development and implemention of a framework to continuously enhance operational resilience for identified critical operations
Execution and Clearing	▪ Various Financial Benchmark Standards ▪ EU MiFID II / MiFIR ▪ EU EMIR ▪ EU Securities Financial Transaction Regulation (SFTR)	▪ Enhanced pre/ post trade due diligence ▪ Mandatory clearing of certain instruments ▪ Asset Segregation Rules ▪ Third-country Equivalence ▪ Increased Reporting	▪ Enhanced risk and control framework ▪ Disclosure / Choice of account structures ▪ Enhaced Liquidity / Collateral Mgmt. ▪ Real – time credit / margin management ▪ Client categorization, Know Your Client / Know Your Product controls
Settlement	▪ EU CSDR ▪ EU Target2-Securities (T2S) ▪ EU Settlement Harmonisation ▪ US and APAC T+2 Settlement ▪ SEC CASS	▪ Mandatory Fail Penalties / Buy – ins ▪ Authorisation of CSDs ▪ Asset Segregaration Rules ▪ Transparency of internal transaction	▪ Enhanced settlement siciüline controls ▪ Technology changes / connectivity ▪ Enhanced client performance monitoring ▪ Understanding of equivalence regimes
Safekeeping, Asset Safety and Funds	▪ EU UCITS ▪ EU AIFMD ▪ US Safeguarding Rule ▪ EU MiFID II Safeguarding ▪ UK CASS	▪ Asset Segregation Rules ▪ Liability / Indemnification regime ▪ Safekeeping of assets rules	▪ Review of legal protection clauses and liability indemnification ▪ New account structure / operating model and supporting controls
Asset Servicing	▪ EU Shareholder Rights Directive (SRDII) ▪ Various domestic voting regimes ▪ European Central Bank (ECB) Score Standards	▪ Client classification ▪ Increased reporting	▪ Enhancements to KYC controls
Tax	▪ US Financial Transaction Tax (FTT) ▪ EU WHT Harmonization Directive ▪ Various Certificate of Residency regimes	▪ Client classification ▪ Withholding tax requirements ▪ Increased reporting	▪ Enhancements to tax processes
Information Security and Data Protection	▪ EU General Data Protection Regulation (GDPR) ▪ US SEC Cyber Rule ▪ EU Agency for Cyber Security (ENISA) Cyber Framework ▪ EU Cybersecurity Act ▪ EU Digital Operational Resilience Act (DORA) ▪ EU Network and Information Security (NIS 1 & NIS 2) Directives	▪ Disclose material cybersecurity incidents	▪ Enhanced reporting and procedures ▪ Technology testing
Digital Assets	▪ EU Markets in Crypto-Assets (MICA) Regulation ▪ EU DLT Pilot regime ▪ Bank of International Settlements (BIS) Prudential Framework for digital assets ▪ IOSCO Policy Recommendations ▪ US Staff Accounting Bulletin (SAB 121) Regulation ▪ HKMA draft circular on digital assets ▪ Australia Treasury framework on digital assets	▪ Embody existing regulations adapted to cover digital assets	▪ Introduction of frameworks incorporating digital assets

Regulation Addressing	Regulations / Standards	Regulatory Requirements	Implementation Requirements
Sustainability	▪ EU Sustainable Finance Disclosure Regulation (SFDR) ▪ EU Corporate Sustainable Reporting Directive (CSRD)	▪ Dislosure requirements ▪ Increased reporting requirements	▪ Enhancements to operational and reporting processes

6.5 Regulatory, Legal and Compliance Risk Threats

As already mentioned, the regulatory, legal and compliance landscape is complex and there are multiple factors that Securities Services Providers need to consider. The following table outlines the key regulatory, legal and compliance risks and possible mitigants.

Illustration 6.5 Regulatory, Legal and Compliance Risk Table

Risk Description	Risk Mitigation
Securities Services Provider governing ineffectively	▪ Establish suitable internal senior management regime and compliance and risk strategy, to govern and ensure adherence to regulations and regulatory change requirements ▪ Implement a comprehensive suite of management reporting including, but not limited to: KRIs, KPIs and SLAs ▪ Arrange training to ensure that staff understand their responsibilities and the action and escalation requirements should a breach be identified
Active engagement regarding changes to regulations / laws not undertaken	▪ Scan the regulatory / legal environment for upcoming changes ▪ Complete initial impact analysis of potential changes ▪ Participate in regulator's consultation papers on new or proposed regulation ▪ Advocate / lobby legislators / regulatory bodies, either directly or through industry / trade associations
Preparation for changes to regulations / laws not managed	▪ Complete analysis of impact of regulatory / legal changes on current business model, operations, technology and clients ▪ Complete a 'risk vs return' assessment to ascertain the risk appetite of continuing to do business vs financial reward ▪ Review potential new product opportunities ▪ Involve operations, technology, product and business lines in preparing for change
Regulatory / legal changes not properly implemented	▪ Use risk framework tools such as Key Risk Indicators and Risk Control Self Assessments to assess project delivery risk, execution risk and business risk profile ▪ Implement metrics, including KPIs, to measure quality of implementation
Client and Third-Party Provider relationships not assessed	▪ Consider the information or data points required to comply with regulation at the outset of a client or third-party provider relationship and on an ongoing basis (e.g. MiFID client classification, sanctions rules, tax status)

Risk Description	Risk Mitigation
Appropriate terms not agreed with Clients and Third-Party Provider relationships	▪ Conduct a KYC 'Know Your Client' or KYP 'Know Your Provider' ▪ Complete a Product / Client Suitability & Appropriateness Assessment ▪ Review operational capabilities ▪ Complete a Capital Assessment and Credit Assessment ▪ Ensure regulatory considerations are met (e.g. UCITS / AIFMD / FATCA / VOLCKER / MiFID / DGSD) ▪ Put in place a legal agreement that covers liability and securities interest ▪ Agree Environmental, Social and Governance considerations
Change of legal title not completed in a timely manner (particularly for Securities Lending)	▪ Ensure legal documentation covers the ability to transfer title appropriately

7. Client Risk

7.1 Introduction

Client risk can occur when a Securities Services Provider, or a Client, have not undertaken the necessary measures to assess the suitability of the other party before commencing a relationship. The risks can also occur when the parties do not continue to monitor each other on an ongoing basis.

This chapter focuses on outlining Client risk and the measures that should be taken - by both Securities Services Providers and Clients - to ensure that this risk is mitigated. Measures, such as due diligence and Know Your Client, are explained and the key risk mitigants outlined. It should be noted that risks that require assessment at onboarding, such as Credit Risk or Information Security and Data Protection Risk, are also provided in detail in other chapters of this report.

7.2 Definition

Client risk refers to the risks to a Securities Services Provider associated with onboarding a new Client against selection criteria, as well as the risk of servicing that Client on an ongoing basis. It also refers to the risks to a Client of entering into and retaining a relationship with a Securities Services Provider.

7.3 Client Risk Landscape

Post the 2008 financial crisis, 'suitability and appropriateness standards' were enhanced by a number of global and regional regulators to enhance investor protection and create a safer, harmonized Securities Services market. At the forefront of these enhancements are measures that need to be taken by a Securities Services Provider to ensure that products and services are transparent and suitable for the Client and, equally, that the Client itself is assessed for its suitability by the Securities Services Provider. Additionally, regulations consistently demand improved transparency with new requirements for the Securities Services Provider. An example is mandating detailed information be sent to Clients disclosing costs and charges which must be evidenced with full description.

In recent years, there has also been increased attention and focus on sanctions enforcement and counter-terrorism measures. The complexity of the securities holding chains has led regulators to adopt new standards especially relevant to omnibus accounts which obscure the beneficial ownership of sanctioned parties through its 'layers'. A Securities Services Provider needs to ensure that KYC and suitability and appropriateness assessments delve into the prospective Clients' investor base and that, as a minimum, there are controls in place to complete these assessments on an ongoing basis.

7.4 Due Diligence

Due diligence is the process whereby an organization assesses another party through collecting and analyzing information on that party to ensure their suitability. For both Securities Services Providers and Clients, these measures

are key to mitigate client risk. The requirements of meeting the relevant measures imply the clear articulation of responsibilities, liabilities, disclaimers and disclosures in the contract.

Whilst due diligence is a critical part of the onboarding process, ongoing due diligence is also needed throughout the term of the relationship. Both Securities Services Providers and Clients will therefore need a robust control suite to monitor each other's performance and have the ability to freeze / limit activity should the other party show signs of difficulty, inappropriate behaviour or deterioration in their creditworthiness.

7.4.1 Securities Services Provider Due Diligence Responsibilities

A number of criteria must be fulfilled by a Securities Services Provider before a relationship is fully entered into with a Client in order to limit risk and exposure to the Securities Services Provider and also the possibility of contagion in the asset lifecycle. Measures should be assessed and agreed as part of a 'new business' approval process before business can commence between the two parties, as well as reviewed during the relationship.

Key due diligence responsibilities include, but are not limited to the following:

- Client Assessment
- Securities Services Provider Legal Entity Assessment
- Client Acceptance Process
- Environmental, Social and Governance considerations

Securities Services Providers also have a responsibility to assess their Third-Party Providers. See Chapter 8 for further information.

7.4.1.1 Client Assessment

The Securities Services Provider should take clear measures to assess each Client. This should include getting to know the Client - often referred to as Know Your Client (KYC) – as well as understanding the Client's knowledge and experience.

KYC requirements are a common and prevailing area of focus for global regulators. Indeed, KYC comes in many shapes or forms and there are many aspects to consider. The reputational and financial risks for Anti Money Laundering (AML) failures compound the pressure to ensure that KYC processes in initial and ongoing Client evaluations are watertight.

When completing KYC requirements, the following should be considered, but will not be limited to:

- Type of institution: Broker dealer / hedge fund / investment firm, etc.
- Credit strength
- Politically Exposed Persons (PEPs)
- Embargo list
- Management structure
- Client's country of domicile and any country specific KYC requirements (e.g. FATCA, Volcker, AMLD)
- Any restrictions in the intended market of business (e.g. domestic versus international market rules)
- Contractual expectations of the Client (consideration of exclusions to standard legal terminology and protection clauses vs risk appetite)

- The risk versus return the Client presents (margin and growth versus risk appetite)

Additionally, the Securities Services Provider must ask the potential Client to provide information regarding their knowledge and experience in order to be able to assess whether the service or product is suitable for the Client. Whilst - at the beginning - the implications may not be clear, the natural impact will be reputational risk and the potential for operational risk (loss, errors, litigation and regulatory breaches).

Areas of focus should include, but will not be limited to:

- Client Suitability
  - Establishing whether the prospective Client requires the standard service provided by the Securities Services Provider
  - The regulatory and legal framework e.g. country risk and enforceability of any provisions in legal agreements
  - Historical performance and compliance with regulatory and best practice standards
  - Any involvement in any breach of financial markets integrity, including market abuse, financial crime and money laundering activities
  - Reputation including client base
- Operational Capability
  - Intended trading strategy including volume, client base, market, trade type, products
  - Fit for purpose procedures and internal controls in accordance with prevailing regulatory and market standards
  - Operational and system capability vis à vis volumes and product complexity
  - Operational resources including technological interfaces/connectivity
  - Internal risk control systems
  - Contingency plans and recovery & resolution provisions
- Credit and Liquidity Suitability
  - Sufficient financial strength to support the proposed business, pre-fund and or obtain credit lines
  - Collateral requirements
  - Payment systems and arrangements that enable clients to effect timely transfer of assets/cash (as margin) required
  - Systems and/or access to information that helps Clients to respect any maximum trading limit

7.4.1.2 Securities Services Provider Legal Entity Assessment

Having undertaken an overall Client assessment, a Securities Services Provider must then assess the risk of a Client's business and understand whether the legal entity that it anticipates providing the services has adequate financial resources.

Factors for consideration include:

- sufficient capital for the risks (i.e. the extent to which cash will be required to be deposited or withdrawn from the bank's balance sheet and an assessment of the implications on capital usage)
- an understanding of the Client's liquidity needs
- an assessment of the operational risks

Operational risk capital is often determined based on a factor of the revenue received for providing the service or by modelling relevant external losses, internal losses and conducting risk-based scenario analysis.

It should be noted that certain Securities Services Providers – specifically large Global Custodians - have often been designated as Globally Systemically Important Financial Institutions (SIFIs). As a consequence, these organizations have greater regulatory requirements for financial stability including the need for higher capital requirements, increased liquidity requirements and higher requirements in terms of resolvability.

7.4.1.3 Client Acceptance Process

Following the comprehensive due diligence detailed above, a Securities Services Provider will typically have a decision-making process it needs to follow in accordance with its governance frameworks. This process, often referred to as 'business acceptance' will consist of pertinent information being presented for approval. Such processes should be formed by a balance of suitably senior and experienced representatives across various divisions (such as risk management, operations, compliance, business and finance) who will ensure that decisions are made fairly, without prejudice, and together with the appropriate legal entity approval. In the event that a decision cannot be met, exceptions might go to a more senior committee to achieve a decision. A specific deal approval process may also be practiced reviewing new business at an early stage.

7.4.1.4 Environmental, Social and Governance Assessment

Given the ever-increasing importance of Environmental, Social and Governance (ESG) when looking at the financial industry, a Securities Services Provider may wish - and in some markets is required - to ensure it assesses its Client against its internal ESG risk appetite. An ESG assessment may include reviewing names against databases that provide information on adverse ESG publicity and assessing links to industry segments associated with adverse environmental impacts. This assessment may stand alone or be part of a more formalized process, following a similar governance model as KYC reviews, to obtain approval.

7.4.2 Client Due Diligence Responsibilities

When selecting and appointing a Securities Services Provider, the Client itself has the responsibility to conduct its own due diligence. The Client also has the responsibility to fully satisfy itself and - in turn - satisfy the Securities Services Provider, that they understand the product(s) and the service(s) the Securities Services Provider is to perform.

An approach often used, when going through the process of selecting a Securities Services Provider is to utilize a request for proposal (RFP). This involves a review of the Securities Services Provider, their structure, their management, their reporting / control capabilities and the supporting service offering. Such a thorough assessment, which may be conducted under a non-disclosure agreement (NDA), is essential to ensure that the delegated / nominated party has the capability to support their business.

Areas of focus might include, but will not be limited to:

- Capital (ICAAP, Basel Pillar 3 public disclosure) assessing sufficient financial strength to support the Client's business
- Regulatory and legal framework and enforceability of provisions in legal agreements
- Disclosure of annual results, audit reports and control reports documented by the Securities Services Provider and then externally audited (such as SAS70 AS: SSAE16 and ISAE 3402)

- Governance framework including management and board structure
- Risk management policy and control framework; disclosure of policies and procedures
- Historical performance and compliance with regulatory and best practice standards
- Contingency plans and recovery and resolution provisions
- Reputation including client base
- Operational and system capacity and capability vis à vis volumes and product complexity
- Account structure including conformance with any segregation requirements

Any such requests of a Securities Services Provider are designed to give the Client a good insight into the quality and sustainability of the operations offered by the provider. However, it should be noted that a Securities Services Provider will only be able to share public, non-proprietary information, except where specifically covered under an NDA. The Securities Services Provider has the responsibility to ensure non-public information, in respect of its operation and - of course - its other Clients, remains confidential. It is recommended to review collected information during the relationship at least annually or on a dynamic basis.

7.5 Client Risk Threats

There are many Client risks that can arise when a Securities Services Provider and a Client form and maintain a relationship. The key risk threats - applicable to both the Securities Services Provider and the Client - are outlined below, along with potential risk mitigants that could be considered.

Illustration 7.5 Client Risk Table

Risk Description	Risk Mitigation
Securities Services Provider failure to perform initial and ongoing AML/KYC checks against Client and UBOs	▪ Implement robust KYC policies and procedures including periodic reviews with risk-based frequencies and clear/transparent implications to freeze services if required information is not provided within deadlines ▪ Create processes to ensure UBO details can be disclosed and that required KYC reviews and scans are being performed throughout the Securities Services value chain (refer ISSA Financial Crime Compliance Principles)
Securities Services Provider or Client failure to monitor relationship on an ongoing basis	▪ Implement and apply control procedures to monitor contracting party on an ongoing basis, such as: ○ Continued creditworthiness ○ Governance framework ○ Compliance with relevant regulations and rules ○ Sanctions screening ○ Business profile, account usage and transaction volume assessment vs expectations
Securities Services Provider or Client failure to identify non-standard servicing operating model / high-risk manual processes	▪ Ensure onboarding process includes detailed review by operational experts at the Securities Services Provider to identify where Client requested non-standard processes ▪ Work with Client to agree and implement automated approaches ▪ Ensure that a comprehensive RFP process is completed by the Client

Risk Description	Risk Mitigation
Strong contractual arrangement not implemented	▪ Implement an agreement detailing the contractual relationship between the Securities Services Provider and the Client prior to the business onboarding and amend in the event of a change in business model / requirements ▪ Ensure clear documentation of liabilities, indemnities, termination, confidentiality, security, resiliency, representation and warranties are expressed
Appropriate licences, capabilities and financial resources exist for the Client not identified	▪ Ensure the onboarding process has clear booking principles which consider the domicile and licences the Client has versus the licences and approvals at the legal entity providing the services at the Securities Services Provider ▪ Consider financial risk implications (such as on-balance sheet deposits and credit requirements) are sufficiently covered for the Client by the legal entity at the Securities Services Provider providing the services
Appropriate Client account set up not ensured by the Securities Services Provider	▪ Ensure control processes exist to check that cash and securities accounts cannot be activated by the Securities Services Provider or the Client without full executed agreements in place ▪ Ensure control processes exist to check account accurate set up by the Securities Services Provider of Client accounts and static data requirements ▪ Implement Client information packs from the Securities Services Provider for the Client to confirm the accurate set up as well as regular static data confirmation processes
Appropriate pricing, interest rate application and billing processes not ensured	▪ Ensure control process exists to confirm pricing relative to cost and risk (considering any non-standard high risk manual processes and reduced contractual protections) by the Securities Services Provider is appropriate for the Client ▪ Ensure control process exists for billing by the operational experts at the Securities Services Provider to confirm pricing approach follows standardized automated billing approach for the Client

8. Third-Party Provider Risk

8.1 Introduction

Where a Third-Party Provider offers material services to a Securities Services Provider - that are an inherently integral part of the Securities Services offering to Clients - then a number of risks need to be managed.

It is key that the Securities Services Provider looks at both the suitability and the appropriateness of each Third-Party Provider. This is not only from a service level and risk perspective but, increasingly, there is a strong regulatory focus on third-party governance, outsourcing, operational resilience and business continuity. Therefore, formalization and strengthening both external and internal Third-Party Provider arrangements is a key focus area for recovery and resolution planning.

8.2 Definition

A Third-Party Provider is an entity that provides functions, capabilities or services to a Securities Services Provider but is not a part of that performed by that Securities Services Provider. The Third-Party Provider may be external to the Securities Services Provider or another legal entity within the same organization. There may be further chain service providers (e.g. fourth or fifth-party providers) which would then also need to be included in this framework.

8.3 Third-party Provider Services

Common services and functions provided by Third-Party Providers to Securities Services Providers include, but are not limited to:

- Sub-custodian services
- Business Process Outsourcer (BPO)
- Specialist service providers (such as Proxy Voting services and Tax Reclaim/Filing services)
- Data providers that supply data such as:
    - Share price and FX feeds
    - Instrument reference data and corporate action data
    - Standard settlement instructions and legal entity identifiers
    - Credit rating and market data
- Messaging and communication such as SWIFT
- Technology services and applications such as:
    - Core operational office systems (back-office systems)
    - Corporate governance services such as proxy voting platforms
    - Finance systems
    - Reconciliation systems
- Sub custodian network oversight services

- Trade / settlement matching, instruction processing and reporting platforms

8.3.1 Outsourcing

One type of Third-Party service is outsourcing. Outsourcing means an arrangement between a Securities Services Provider and a Third-Party Provider by which that service provider performs a process, a service function or an activity that would otherwise be undertaken by the Securities Services Provider itself.

Throughout the Securities Services value chain, virtually every participant has the ability to outsource activities to a Third-Party Provider assuming no regulatory or contractual restrictions apply. However, whilst the business process may be outsourced, the Securities Services Provider is still accountable and needs to have sufficient oversight of the entity providing the service, the outcomes of their processing and be able to manage the risks that arise from having assigned a Third-Party Provider including business continuity.

8.3.2 Sub-custodian Network

A critical function for a Securities Services Provider is the ability to be able to access domestic markets to support their Clients' investment requirements. This is particularly true for Global Custodians who provide their Clients with 'global' connectivity and to I(CSDs) that provide direct access for eligible institutions to transmit and hold securities without holding accounts with each domestic CSD.

To access domestic markets, a Securities Services Provider may use its own Sub-custodian network, go directly to the CSD or engage Third-Party Providers domestically. Where a Sub-custodian is used, it will interface with the CSD and operate the accounts where the assets are ultimately held and transmit all relevant instructions received from the Securities Services Provider. Similarly, the ICSD will access domestic markets via a Sub-custodian or through a direct relationship with the domestic CSD referred to as 'CSD links'.

The Securities Services Provider's Sub-custodian Network Management group performs a critical third-party management function. It will have the responsibility to manage the various Sub-custodian relationships employed by a Securities Services Provider in accordance with an agreed network management policy. The Securities Services Provider will have a similar framework to manage and oversee its CSD network and ICSDs will have a similar team overseeing its own Sub-custodian relationships. Many of the oversight functions performed by the Sub-custodian Network Management function are critical to the overall process of ensuring asset safety, operational efficiency and compliance with regulations. Alternatively, Securities Services Providers who use external Sub-custodians may also decide to delegate the oversight function to a Third-Party Provider (such as a specialist consultancy firm). In these instances, the Securities Services Provider still needs to have oversight of that business and be able to manage the risks that arise from having assigned a Third-Party Provider.

The Sub-custodian Network Management function may be a separate unit within a Securities Services Provider but work closely to ensure it is aligned to both the business as well as technology and operations. The function will have

defined responsibility for various Third-Party Providers. This typically includes the selection, due diligence, documentation, performance and risk assessment of Sub-custodians, CCPs, CSDs and Nostro Banks as well as oversight and monitoring of the platforms provided by the Sub-custodian Network Management function. This team also has a detailed knowledge and insight into domestic markets which are critical for asset protection, operational efficiency and business intelligence. The network team will have domestic market expertise and knowledge of market conventions and regulations and will be integral to client service in educating Clients of the nuances of each market. In addition, the team may have responsibility for the dissemination of market intelligence internally and to Clients.

Assessments that the Sub-custodian Network Management function will oversee would include:

- Governance structure
- Business continuity provisions
- Key participants and how they translate into the risk profile
- Capital
- Investments
- Recovery and resolution provisions
- Quality of services such as tax, asset servicing
- Messaging and technical requirements / compatibility
- Settlement finality model
- Risk management model
- Change management model
- Compliance with regulations (e.g. CSDR in Europe)
- Pricing
- Adherence to terms and conditions

8.4 Third-party Oversight

A Securities Services Provider needs to establish a clear framework to manage the Third-Party Provider's activities which may require establishing dedicated units to oversee Third-Party Provider relationships. A key balancing act for the Securities Services Provider is to work as closely as possible with the Third-Party Provider to ensure optimal processes and efficiency, as well as to retain the institutional ability to move to an alternative Third-Party Provider should the need arise.

Where an activity has been outsourced, a key consideration - influenced by contractual, regulatory and risk appetite - is the extent to which the activity can be recovered and over what period the recovery can be sustained. Further, the industry focus on operational resilience has increased the regulatory scrutiny of these relationships. Securities Services Providers should be vigilant in understanding their regulatory obligations when assessing these relationships.

8.5 Third-Party Provider Risk Threats

Operational, business and reputational risk are the main elements that need to be considered by Securities Services Providers when appointing and using the services of a Third-Party Provider. Below is a table that summarizes the key risk threats and some potential mitigants.

Illustration 8.5 Third-Party Provider Risk Table

Risk Description	Risk Mitigation

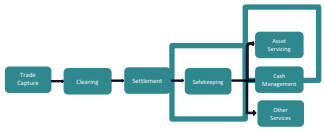
Appropriateness of Third-Party Provider not assessed and qualified by Securities Services Provider	▪ Establish and deploy a Third-Party Provider strategy
	▪ Create a team of qualified resources at the Securities Services Provider that is able to assess the appropriateness and suitability of a potential Third-Party Provider
	▪ Assess and monitor services and performance of a Third-Party Provider on an ongoing basis, including:
	  ▪ Qualifying eligibility by validating credit rating, financial soundness/resources relative to the activity, liability insurance, good standing, regulatory permissions (where appropriate), BCP facilities, third-party management, ESG (goals and risks), ensuring conformity with corporate identity
	  ▪ Managing concentration risk so that a Third-Party Provider does not take on too much business with the Securities Services Provider that then compromises service
	  ▪ Ensuring that a Third-Party Provider delivers the contracted services at agreed quality levels, within agreed processing timeframes and agreed prices
	▪ Establish a news alert process to identify potential concerns with a Third-Party Provider

Appropriate regulatory / Client approvals not arranged before using Third-Party Provider	▪ Implement an internal process at Securities Services Provider to assess whether, and what, regulatory approvals are required to contract with a Third-Party Provider ▪ Complete all regulatory approvals prior to contracting with a Third-Party Provider ▪ Establish a process to assess all Client contracts to identify any pre-approval and notification requirements
Third-Party Provider failure leading to service no longer being performed	▪ Establish a policy at the Securities Services Provider to ensure that an alternative solution has been identified and will be available in the event of a failure of a Third-Party Provider. This could be through the approval for appointment of an alternative Third-Party Provider or by bringing the service in-house
Alternative provider not appointed within a timely manner	▪ Create a detailed contingency framework at Securities Services Provider, including written procedures and timeline, to cover the process required to move a service from a Third-Party to an alternative solution should a trigger event occur
Appropriate incident management process not implemented and / or followed	▪ Implement a contractual arrangement between Securities Services Provider and Third-Party Provider which outlines a Third-Party Provider's responsibilities with regards to incident management ▪ Assign internal responsibilities at Securities Services Provider for Third-Party Provider policy, management and oversight function including incident management

Risk Description	Risk Mitigation
Third-Party Provider failure to follow expected incident management process	▪ Include, in the contractual arrangement between a Securities Services Provider and a Third-Party Provider, language covering implications and liabilities in the event of non-compliance with incident management processes
Sub-custodian failure due to inability to provide service or local market issues	▪ Implement a process for ongoing monitoring of a Sub-custodian by the Securities Services Provider ▪ Complete selection and contractual appointment of an alternative Sub-custodian with active contingency accounts opened to be utilized in the event of a trigger event ▪ Agree on an approach for making a decision, should a trigger event occur, to divert new / existing business to the contingency provider

9. Asset Protection Risk

9.1 Introduction



There are a number of ways in which a Client's assets can be at risk of loss or non-availability throughout the Securities Services value chain. These include fraud or misappropriation of assets, inadequate controls, servicing error or insolvency of one or more Securities Services Providers.

The 2008 financial crisis, and specifically the collapse of Lehman Brothers, highlighted the risks for Securities Services Providers and resulted in increased regulatory attention on asset safety and investor protection throughout the Securities Services value chain. In more recent times, both the collapse of certain Cryptocurrency exchanges - which also acted as the apparent Custodians of the cryptocurrencies and the application of sanctions and countermeasures - underlined the criticality and Client benefit of strong asset protection rules.

This chapter explores the key principles of asset protection as well as outlines the different risks and risk mitigation opportunities. It should be noted that the focus of this chapter is on securities assets - which can be held off-balance sheet with a Securities Services Provider. In the majority of cases, cash is fungible and on-balance sheet with banks and subject to prudential regulations to ensure that appropriate safety and soundness requirements are in place.

9.2 Definition

Asset protection involves measures taken by Securities Services Providers to ensure the safety of Client assets and to mitigate against loss or non-availability, concealment, fraudulent use or transfer of assets, impacts of insolvency in the Securities Services value chain and breach of legal or regulatory requirements, in accordance with national, regional or international asset protection laws.

9.3 Key Principles of Asset Protection

Many of the key requirements for asset protection depend on the nature and jurisdiction(s) of the assets being held and of the Securities Services participants and Clients involved. Asset protection risk therefore needs to be assessed and mitigated at the Client onboarding stage as well as when Securities Services Providers extend into new jurisdictions or asset types.

Risks to asset protection are present throughout the Securities Services lifecycle. Measures to detect breaches or abnormalities are found throughout the lifecycle, with particular emphasis on the settlement, safekeeping, reporting and asset servicing stages. Securities Services Providers therefore need to ensure:

- Timely and accurate recordkeeping of assets and their ownership
- Regular reconciliation between their own records and upstream or downstream Securities Services Providers
- Timely and comprehensive reporting to their Clients

Considering the evolving regulatory environment, Securities Services Providers also need to stay abreast of the regulatory agenda and ensure timely deployment of any changes to achieve compliance (e.g. system, legal, risk framework, sanctions).

The 2014 International Organization of Securities Commissions (IOSCO) paper provides recommendations regarding asset protection and sets out a number of key principles on this topic.
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD401.pdf

These are summarized below:

- 'Proprietary Assets' held by the Securities Services Provider are physically and legally separate from Client assets and, in a default scenario of the Securities Services Provider, an administrator should be able to identify assets belonging to the Client and that the Sub-custodian is purely facilitating custody on behalf of the Client. The importance of precise account naming conventions is critical
- The Securities Services Provider should also be able to identify the amount, location, ownership status and identity of Client assets at all times and without delay. Reconciliation processes must be in place to confirm this In addition, prior consent from the Client must be held for any use of a Client asset
- The Securities Services Provider should provide a statement to its Clients on a regular basis and on request
- The Securities Services Provider must understand the implications of holding assets in a foreign regime and ensure clarity and transparency in the disclosure of relevant Client asset protection regimes

CASE STUDY: FTX Trading

On 11 and 14 November 2022 FTX Trading Ltd (a cryptocurrency exchange firm) and affiliates filed a petition for relief under Chapter 11 of the US Bankruptcy code. Investigations based on the debtor's analysis consider that FTX exchanges owed Clients approximately USD 8.7Bn. The Debtors Report highlighted commingling and misuse of Client deposits and noted:

"The FTX Group touted a commitment to protecting customer deposits from misuse or misallocation, and publicly championed legislative and regulatory efforts to protect crypto industry customers. Through its website, social media, and in statements and submissions to Congress, regulators and other third parties, the FTX Group represented that it maintained a strict separation of customer and corporate funds, including by maintaining customer funds in omnibus bank accounts "for the benefit of" ("FBO") FTX exchange customers. At all times, with the exception of isolated jurisdictions, the FTX Group's representations in this regard were false." (Source – US Bankruptcy Court, Delaware - case 22-11068 – Second Interim Report dated 26th June 2023).

FTX commingled Client and proprietary assets. If they had followed the key principles for Client segregation regulations, this situation would have been avoided. At the time of writing, Regulators are in advanced stages of completing regulation to clarify and ensure appropriate frameworks are established; for example ESMA's Markets in Crypto Assets Regulation (MiCA).

9.4 Asset Protection Risk Threats

The tables below describe the most prevalent risk threats which may compromise asset protection. These risk threats include:

- Political / country risk
- Evolving regulatory framework risk
- Account structure and registration risk
- Insolvency / default risk
- Fraud and negligence risk

However, it is important to note that even after stringent risk mitigation practices have been deployed, asset protection risk cannot be fully avoided. Absence of established and proven legal frameworks, country risk events (such as freezing of assets) and participant insolvency are amongst the key risk factors that need to be considered in a Client's investment decisions and the risk appetite decision of both a Securities Services Provider and Client.

9.4.1 Political / Country Risk

Political and country risk can occur when there is instability or uncertainty in a country's governance or political regime. Political or economic unrest could lead to changes to laws, regulations or policies that impact asset protection.

The implications for Securities Services Providers and their Clients should this situation occur could be severe with assets potentially being blocked, frozen or even lost. Securities Services Providers and Clients should conduct an analysis of each market to understand the political and economic environment and continuously monitor the situation in order to be able to react in the event that a situation changes.

Illustration 9.4.1 Political / Country Risk Table

Risk Description	Risk Mitigation
Market collapses	▪ Ensure focused internal groups monitor the different jurisdictions where Clients are holding assets through the Securities Services Provider ▪ Have contingency / diversification arrangements in place with proactive inventory management to hold transferable assets in a cross-border location
Political unrest, war, acts of terrorism impacting liquidity, systems, stock exchange, central banks	▪ Ensure focused internal groups at the Securities Services Provider to monitor the political environment ▪ Have contingency arrangements in place with proactive inventory management to hold transferable assets in a cross-border location ▪ Ensure active liquidity management for cash
Embargo / sanctions being introduced which limit the movement of, or access to, assets	▪ Ensure robust embargo / sanctions screening tools and escalation procedures are in place ▪ Ensure legal documents cover Securities Services Provider / Client responsibilities and liability in the event of an embargo / sanction being put in place
Regulators' expectation lack transparency or are unclear	▪ Ensure strong country risk analysis and connections with local regulators and jurisdictional legal experts

Risk Description	Risk Mitigation
Securities Services Provider lacking transparency of Investors which hinders detection of sanctioned Investors / assets	▪ Implement enhanced omnibus account suitability requirements for at-risk jurisdictions /businesses ▪ Create enhanced KYC processes, including looking through to the UBO ▪ Ensure ongoing performance / transaction monitoring of Investors / assets

9.4.2 Evolving Regulatory Framework Risk

Regulations are continuously changing with regulators creating and implementing new and updated regulations as markets evolve and grow. Any change to a regulatory framework may require action by a Securities Services Provider and/or a Client as a regulatory breach could have potential implications for asset safety. Therefore ongoing monitoring of the different regulatory frameworks is critical to ensure ongoing adherence.

Illustration 9.4.2 Evolving Regulatory Framework Risk Table

Risk Description	Risk Mitigation
High frequency and complexity of regulatory change	▪ Ensure active engagement in order to stay abreast of the regulatory agenda
Impact to reputation and business due to non-adherence to regulations	▪ Carry out internal impact assessments to ensure timely deployment of any changes to achieve compliance (e.g. system, legal, risk framework)
Regulatory changes lack transparency or are unclear	▪ Ensure strong country risk analysis and connections with local regulators and jurisdictional legal experts

9.4.3 Account Structure and Registration Risk

The choice of account structure may have an influence on the level of asset protection – i.e. providing assurance that the Client ultimately retains (legal) ownership with all associated rights (income, corporate events, proxy voting etc.) and access to the assets in line with applicable regulations across the various jurisdictions involved. As outlined in the Account Structure chapter, the most common options are:

- Omnibus account (where there are assets of multiple Investors together)
- Segregated account (where assets are split either at Sub-custodian or CSD level)
- Nominee account (where the assets may be held in an omnibus or segregated account but are registered in the name of a nominee)

These account structures are possible at several levels of the Securities Services chain but may not always be allowed, or advisable, under applicable regulations. Whilst differing account structures exist, provided practices are followed (such as naming conventions, robust contractual arrangements, accurate and timely recordkeeping at asset owner level, reconciliations and local regulations), then the structures referenced should provide adequate asset protection. However,

there are advantages and disadvantages, particularly cost and efficiency, which drive the decision as to which approach to take.

Illustration 9.4.3 Account Structure and Registration Risk Table

Risk Description	Risk Mitigation
Inappropriate use of nominee concept	▪ Use nominee account structure only in markets where concept is recognized ▪ Where the nominee concept is recognized in a jurisdiction, the account is held in a nominee name which is different from the Securities Services Provider's name ▪ Assessment of assets in the nominee to ensure no liability on the nominee (e.g. partially paid assets with obligations / calls may not be appropriate)
Recognition of nominee naming concept lacking in a jurisdiction	▪ Establish account at Sub-custodian / CSD in the name of the Client or UBO
Sub-custodian default / insolvency	▪ Ensure Securities Services Provider assets are ring-fenced and distinguishable at Sub-custodian level ▪ Ensure Client assets are wholly segregated from proprietary and all other assets ▪ Have Sub-custodian account in Securities Services Provider nominee, Client or UBO name and is visible to creditors
CSD default / insolvency	▪ Ensure Securities Services Provider assets are ring-fenced and distinguishable at CSD level ▪ Ensure Client assets are wholly segregated from proprietary and all other assets ▪ Have CSD account in Securities Services Provider nominee, Client or UBO name and is visible to creditors ▪ Understand the CSDs' process for transferring assets to another CSD in case of winding down (for reasons of default, insolvency or withdrawal of CSD licence)

9.4.4 Insolvency / Default Risk

The impact of the insolvency of - or default by - a Securities Services Provider or a Client will have a huge effect on both the party that is insolvent / in default as well as others doing business with that party. However, insolvency - in particular - may also have broader implications for the whole industry. It is therefore imperative that strong asset protection measures are implemented to ensure that a Securities Services Provider and a Client's assets are separate and ring-fenced. Robust reconciliation and reporting processes need to be implemented and ongoing credit-worthiness checks completed by both parties. In jurisdictions where asset protection regimes are in place, contractual arrangements should reflect these regulatory requirements.

Illustration 9.4.4 Insolvency / Default Risk Table

Risk Description	Risk Mitigation
Securities Services Provider insolvency or default	▪ Implement a strong Securities Services Provider selection criteria and business acceptance process at the Client ▪ Ensure Client assets are wholly segregated from the Securities Services Provider's assets ▪ Check credit rating, credit limits, credit control and monitoring together with contractual mitigants (lien and right of sale) on an ongoing basis

Risk Description	Risk Mitigation
Client insolvency or default	▪ Implement a strong Client selection criteria and business acceptance process at the Securities Services Provider ▪ Have ability to segregate Client assets in the event of Client insolvency in order that the Securities Services Provider can continue normal business ▪ Check credit rating, credit limits, credit control and monitoring together with contractual mitigants (lien and right of sale) on an ongoing basis
Sub-custodian / CSD insolvency or default	▪ Have a strong Sub-custodian / CSD selection criteria in place at the Securities Services Provider ▪ Ensure Securities Services Provider and / or Client assets are ring-fenced and distinguishable at local market level and monitor on an ongoing basis ▪ Understand governmental guarantees or other backstops available to prevent CSD functions from ceasing
Contagion of a globally significant Securities Services Provider	▪ Apply bank recovery and resolution provisions ▪ Understand financial implications of contagion of a globally significant Securities Services Provider including credit exposures from unsettled trades, securities lending (stock loans and borrows), etc.
Legal framework, where assets are held, may not have established clear and proven asset safety or insolvency remote structures	▪ Have clear review and acceptance process for jurisdictional regulatory and legal requirements concerning asset protection ▪ Include appropriate language in Securities Services Provider contractual agreements that explains limitations in asset protection regimes
Contractual agreement legal language deviates from country's regulatory / legal framework	▪ Have clear review and acceptance process for jurisdictional regulatory and legal requirements concerning asset protection ▪ Monitor regulatory and legal regime in each jurisdiction to ensure jurisdictional changes are captured and any contractual changes identified and added to agreements

9.4.5 Fraud and Negligence Risk

Fraud and negligence are two further threats to the protection of assets. Whilst negligence involves making a careless mistake, fraud is an intentional act designed to deceive.

Fraud is perpetrated by criminals who are continuously coming up with new, and increasingly sophisticated, methods of deception. Within Securities Services, fraud could occur through a variety of means such as unauthorized access to Client information, fraudulent transactions or cyber-crime.

Negligence, by a Securities Services Provider or Client, is where there is a mistake such as an error in inputting a transaction, sending a late transaction, information provided being incorrect or transactions / information being missed. Whilst negligent actions are not deliberate, the implications can still be severe. Therefore, taking steps to minimize these types of risk is also important.

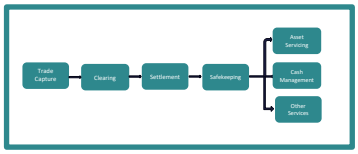
Negligence and fraud can occur at many points in the Securities Services value chain. Therefore, it is incumbent on both Securities Services Providers and Clients to take active steps to understand where these risks could occur and have mitigants in place to prevent them.

Illustration 9.4.5 Fraud and Negligence Risk Table

Risk Description	Risk Mitigation
Fictitious trade bookings or fraudulent transactions sent to Securities Services Provider	▪ Implement a strong Securities Services Provider / Client selection criteria and business acceptance process ▪ Ensure a robust risk framework / policy and procedures, including establishing expected ethical standards / code of conduct to set risk behaviour ▪ Implement automated methods at Client covering: ○ transmission of transactions ○ stringent authentication / validation processes ○ allocation / confirmation affirmation processes (where supported in a jurisdiction ○ regular reconciliations of books and records
Transactions not processed in an accurate, comprehensive and timely manner	▪ Implement comprehensive transaction checking and end-to-end controls and reconciliations at Securities Services Provider and Client ▪ Ensure strong policies / procedures / staff training / risk culture in place ▪ Encourage automated methods for transmitting transactions, along with stringent authentication / Client validation processes
Manual / non-STP process / incorrect static data	▪ Implement automated methods for transmitting transactions, along with stringent authentication / validation processes at both Securities Services Provider and Client ▪ Provide incentives to Clients to deter manual, late and inaccurate instructions ▪ Ensure multi hierarchy input, approval and release controls for transactions

10. Execution, Delivery and Process Management Risk

10.1 Introduction



All parties in the Securities Services chain can be exposed to the risk of loss or delay arising from operational errors, resulting from - for example - inadequate internal processes, human error or system failure. These risks are commonly known as execution, delivery and process management risks.

This chapter looks at how an error of this nature may leave a Client or Securities Services Provider at risk of losing part, or all, of the value of an investment, entitlement and / or opportunity and may lead to claims between parties. As such, the contractual provisions between a Client and its Securities Services Provider related to breach of contract and negligence are important in mitigating the risk to the parties from recovering its losses.

It is important to note that these risks are not unique to Client and Securities Services Provider relationships. They are risks that are inherent in using any service provider for holding assets and handling transactions.

10.2 Definition

Execution, delivery and process management risk can be defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This risk can impact both Securities Services Providers and Clients through the use of Securities Services functions and is the risk assumed by a Securities Services Provider when performing services on behalf of a Client and vice versa.

10.3 Trade Capture, Clearing and Settlement Risk Threats

This aspect of the service relates to the capture of trade details from a Client, followed by the creation of a securities delivery or receipt transaction, together with the matching, clearing and settlement as the main processes concluding the transfer / exchange of assets post the trade execution between the two trading counterparties.

10.3.1 Trade Capture Risk

The trade capture process is exposed to a number of operational risks which can lead to settlement failures. It is therefore key that the trade capture process is as automated as much as possible and that controls are implemented to check and validate the completeness and accuracy of the trade capture process.

Illustration 10.3.1 Trade Capture Risk Table

Risk Description	Risk Mitigation
Client's instructions not captured	▪ Use of structured messaging formats to increase straight-through processing (STP) ▪ Establish message control reconciliation ▪ Establish controls and alerts for repaired / rejected instructions ▪ Monitor alleged trades

Risk Description	Risk Mitigation
Trade details not captured / authenticated accurately	▪ Accept instructions through automated STP (straight-through processing), subject to: ○ Established system controls that can uniquely identify that the origination of the instruction has come from the Client or intermediary acting on their behalf ○ Established system controls to uniquely validate the correct Client account and standard settlement instructions (Sis) ▪ Accept, only exceptionally, manual instructions (e.g. in a contingency situation or for non-standard transactions), subject to: ○ Established controls for accurate capture of manual instructions (e.g. high-risk media such as fax, e-mail) ○ Controls to ensure manual instruction verification to validate client authenticity through signature verification/call back / verification of email sender. (These media types are high-risk to the client and should be discouraged as much as possible)

10.3.2 Clearing Risk

Securities Services Providers using CCPs to clear trades, act as the counterparty to the trade on behalf of a Client. As a result of this process, Securities Services Providers are exposed to multiple risks associated with clearing, including credit, market and operational risk.

Illustration 10.3.2 Clearing Risk Table

Risk Description	Risk Mitigation
Client's trade instructions are not captured by the CCP	▪ Use structured messaging formats to increase straight-through processing (STP) ▪ Establish transaction reconciliation controls between the trading file (i.e. the venue where the trade executions take place) and the CCP file (i.e. the netted trades processed by the CCP) ▪ Establish controls for repaired / rejected instructions
Instructions received do not match counterparty	▪ Establish controls for handling unmatched instructions ▪ Implement controls to monitor and retrieve notifications from the CCP which may identify discrepancies ▪ Establish communication and service reviews to raise any ongoing issues with Client instructions
Securities Services Provider does not duly monitor credit risk and exposure to the CCP	▪ Ensure CCP has a comprehensive entry criteria / onboarding protocol and completes full due diligence on each of all of its members both prior to their joining the CCP as well as on an ongoing basis ▪ Establish controls at the Securities Services Provider to monitor the market and Client positions ▪ Ensure that appropriate levels of collateral, either as cash or securities, is provided by the Client as security against potential losses

Risk Description	Risk Mitigation
Securities Services Provider misses a buy-in notification	▪ Establish operational process at the Securities Services Provider to ensure buy-in notifications are retrieved from the CCP on an automated basis ▪ Create a workflow event, in the event that STP is not supported – to monitor the CCP website or messaging portal for relevant notifications ▪ Establish a time-sensitive notification process and SLA to notify Clients of a buy-in event ▪ Ensure that sufficient collateral is posted by the Client to mitigate the Securities Services Provider in the event that buy-ins occur ▪ In the event that a buy-in is executed against a Client's trade, immediately cover the loss using the Client collateral provided
Clearing member defaults at CCP	▪ Ensure Securities Services Provider has stringent CCP risk management processes to identify potential counterparty risk issues before they occur ▪ Ensure CCP has established communication protocols to notify other clearing members of the default of a clearing member in accordance with the CCP rulebook and relevant regulation ▪ Ensure that both CCP and Securities Services Provider have appropriate levels of collateral (either as cash or securities) ▪ Ensure that margin calls are in place and called in a timely manner by the Securities Services Provider ▪ Ensure that additional margin is paid in a timely manner by Securities Services Provider in accordance with the CCP rulebook and that internal capital and liquidity requirements appropriately cover the credit risks associated with CCP exposure ▪ Have publicly disclosed insolvency and default policies in place on the Securities Services Provider's website ▪ Ensure that a back-up GCM has been nominated by the Client in the event their Securities Services Provider GCM defaults and that operational protocols are in place to 'port' their positions to the replacement GCM
Client defaults	▪ Ensure Securities Services Provider implements a process so that sufficient collateral is posted by the Client to mitigate the Securities Services Provider's risk and that appropriate levels of margin are called from the Client in accordance with daily mark-to-market price changes ▪ Ensure Securities Services Provider monitors that lien / right of sale or set off is in place to provider additional covers versus exposure to the Client ▪ Have publicly disclosed insolvency and default policies in place on the Securities Services Provider's website
CCP defaults	▪ Implement documented risk and liability monitoring and an escalation / communication framework at the Securities Services Provider to monitor CCPs' performance and credit worthiness ▪ Ensure capital and liquidity requirements at the Securities Services Provider that appropriately cover the credit risks associated with CCP exposure ▪ Ensure that a back-up CCP has been identified by the Securities Services Provider to 'port' positions in order to limit / avoid service degradation and financial harm to the Client ▪ Have publicly disclosed insolvency and default policies in place on the Securities Services Provider's website

10.3.3 Settlement Risk

A securities transaction may not settle due to a variety of reasons, including – most frequently - a late instruction, a missing instruction, an incomplete or inaccurate instruction or due to a lack of cash or securities. However, other less frequent reasons include Client or counterparty insolvency, suspended security code due to sanctions or a reconciliation issue. Each of these issues can create settlement risk for both the Securities Services Provider and the Client and therefore proactive management and monitoring of incoming trades and pending settlements are both key requirements to mitigate this risk.

CASE STUDY: Settlement Fail Issue

In some markets, debt securities are accounted for in units, with each unit representing a nominal value. This may lead to operational errors when a settlement instruction quantity for such securities is entered in face amount, so that the total quantity of such instruction far exceeds the intended amount and may exceed the Securities Services participant's total position or even the total amount of securities issued in this instrument.

If such instruction is matched by the counterparty, it will be submitted for settlement, but it is likely that the transaction fails to settle on the intended date. As a result, the receiving participant may be unable to settle onward transactions, and the participant that is unable to deliver will be exposed to claims. In addition, in the EU, such fails are now consistently subject to settlement penalties under the Central Securities Depositories Regulation (CSDR) framework. Given the fact that the failed transaction amount in such cases is a multiple of the intended amount, the applied penalties are as well much higher than for a regular fail. The only option for participant to neutralise the consequence of their error is to have the penalty amount compensated on a bilateral basis.

This case highlights the critical importance of accurate data entry, accurate representation by data vendors, full economic -pre-matching and the need for robust validation mechanisms to prevent such errors by all actors in the post trade value chain. It underscores the potential financial and reputational risks associated with operational mistakes in the securities settlement process. Furthermore, it emphasizes the necessity for continuous monitoring and timely detection of discrepancies and abnormalities to mitigate the impact of such operational risks. This serves as a reminder of the complexities involved in securities settlement and the importance of strong data quality, stringent controls to ensure the integrity of the process.

Illustration 10.3.3 Settlement Risk Table

Risk Description	Risk Mitigation
Client / Securities Services Provider sends incorrect settlement instructions	▪ Establish system controls to validate content and ensure instruction is complete ▪ Establish standing settlement instruction (SI) templates to ensure compliant message formats are sent ▪ Leverage industry platforms to ensure correct SIs are used ▪ Use SWIFT instructions, and other standardized communication platforms, which ensure that mandatory fields are populated for each settlement type

Risk Description	Risk Mitigation
Trade not checked for securities availability	▪ Establish a Securities Movement and Control (SMAC) system and check for availability and location of securities ▪ Ensure securities for delivery need to be available on an actual basis (not the contractual or traded view)except for linked receipt / delivery trades ▪ Complete periodic automated reconciliation of positions between the Securities Services Provider and the Sub-custodian / CSD in line with local regulations and / or market convention
Trade not checked for cash availability	▪ Establish check on source of funds (e.g. cash, credit limits, FX, etc) ▪ Ensure cash for receipt of securities is available in the account and not shown as contractual unless a credit arrangement is in place depending on market and Securities Services Provider requirements ▪ Complete periodic automated reconciliation of cash positions against the Sub-custodian / CSD cash accounts in line with local regulations and / or market convention
Sub-custodian / CSD not instructed	▪ Establish robust end to end completeness review controls and reconciliation of transactions at Securities Services Provider ▪ Implement an automated end-to-end STP process from the Client through the Securities Services Sub-custodian chain to the CSD
Client trade matching status not monitored and Client not updated (where applicable)	▪ Establish automated trade matching capability ▪ Contact trading or settlement parties to establish reasons for failed pre-match when trades fail to pre-match ▪ Accept new instructions from Client and send to Sub-custodian / CSD where appropriate to achieve matched status ▪ Report matching status to end client ▪ Establish frequent automated matching status workflow prompts to ensure complete oversight
Trade failure not monitored	▪ Establish automated trade monitoring capability ▪ Contact trading or settlement parties and establish reasons for failed pre-match where trades fail to pre-match ▪ Accept new instructions from Client and send to Sub-custodian / CSD where appropriate to achieve settled status ▪ Report trade settlement status to the Client ▪ Agree process / policies to cancel aged-failed trades where appropriate in accordance with local regulatory guidance and / or market conventions

Risk Description	Risk Mitigation
Transactions not settled in a timely manner, including cross-border transactions	▪ Establish automated trade monitoring capability ▪ Establish SSI templates to ensure compliant message formats are sent in conformance with market standards e.g. Securities Market Practice Group (SMPG) Standards https://www.smpg.info/ ▪ Use SWIFT instructions, or other standardized communication platforms, which ensure that mandatory fields are populated for each settlement instruction ▪ Ensure cash and securities are available for timely settlement ahead of intended settlement date ▪ Arrange a securities lending 'borrow' to cover any short position or utilize Sub-custodian / CSD auto-borrow facilities where available ▪ Ensure that inventory is optimized by offering / accepting partial settlement or splitting deliveries to the same nominals as receipt instructions ▪ Ensure market deadlines for cross-border instructions are known and instructions are sent in accordance with the market timetables to avoid late instructions or delayed settlement due to mis-aligned market conventions
Buy-ins / sell-outs not prevented	▪ Ensure timely settlement of transactions ▪ Implement regular reporting of short deliveries ▪ Ensure robust understanding and communication of buy-in /sell out markets / timeframes / penalties ▪ Implement effective monitoring / reporting of trades at-risk of buy-in with timely delivery of buy-in/sell out notifications
Matching / settlement fines / penalties not prevented	▪ Ensure that deliveries are covered by available securities' balances prior to trading and / or implement a matched trading book to ensure that deliveries are covered by corresponding purchase trades for the same intended settlement date ▪ Ensure timely settlement of transactions ▪ Provide regular reporting of short deliveries to identify short positions ▪ Arrange to borrow short positions through securities lending arrangements or utilize Sub-custodian / CSD auto-borrow facilities where available ▪ Maximize inventory held by offering / accepting partial settlement ▪ Ensure good understanding of the fine regime in each market / security type in accordance with market conventions and regulations including CCP / CSD rule books ▪ Ensure effective monitoring / reporting of potential / breached limits

10.4 Securities Safekeeping Risk Threats

A key risk within the Securities Services value chain is that of loss of assets whilst in safekeeping. The Securities Services Provider must ensure that a Client's assets (both dematerialized and physical) are held properly protected against insolvency of Sub-custodian and / or CSD, fraud, processing error, etc. For further information, please review Chapter 9: Asset Protection.

Illustration 10.4 Securities Safekeeping Risk Table

Risk Description	Risk Mitigation
Client assets not protected from insolvency of Sub-custodian and CSD	▪ Implement robust selection and monitoring including due diligence of Sub-custodians and understanding of CSD account structures and local safekeeping regulations ▪ Ensure daily monitoring of Sub-custodian and CSD news (e.g. through reviewing credit ratings) ▪ Implement robust incident / crisis management process ▪ Provide ongoing review and assessment of insolvency protection related legal opinions ▪ Ensure compliance with all relevant asset protection regulations ▪ Ensure appropriate account titling, naming and registration ▪ Complete frequent reconciliation of assets held at a Sub-custodian / CSD vs a Securities Services Provider's own books and records
Client assets not protected from fraudulent misappropriation	▪ Establish and maintain robust system and physical access control (role-based privileges, strong ongoing validation) ▪ Ensure frequent reconciliation of assets held at a Sub-custodian / CSD as well as registrar records (for physical securities) vs a Securities Services Provider's own books and records ▪ Provide frequent statement generation to Clients
Client assets not protected from erroneous delivery	▪ Establish and maintain robust system and physical access control (role-based privileges, strong ongoing validation) ▪ Establish automated operating model minimising opportunity for human error ▪ Establish system-enforced dual controls conducted by trained and capable staff members ▪ Ensure frequent reconciliation of assets at a Sub-custodian / CSD vs a Securities Services Provider's own books and records ▪ Provide frequent statement generation to Clients ▪ Implement robust controls to check for availability of holdings / positions in a Client's account before sending delivery trades to a Sub-custodian / CSD or releasing the delivery instruction for settlement (especially where omnibus accounts are held with these parties)
Client assets not protected from market changes / force majeure events (e.g. sanctions restricting access to assets in the local markets	▪ Ensure daily monitoring of Market News, Sanctions, etc. and provision of information to Clients ▪ Implement close coordination with Sub-custodians ▪ Ensure ongoing compliance with existing regulatory regimes and scan for new regimes that require compliance
Physical assets not protected	▪ Ensure physical securities are registered where possible ▪ Ensure vault / secure room appropriately secure, fire / water resistant and insured for value / nature of assets held ▪ Implement a secure method and insurance to cover moving physical securities between locations ▪ Ensure regular reconciliation of physical securities to books and records of the Securities Services Provider and the Registrar where it exists ▪ Ensure ongoing compliance with existing regulatory regimes and scan for new regimes that require compliance

10.5 Asset Servicing Risk Threats

Asset servicing refers to the actions taken to service assets once they are held by a Securities Services Provider. It may cover corporate action, income and tax processing. In its broadest sense, it also includes corporate governance such as proxy voting and class actions.

10.5.1 Corporate Action Processing Risk

The key risks associated with the processing of corporate actions are operational in nature where either a corporate action is late, not identified, not actioned or incorrected processes. This can lead to failures which could cause reputation risk to the Securities Services Provider and / or Client.

CASE STUDY: Unstructured Corporate Action Messages

Use of unstructured message types to send instructions for voluntary corporate events could result in errors in the processing of these instructions. While the potential loss is usually the price differential between the price of the security upon participation of the event, versus the current market price, there is also the risk of the loss for the entire value of the securities.

For example, a Client sends an MT599 to its Securities Services Provider with multiple instructions on the message. Given the different instructions, the operations' team misses an instruction to participate in an optional bond swap which results in the Client not receiving the equivalent quantity of the new bond. The Issuer defaults on the old bond.

As a result of the error, the Securities Services Provider would then have to either purchase the new bond or pay the Client for the value of the new bond without any recovery from the old bond.

Illustration 10.5.1 Corporate Action Processing Risk Table

Risk Description	Mitigation
Corporate action not identified in a timely manner and/or accurately by Securities Services Provider	▪ Ensure trusted source and feed of information from independent sources / corporate action data providers to enable comparison / reconciliation and creation of final interpretation of announcement for onward transmission to clients ▪ Securities Services Provider to ensure that an SLA is in place with Sub-custodian sets out requirements and that processes are carried out in compliance with CSD rule books and local market regulations

Risk Description	Mitigation
Client not notified of original or change to a corporate action by Securities Services Provider	▪ Design and implement an operating model, which leverages technology, to auto notify holders of a new corporate action event / change to a published corporate action ▪ Devise a risk framework with control points to identify notification failures ▪ Implement a STP model to aid timely and accurate notifications ▪ Encourage Client to implement a STP model for corporate action processing ▪ Establish system-enforced dual controls, conducted by trained and capable staff members, to review event details ▪ Ensure notification alerts / reporting by Securities Services Provider which includes status, such as confirmed / unconfirmed and complete / incomplete
Action on voluntary event not taken	▪ Implement an operating model to receive Client responses through automated and STP means and establish system-enforced dual controls, conducted by trained and capable staff members, to input / approve voluntary elections ▪ Ensure confirmation messages and exception / follow up notifications are sent to the Client ahead of event deadlines ▪ Ensure Clients follow operating model and use electronic messaging to support STP and to review and respond to confirmations / notifications where appropriate ▪ Reconciliation by Securities Services Provider of instructions received vs instructions submitted
Client instructions incorrectly submitted to the market	▪ Establish system-enforced dual controls, conducted by trained and capable staff members, to input / approve manual instructions to the Sub-custodian / CSD ▪ Ensure reconciliation of instructions received vs instructions submitted
Client entitlements not applied by Sub-custodian / CSD	▪ Implement an operating model, and technology, designed to ensure Client entitlements corporate action options are auto calculated and consider the availability of the position and ensure that it is protected ▪ Ensure reconciliation of securities or cash position received from Sub-custodian / CSD to Securities Services Provider's books and records
Standing Instructions (SIs) for Client entitlements not applied	▪ Ensure robust process for storing and applying Client SIs to ensure entitlements are correctly applied in accordance with the Client's preference ▪ Ensure timely reporting to Clients in accordance with the Client's SIs for entitlements
Instructions received after Securities Services Provider cut off but before market cut off not acted on	▪ Ensure Securities Services Provider and Client contractual agreement clearly outlines impact of instructing late ▪ Ensure SLAs are in place at the Securities Services Provider and a process, such as a score card to monitor Client instruction timelines, and consider outreach / training to avoid repeat occurrences

10.5.2 Proxy Voting Risk

The risks associated with proxy voting are mainly operational risks due to failures to identify, notify or accurately process an event. Again, this can lead to reputational risk at the Securities Services Provider and / or Client.

Illustration 10.5.2 Proxy Voting Risk Table

Risk Description	Risk Mitigation
Proxy voting event and detail not identified in a timely manner and /or accurately by Securities Services Provider	▪ Ensure reliable feed of information from independent sources to enable comparison, reconciliation and creation of final interpretation of announcement for onward transmission to clients ▪ Securities Services Provider to ensure SLA with Sub-custodian which sets out requirements and that processes are carried out in compliance with CSD rule books and local market regulations
Client not informed of proxy voting requirement	▪ Design an operating model, supported by technology, to ensure proxy voting entitlements are automatically calculated and consider the availability of the position and ensure it is protected ▪ Ensure that the operating model provides the capability to automatically notify Clients holding positions of voting requirements and outcomes
Proxy voting event not tracked and Client not notified after announcement, missing changes to terms	▪ Ensure trusted source and feed of information ▪ Design an operating model, supported by technology, that can automatically notify Clients holding positions with a full audit trail ▪ Have a control point framework in place to identify notification failures ▪ Implement an STP reporting model to aid timely and accurate notifications
Client does not respond to voting request	▪ Establish controls for timely reminder to Client on lack of response ▪ Ensure a contractual arrangement is in place between the Securities Services Provider and the Client documenting responsibilities including response times and deadlines
Client's manual entry of proxy votes in processing applications, leads to incorrect voting instructions or mis-recorded preferences	▪ Support operational processes and technologies at the Securities Services Provider that enables the Client or voting authorities to enter the proxy voting information ▪ Implement automated data processing, with validation checks, to avoid manual key-in of voting data in different processing systems ▪ Ensure full daily reconciliation is in place to detect imbalances / anomalies where separate processing systems handle proxy voting transactions
Securities Services Provider's manual management of proxy materials like ballots, Power of Attorney documents, certificate of holdings leads to unauthorized voting	▪ Implement at the Securities Services Provider a centralized document management solution with tracking capabilities, including expiry of documents and identifiers for various entities covered by these documents ▪ Implement automated checks for various documentation leading to sufficient verification of Client and voting authority identities and their eligibility
Securities Services Provider does not send or sends incomplete or incorrect proxy voting event to the Sub-custodian / CSD	▪ Establish controls and exception alerts to ensure that the correct proxy voting event is identified and completed accurately ▪ Establish controls at the Securities Services Provider to ensure that proxy voting event is sent to the Sub-custodian / CSD ▪ Ensure reconciliation controls are in place between the Client / Securities Services Provider and the Sub-custodian / CSD

10.5.3 Class Actions Risk

Class actions require robust controls as the timeframes for the completion of a class action are usually long. Operational risks can arise when a class action is not identified by the Securities Services Provider, when a Client is not notified or does not respond to a class action or when active tracking of a class action is not undertaken.

Illustration 10.5.3 Class Actions Risk Table

Risk Description	Risk Mitigation
Class action event and details not identified by Securities Services Provider	▪ Ensure reliable feed of information from independent sources to enable comparison ▪ Ensure Securities Services Provider implements an SLA with Sub-custodian sets out requirements and that processes are carried out in compliance with CSD rule books and local market regulations
Client not informed of class action details	▪ Design an operating model at the Securities Services Provider to ensure class action information is auto calculated considering availability of position ▪ Ensure reconciliation of details received from Sub-custodian / CSD to Securities Services Provider's books and records ▪ Design operating model at Securities Services Provider to ensure accurate and complete data entry to maintain records of Client holdings and transaction histories to compute eligibility in class action
Client class action decision not acted on	▪ Implement automated tracking of class action decisions for all Clients
Client does not respond to class action information	▪ Establish controls for timely reminder to Client on lack of response ▪ Ensure contractual arrangement is in place between Securities Services Provider and Client documenting Client responsibilities including response times and deadlines ▪ Ensure Client notifications clearly articulate Client's rights, deadlines and process to participate in settlements
Securities Services Provider does not send, or sends incomplete, class action information to the Sub-custodian /CSD or class action agent	▪ Establish controls to ensure that the correct class action event is identified and completed accurately ▪ Establish controls, or exception alerts, to ensure that class action event is sent to the Sub-custodian / CSD or class action agent ▪ Ensure reconciliation controls are in place between the Client / Securities Services Provider and the Sub-custodian / CSD
Class actions not actively monitored by the Securities Services Provider and Clients over the long term	▪ Ensure authorized and verified Client payment details are maintained as class actions may take significant time to complete ▪ Active management by the Securities Services Provider and the Client of class actions in situations where the Clients has changed Securities Services Provider to ensure that class actions continue to be monitored and monies are paid out correctly once received

10.5.4 Income Processing Risk

Similar to corporate action processing, a key risk to a Securities Services Provider and Client is a failure to process the notification of income events and reconciliation of entitlements to a Client. Again, failure to complete this process could result in reputational risk.

Illustration 10.5.4 Income Processing Risk Table

Risk Description	Risk Mitigation
Income event and details not identified	▪ Ensure trusted source and feed of information from independent sources to enable comparison ▪ Establish controls to ensure the accuracy of manually received income events ▪ Ensure Securities Services Provider creates an SLA with Sub-custodian that sets out requirements and that processes are carried out in compliance with CSD rule books and local market regulations
Income not applied to Client entitlements	▪ Design an operating model, supported by technology, which ensures Client entitlements are automatically calculated considering availability of position and ensure position protected ▪ Ensure reconciliation of cash position received from Sub-custodian / CSD to Securities Services Provider's books and records
FX not applied in an accurate and timely manner per Client's requirements	▪ Provide automated tracking / booking of Client FX requirements
Events not tracked and Client not notified after announcement, missing changes to terms	▪ Ensure trusted source and feed of information ▪ Design an operating model, supported by technology, to automatically notify holders ▪ Devise a risk framework at the Securities Services Provider with control points to identify notification failures ▪ Implement STP reporting to aid timely and accurate notifications
Standing instructions (SIs) not applied to Client entitlements	▪ Ensure robust process for storing and applying Client SIs to ensure entitlements are correctly applied in accordance with Client's preference ▪ Ensure timely reporting to clients, in accordance with Client's SIs for entitlements
All or part of an entitlement is not received by Securities Services Provider from the Issuer	▪ Ensure an operating model, supported by technology, is in place which monitors Issuers' announcements and geopolitical situations in order to anticipate any issuer the Issuer may be experiencing / subject to ▪ Ensure reconciliation of cash position received from Sub-custodian / CSD to Securities Services Provider's books and records

10.5.5 Tax Processing Risk

A Securities Services Provider that offers tax services to its Clients must ensure that accurate and complete tax information is provided by each Client. As well as operational risks, a Securities Services Provider and its Clients could be exposed to financial losses and, potentially, fines for failure to provide complete information in the required timeframes.

10.5.5.1 Tax Relief at Source Risk

Applying appropriate tax relief at source, dependent on Client status and tax documentation, can be a significant risk. This is particularly the case in markets which prevent subsequent tax reclaims. The complexity of tax treaties and the development of tax transparent vehicles/funds have led to an increased risk of failure to perform activities, thus resulting in the expanded use of tax experts.

Illustration 10.5.5.1 Tax Relief at Source Risk Table

Risk Description	Risk Mitigation
Tax table set up incorrectly	▪ Establish an accurate tax table ▪ Ensure independent periodic reviews of tax rates
Appropriate tax rate not applied	▪ Ensure an independent review of the tax rate set up versus Client status ▪ Establish system-enforced dual 'create / approve' permissions and controls for tax rate set-up
Tax relief at source markets not identified	▪ Ensure trusted source and feed of information ▪ Ensure Securities Services Provider creates an SLA with Sub-custodian that sets out requirements and that processes are carried out in compliance with local market regulations / tax laws
Appropriate tax documentation not obtained from the Client prior to filing	▪ Establish diary events / controls for timely reminder to Clients for required tax documentation including renewals ▪ Establish monitoring / missing documentation reports, management information to identify areas of concern ▪ Ensure procedures are in place to identity that documentation is accurate and complies with all applicable AML rules (e.g. screening of UBO names against sanctions lists)
Tax relief at source instructions on Client holdings not generated	▪ Implement processes and controls to ensure set up of tax relief at source on Client holdings ▪ Establish tax relief at source reports and perform ongoing monitoring
Financial Transaction Taxes (FTT) / Stamp Duty not reported / paid	▪ Ensure understanding of which Clients are eligible / exempt from FTTs ▪ Automate identification of eligibility rules, payment and reporting requirements
Required tax authority reporting not completed	▪ Establish controls to follow and comply with relevant tax authority requirements ▪ Implement compliance monitoring to ensure awareness and compliance with any changes to the requirements
Client tax documentation not submitted to the tax authorities within the required timeframes	▪ Establish controls and monitoring process to ensure that required timeframes are known ▪ Ensure valid tax documentation is submitted within the required timeframes ▪ Reconcile the projected income payments between the CSD, Sub-custodian and the Global Custodian to identify any tax documentation discrepancies

10.5.5.2 Tax Reclaims Risk

Certain markets, whilst allowing tax reduction dependent on treaties and Client status, do not function on a particularly timely basis and can have prolonged timeframes to receive tax reclaims. A point of note here is the importance of the provision of payment details on file as there is the risk that the relationship between a Securities Services Provider and a Client may have ended before tax reclaim monies are received.

Illustration 10.5.5.2 Tax Reclaims Risk Table

Risk Description	Risk Mitigation
Tax table set up incorrectly	▪ Establish an accurate tax table ▪ Ensure periodic independent reviews of tax rates
Appropriate tax rate not applied	▪ Ensure an independent review of the tax rate set up versus Client status ▪ Establish system-enforced dual 'create / approve' permissions and controls for tax rate set-up
Tax reclaim markets not identified	▪ Ensure a trusted source and feed of information ▪ Securities Services Provider to ensure SLA with Sub-custodian sets out requirements and that processes are carried out in compliance with local market regulations / tax laws
Appropriate tax documentation not obtained from the Client	▪ Establish diary events / controls for timely reminder to Clients on required tax documentation including renewals ▪ Establish monitoring / missing documentation reports, management information to identify areas of concern ▪ Ensure procedures are in place to identity that documentation is accurate and complies with all applicable AML rules (e.g. screening of UBO names against sanctions lists)
Tax reclaims not generated	▪ Establish aged outstanding reclaim reports and perform ongoing monitoring
Tax reclaims not submitted in line with deadlines	▪ Establish reconciliation control between tax reclaim instructions received and submitted ▪ Establish monitoring of deadlines and follow-up process back to Client
Receipt of Tax reclaim monies not monitored	▪ Establish reconciliation processes with Sub-custodians and tax authorities ▪ Establish expected repayment schedules and monitor out-of-date reclaims
Financial Transaction Taxes (FTT) / Stamp Duty not reported / paid	▪ Ensure understanding of which Clients are eligible / exempt from FTTs ▪ Automate identification of eligibility rules, payment and reporting requirements
Tax overpaid in certain constituencies cannot be repaid and / or penalties levied on tax reclaims	▪ Additional control checks on tax rates in markets with low / no reclaim ability
Sufficient documentary evidence / proof of tax reclaim eligibility not obtained from Client prior to submitting reclaim (speculative / reclaim) leading to delays in reclaim, risk of losing tax agent status	▪ Ensure understanding of requirements in each constituency ▪ Establish detailed pre-reclaim validation process ▪ Ensure Client is aware of requirements and implications if not provided within the required timeline

Risk Description	Risk Mitigation
Required tax authority reporting not completed	▪ Establish controls to follow and comply with relevant tax authority requirements ▪ Implement compliance monitoring to ensure awareness and compliance with any changes to the requirements
Client tax documentation not submitted to the tax authorities within the required timeframes	▪ Establish controls and monitoring process to ensure that required timeframes are known by the Securities Services Provider ▪ Ensure Client is aware of the timeline and implications if not provided within the required timeline ▪ Ensure valid tax documentation is submitted within the required timeframes

10.6 Foreign Exchange Risk Threats

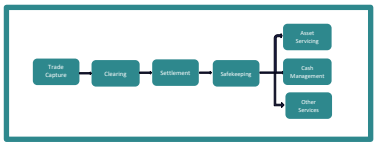
Risks associated with FX services are mainly operational, although reputational risk could occur if there are ongoing failures. From a Client perspective, disclosure of FX pricing methods from its Securities Services Provider is important as are clear and timely instructions. From a Securities Services Provider view, accurate and timely processing is assisted by straight through processes and standing instructions.

Illustration 10.6 Foreign Exchange Risk Table

Risk Description	Risk Mitigation
Clear FX pricing methodology lacking	▪ Ensure clear documentation between Securities Services Provider and Client that sets out standard approach to FX pricing
FX is not processed in an accurate, complete and timely manner in accordance with Client requirements	▪ Ensure clear account opening and FX standing instruction set up process and controls with system-enforced dual 'create / approve' permissions and controls ▪ Implement periodic review and confirmation of account set-up / standing instructions ▪ Implement a STP operating model with robust queue management ▪ Ensure a confirmation process is in place with full audit trail
FX settlement failure	▪ Selection of approved FX counterparties by Securities Services Provider ▪ Monitoring of exposures ▪ Use of counterparty netting (Continuous Linked Settlement) ▪ Robust daily reconciliation

11. Information Security and Data Protection Risk

11.1 Introduction



This chapter looks at how a Securities Services Provider ensures the security of information and protection of data through implementing measures such as network security, application security, endpoint security and cyber security. Each of these measures needs to be managed to ensure the ongoing confidentiality, integrity and availability of the Securities Services Provider's and Client's data.

11.2 Definition

Information security and data protection risk is the risk to a Securities Services Provider of exposure and vulnerability to threats and cyber-attacks associated with the operation and use of information systems. Threats can be due to internal or external factors, can materialize in both electronic and physical ways and can compromise organizations through different methods, such as malware, social engineering or supply chains.

11.3 The Information Security Landscape

Whilst the theft of assets and cash is often a key threat to a Securities Services Provider, it could also be exposed to the theft of valuable information. The books, records and databases held by Securities Services Providers could provide criminals with access to sensitive data such as client investments, portfolio details, performance and strategy, relationship information and fee agreements. Cyber and ransomware attacks could also lead to substantial damage to Clients and to Securities Service Providers being able to execute critical services.

Nation states advanced persistent threat (APT) groups and organized criminal gangs are becoming more sophisticated creating a significant challenge for security professionals tasked with protecting data. Cyber space remains a preferred operational domain for a wide range of industrial espionage and a means for some nation states to support their economic policy objectives. These threat actors, if successful, may remain resident on a Securities Services Provider's information systems to obtain information for their state sponsor's foreign policy objectives.

A strong information security programme, with a robust set of information security controls, is therefore critical to ensure the safety and soundness of a Securities Services Provider's information. Securities Services Providers rely heavily on the information technology systems that support their ongoing activities. Deploying a defence in-depth strategy that builds upon concentric rings of defences is the most generally accepted way in which to ensure malicious computer activities are prevented.

Information Security measures, such as network segregation, isolation from the internet and resilience, are designed so that single points of failure do not result in the complete compromise of critical resources or systems. Protections are used on the external perimeter, the internal areas and the most sensitive or valuable locations. It is expected that problems will occur in various locations and defences will be tested by those attempting to do harm.

A properly built environment will ensure that a failure of one component does not directly result in a failure of the entire system. This involves 'layered defences', 'defence in depth', 'security by design', 'least privileged accesses', 'need to know accesses', 'segregation of duties', 'assumed breaches' and the implementation of a set of strong controls to enforce them.

In order for an Information Security programme to be effective, it is key to first understand what the programme is trying to protect. Identifying critical processes and data sets helps build the foundation for strong security practices. A Securities Services Provider may use data classification schemes to continually identify what elements of their organization are most important and therefore requires the most effort to protect. Conducting risk assessments of an organization's applications, infrastructure and critical processes will also assist in directing efforts on a prioritized approach. Not all areas are equal, nor do they require or demand the same levels of protections. Understanding what needs to be protected and how best to protect it helps to ensure a reliable Securities Services Provider Information Security framework.

Continuing Information Security developments, and a reliance on changing technology (e.g. robotics, machine learning, artificial intelligence, cloud data storage, cryptocurrencies and blockchain), all impact Securities Services Providers. The Information Security threat is therefore likely to increase and organizations must continue to invest in risk mitigation strategies and develop Securities Services' specific collaborative and active intelligence networks and mitigation techniques.

11.4 Key Areas of Information Security and Data Protection Risk

Within the Securities Services value chain, one can distinguish between four broad clusters of Information Security and Data Protection risks which may be either internally or externally introduced. Below, the key threats - and the motives behind them - are identified.

11.4.1 Cyber-Attack

Significantly adverse consequences associated with cyber-attacks are seen on a far too regular basis across many industries, services and infrastructure environments. This threat is real and requires detailed and constant focus for those operating within the Securities Services industry. As seen in other industries such as healthcare, education and energy, major cyber-attacks - driven by a desire to materially disrupt key infrastructure - are among the most material and impactful of the Information Security threats faced. Securities Servicers Providers are the infrastructure of the investment sector and disruption to CSDs, globally and domestically significantly important financial services firms (including Global and Sub Custodians), together with the industry wide utilities (such as SWIFT and other large industry vendors) could have a major adverse effect on the flow of monies at a national and international level.

A Securities Services Provider is largely required under local regulation to implement an industry-accepted cyber security framework. Standards, such as ISO 27000 series, NIST Cybersecurity Framework and Cyber Risk Institute

Financial Services Profile, exist to help benchmark a Securities Services Provider's cyber security policies, standards, controls and procedures. In the event of a cyber-attack, management must react rapidly to detect the attack, isolate the issue and assess the impact. Major security frameworks therefore typically base their defensive controls around 'govern, identify, protect, detect, respond and recover'.

While a Securities Services Provider clearly needs to have a robust cyber security framework, it also needs to assess the risk to itself of cyber-attacks on its Clients, Third-Party Providers and counterparties. Due diligence of the cyber risk management programme and associated controls of these parties is critical. Appropriate contractual obligations should be placed on these parties to meet the policies and standards of the Securities Servicer Provider, which can include an attestation process of the party to provide their status in complying with these standards.

Of all the cyber-attacks that could create a systemic market impact, a ransomware attack against a large Securities Service Provider is one of the potentially most damaging. A ransomware attack against a Securities Services Provider could result in significant market liquidity issues and eliminate the ability of the Securities Services Provider to service its Client's assets. While SIFIs and large financial institutions may have stronger defences to protect against these attacks, it is plausible that a motivated threat actor could perpetrate this crime. In this case, the reach could be wide and the impact could be very high to the market.

The motive for a cyber-attack is usually either financial gain or to further a nation state's economic policy.

CASE STUDY: ICBC

ICBC Financial Services, a subsidiary of the Industrial and Commercial Bank of China (ICBC), experienced a ransomware attack on 08 November 2023. The incident disrupted the ICBC operations and systems affecting the service levels of execution of customer transactions and communications. The incident raised generic concerns about the cybersecurity posture of financial institutions.

ICBC took action when the cyber-attack was discovered, by reporting the incident to law enforcement while co-ordinating with cyber security experts. The incident was also reported publicly in an article published by the Financial Times on the following day.

The attack was reportedly carried out by the hacking group LockBit, a ransomware-as-a-service (RaaS) group that has been active since September 2019. Their ransomware is used for highly targeted attacks against enterprises and other organizations. It is also known as a 'crypto virus' due to forming its ransom requests around financial payment in exchange for decryption. It is a self-spreading virus that blocks user access to computer systems. It targets enterprises and government organizations globally with some of the following threats: operations disruption with essential functions coming to a sudden halt, extortion for the hackers' financial gain, data theft and illegal publication as blackmail if the victim does not comply.

11.4.2 Asset Theft

A Securities Services Provider may be particularly susceptible to asset theft. This is because it moves significant values of transactions daily, particularly securities delivery / receipt versus payment (DvP / RvP) settlement instructions, large bond maturity payments, corporate actions, dividend and income payments, tri-party repo payments and deposits.

The motive for asset theft is generally financial gain.

11.4.3 Information Theft

The risk of theft of sensitive information is particularly of concern to a Securities Services Provider. This could include the theft of:

- Intellectual property, such as Client contracts, pricing schedules, product or service information
- Sensitive Client data, such as securities positions, holdings, statements and personal contact details

The motive for information theft may be for an advantage over a competitor organization or to potentially cause reputational damage if the information is purposefully leaked. Depending on the amount and type of information stolen, information theft could be used to further a nation state's economic policy. The theft may also be used for financial gain, either through extortion of a ransom in exchange of maintaining confidentiality or through trading on the basis of undisclosed information.

11.4.4 Market Manipulation

Market manipulation is the risk of manipulation of pricing and / or news feeds from a coordinated APT attack. Stock prices would adjust automatically and buy/sell orders would be fulfilled automatically, resulting in potential financial gain if the attackers were stockholders. For a Securities Services Provider, this could include manipulation through:

- Multiple, simultaneous buy and sell orders on a stock, where the increased trading activity artificially increases the stock's price
- Simultaneous rumours or 'fake news' on a stock, by illicitly manipulating multiple newswires or news sources
- Simultaneous manipulated intraday pricing feeds from established financial data Third-Party providers
- Changing the terms of a complex reorganization or Corporate Action, such as a merger, to artificially impact its attractiveness to the market
- Penetration and compromising a pricing feed from a Third-Party Provider or newswire to affect the price of a specific stock, which would then allow the threat actor to buy or sell at the artificial price. As the system or network compromise is physically far from the financial transaction, this type of illicit trade could be difficult to trace

The motive for market manipulation is financial gain, whereby the threat actor seeks to artificially manipulate the price of an asset.

11.5 Information Security and Data Protection Risk Threats

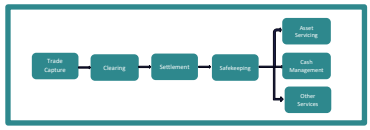
The table below highlights the key Information Security and Data Protection risk threats that could impact a Securities Services Provider.

Illustration 11.5 Information Security and Data Protection Risk Table

Risk Description	Risk Mitigation
Lack of confidentiality of securities in transit	▪ Ensure that data is properly encrypted when electronically transmitting securities instructions (e.g. SWIFT) ▪ Use secure communications protocols or channels when transmitting securities data, such as Secure Sockets Layer (SSL) Secure File Transfer Protocols (SFTP) or electronic banking like solutions
Lack of confidentiality of securities in storage	▪ Use data encryption when storing securities data on file systems or in databases ▪ Establish strong logical access controls and user privilege systems based on 'need to know' principles with periodic renewal and review process ▪ Ensure data encryption routines are in place that provide sufficient strength against brute-force attacks
Suspicious activity not detected	▪ Deploy Intrusion detection systems to monitor for suspicious traffic ▪ Follow a logging and monitoring strategy for critical systems that ensures all electronic communication and actions are properly interrogated for suspicious behaviour
Awareness amongst staff on expected information security practices is lacking	▪ Create and implement robust training programmes that educate the user population on expected behaviours and proper information security practices ▪ Develop awareness campaigns ▪ Ensure regular 'organized educational' phishing attempts
Securities processing systems vulnerable to electronic attack	▪ Deploy vulnerability management programmes that ensure securities processing systems are not susceptible to current threats ▪ Create patch management routines to ensure that systems are patched on a regular basis as new vulnerabilities are released ▪ Leverage penetration testing programmes to help simulate real world attacks and how to best defend against manual techniques
Access privileges of employees to securities data are not properly managed	▪ Implement identity and access management programmes that manage all aspects of the identity lifecycle ▪ Leverage access re-certification to ensure that individuals who no longer require access to securities data have their access revoked ▪ Implement multi-factor authentication for critical systems ▪ Ensure termination routines are in place that monitor for employees who leave the firm so their access is properly removed from critical securities processing systems
Technology systems are not hardened against possible cyber attack	▪ Maintain and deploy hardening documents (security baseline documents) and automated scripts to increase resiliency of technical systems against possible attack ▪ Evaluate system configurations on an annual basis to ensure that required changes are incorporated into the baseline

12. Information Technology Risk

12.1 Introduction



Similar to the information provided in the chapter on Information Security and Data Protection, Securities Services activities rely heavily on the underlying technology infrastructure to operate each day. An unreliable or unstable technology system can result in the lack of processing abilities and essentially leave a Securities Services Provider in an inoperable state. It is therefore important that Securities Services Providers understand Information Technology risk and how these can positively or negatively impact operations.

12.2 Definition

Information Technology risk is a broad category and, effectively, is used to define just about anything that can go wrong within a technology environment. This therefore includes threats to data, processes and / or critical systems.

12.3 Reliability and Resiliency

One of the primary areas that Information Technology risk focuses on is reliability. Systems must be built with appropriate resiliency which ensures they continue to operate during times of crisis.

12.3.1 Business Impact Assessments

The extent to which a system must continue operations during an incident is defined via a comprehensive Business Impact Assessment. On a review basis, aligned to the Securities Service Provider's risk appetite, each Securities Services Provider must evaluate the impact an outage may have on each product and service they operate. These assessments must review legal, regulatory, and contractual requirements while defining the overall impact an outage would have on the organization.

A Securities Services Provider must ensure that there is a clear understanding of which systems are business critical and prioritize funding accordingly to protect these systems. Equally important will be to determine a location strategy and understand how much infrastructure must be built and run out of one - or more - separate locations, as well as taking into account geopolitical considerations (see chapter on Geopolitical risks for further information).

Finally, consideration should be given to ensure cross-regional recovery arrangements exist for critical business activities to enable recovery of workload from one operational location to another. As with other business contingency arrangements, cross-regional recovery arrangements should also be tested.

12.3.2 Recovery Time Objective

Based on the results of the impact analysis, a Recovery Time Objective is determined. This objective is then factored into the overall business continuity strategy.

Choosing accurate recovery times is critical to ensure appropriate continuity of business, particularly for critical businesses both to a Securities Services Provider and to the broader industry. For example, a critical system or product could be defined as requiring a two-hour recovery time. In this case, technology must be deployed to ensure that even during unexpected outages, the product is able to limit itself to no more than two hours of unavailability. Given the systemic importance of the financial sector, there are regulatory requirements determining recovery time objectives and mandating regular system recovery testing. Notwithstanding this, a Securities Services Provider will have multiple intraday market deadlines to meet to ensure securities and cash transactions are completed and, therefore, depending on the time of day an incident occurs additional business contingency actions may need to be planned.

12.4 Information Technology Frameworks

Generally accepted Information Technology risk frameworks exist that articulate areas of focus when creating a robust Information Technology risk programme.

Two of the most common Information Technology risk frameworks currently used are highlighted below. Both of these frameworks provide exhaustive examples of best practices when looking at broader Information Technology risk programmes.

- International Standards Organization (ISO) 20000 – Information Technology Service Management
- Information Technology Infrastructure Library (ITIL) 4

A Securities Services Provider implementing artificial intelligence systems may also consider the following possible frameworks:

- ISO 23894 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO 42001 - Information technology Artificial intelligence, guidance on risk management

12.5 Information Technology Risk Threats

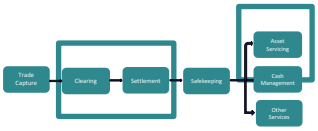
The table below highlights specific risks from a Securities Services Provider standpoint and, therefore, acts as a subset of material covered under the wider frameworks.

Illustration 12.5 Information Technology Risk Table

Risk Description	Risk Mitigation
Technology inventory of securities systems is lacking	▪ Ensure the Information Technology management system has all components required for operating the systems, an up-to-date licence and that expiry records and renewals occur in time ▪ Deploy an Information Technology management system that tracks and catalogues technology assets / systems important to securities processing ▪ Identify the system owner in the Information Technology management system for each technology component to ensure proper individuals are notified if system issues occur
Limited testing exists prior to moving securities applications into production	▪ Create a quality assurance team to test all aspects of securities systems prior to an application being moved into production ▪ Perform - if possible - 'smoke' tests on the live the systems in a way not disrupting the operations before putting them into production ▪ Perform regression testing to ensure new features do not cause adverse impact on legacy activities ▪ Create roll back routines to ensure that new changes can be backed out of production environments if system disruptions occur
Poor capacity planning results in system performance issues	▪ Use performance management systems to monitor system utilization and identify any system spikes ▪ Ensure technology build plans consider existing performance management metrics, combined with projected growth requirements and consider stressed environment
Back-up procedures for interfaces are lacking	▪ Complete testing and monitoring the operation of interfaces between the securities system, cash system, CSDs and external data sources ▪ Implement back-up procedures for contingency / outages ▪ Implement defined recovery times in compliance with regulatory and SLA requirements
Limited change management practices available resulting in loss of integrity of securities platforms	▪ Document all production level changes as part of a formal change management programme ▪ Effectively manage notification and approval of all system changes ▪ Maintain logs that track all system changes in order to facilitate troubleshooting potential incidents
Infrastructure running securities processing systems results in system outages which are not monitored	▪ Leverage a technical operations centre to monitor activity across all aspects of an Information Technology programme ▪ Configure alarms to alert personnel to unusual or concerning system behaviour ▪ Escalation protocols should be established to effectively communicate system problems
Poor 'Incident response practices' results in place causing prolonged recovery times	▪ Implement an incident management function which acts as an escalation element of an existing monitoring function ▪ Ensure incident management routines exist which include proper notification and escalation for all potential incidents. This could include single point of contacts, different communication channels and escalation mechanisms
New technology adopted without sufficient knowledge or experience	▪ Complete an assessment of any new technology, such as AI ▪ Adopt an accepted industry framework for new technology where available

13. Credit Risk

13.1 Introduction



Credit risk for a Securities Services Provider can originate from on-balance sheet obligations - such as loans or other credit facilities – should a Client fail to make the required repayments. Credit risk can therefore be created by items such as trade settlement, counterparty credit risk and securities lending indemnifications, as well as letters of credit. Credit risk for a Client can originate from on-balance sheet items held at a Securities Services Provider, such as cash deposits, in the event of that Securities Services Provider's default.

As a regulated entity, a Securities Services Provider should take actions such as deploying an appropriate credit risk assessment, limit setting and exposure monitoring to ensure the extent of credit taken does not breach its risk appetite and / or regulatory restrictions (such as large exposure rules). In the same way, Clients should complete a credit risk assessment of their Securities Services Provider. This chapter explores these actions, the risks in extending credit and the potential mitigants.

13.2 Definition

Credit risk is the risk of loss arising from debtor's failure due to its inability or unwillingness to perform its financial obligations on time and in full (e.g. arising from a credit facility granted to a borrowing participant). For a Securities Services provider, a debtor will mainly be its Client, a trading or a treasury counterpart.

13.3 The Credit Risk Landscape

There are multiple participants involved in the Securities Services lifecycle and, as a result, the need for credit may occur at many junctures. Participants taking credit risk will include Securities Services Providers (Global Custodians, Sub-custodians and (I)CSDs) as well as Clients.

As banker to the Client, a Securities Services Provider will provide a demand deposit account for the purposes of the Client funding its investments and operating costs and for receipt of investment proceeds and income collection. A Securities Services Provider may choose to provide the Client with credit facilities (particularly intraday credit) for the purposes of enabling the Client to fulfil settlement obligations or advancing income monies when not yet received from the Issuer or counterparty to a matched trade. A Securities Services Provider may also choose to provide these as unadvised and uncommitted facilities and therefore may decide, based on country and counterparty reasons, to remove these.

A Securities Services Provider will perform analysis and set limits taking into account the obligor rating, security (types and value of assets it has a lien on) and the financial capacity / capital adequacy of the lending legal entity. In addition, there are certain markets (for example Middle Eastern markets) where overnight exposure / overdrafts are not permitted and for which a Securities Services Provider cannot provide facilities. As organizations with very low risk appetites, CSDs usually operate a conservative credit policy and, consequently, credit lines are, in principle only granted against collateral.

A credit risk also arises for a Client when holding a cash account with a Securities Services Provider (e.g. a Global Custodian or Sub-custodian for certain restricted markets). The Client must ensure they have performed their own credit analysis on the specific legal entity they have the credit exposure to, which may also include a concentration risk analysis. Clients should also consider the extent to which government backed deposit guarantee schemes exist and whether deposit preference rules apply (which may give preference to certain depositor domiciles over others).

13.4 Key Areas of Credit Risk

Credit risk can occur at multiple points in the Securities Services value chain. The key areas of credit risk for a Securities Services provider are therefore outlined below.

13.4.1 Clearing

A Securities Services Provider offers the Client the capability to execute "on exchange" trades and must ensure that the Client is able to meet all its daily settlement obligations and the obligations to the exchange for maintaining margin payments. The Securities Services Provider - operating in a GCM capacity - is exposed to credit risk due to taking principal risk for its client's trade executions and therefore assuming liability to the CCP in the invent of settlement failure or its client's insolvency. To protect against this liability (between trade and settlement date including any price fluctuations in the trading price 'mark-to-market exposure') a Securities Services Provider will take eligible collateral from the Client to mitigate this risk.

The CCP protects itself by holding initial margin from both the buyer and the seller to ensure that downward changes in value are covered. It also marks to market daily to ensure that both parties are able to fulfil their obligations.

A Securities Services Provider will mitigate its risk through a thorough and ongoing risk management analysis on the Client and set limits on the client ability to execute trades and resulting settlement obligations. The Securities Services Provider also needs to make sure the Client has available collateral such as securities or cash available to meet any margin calls and the cash proceeds to meet the daily CCP cash settlement obligation. Where this collateral is insufficient, a margin call is made for additional eligible collateral.

This clearing facility is normally conducted on a Third-Party agency basis. This is where the Client has the direct account relationship with the clearing organization and appoints a Securities Services Provider to operate this account on the Client's behalf. Service level agreements and contracts will clearly outline the account operations. In the event that the Client cannot provide funding on time there is a risk that a Securities Services Provider holds assets as principal until those securities are fully paid for by the Client. Should this event happen, the Securities Services Provider is exposed to both credit risk to the Client and market risk on the value of the securities.

Given the substantial obligations that can be incurred due to on exchange trading, these arrangements demand a high level of risk analysis automation and price feeds to continuously monitor the Clients' trading activities and resulting collateral requirements. Clear actionable procedures and agreements need to be in place that allow a Securities Services Provider to effectively "stop the clearing" in the event of breach of agreement or Client distress/ insolvency.

13.4.2 Settlement

A clear credit risk is the risk that securities are delivered to the trade counterparty, however, payment is not received or payment is sent but securities are not received. Both situations would lead to a credit exposure to a Securities Services Provider and, ultimately, the Client.

To mitigate this credit risk, simultaneous exchange of securities and cash (Delivery vs Payment; Receipt vs Payment) has been introduced. However, there are both different types of DvP/RvP models by market (including individual transaction based simultaneous exchange through to exchange based on netting securities and / or cash obligations), together with certain more frontier markets that have yet to implement true DvP / RvP. Additionally, not all transaction types can benefit from a DvP / RvP arrangement; for example corporate actions including IPO's may require cash to be paid prior to receipt of securities / asset of value.

Additionally, markets operate on differing settlement cycles after trade date - the longer the cycle the greater the credit risk. In challenging market conditions this can create uncertainty in relation to whether a trade will settle or not. To reduce this risk, most markets now operate on a Trade Date Plus Two (T+2) settlement cycle and some have moved – and others are planning to move – to a T+1 or same day settlement cycle.

13.4.3 Contractual Settlement

A Securities Services Provider will frequently offer contractual settlement date accounting. In this situation, a Securities Services Provider takes a decision based largely on the country risk of a particular market to reflect posting on the Client account at the expected value date of the security settlement rather the actual settlement date. In the context of contractual settlement of sales proceeds, a Securities Services Provider is taking a credit risk on the settlement counterparty for receipt of the monies as well as a credit risk on the Client should the Client become insolvent and the monies cannot be received from the market.

A Securities Services Provider performs settlement pre-matching and affirmation (positive and negative) in accordance with local market conventions. Timeframes / deadlines vary per market but is normally on the day before settlement date (SD-1). In some markets, pre-matching / affirmation constitutes a binding obligation on a Securities Services Provider (under local regulations or depository participant rules) to settle the trades on settlement date. In such instances, in the context of contractual settlement of purchased securities, a Securities Services Provider assumes credit risk exposure on its Client at the point of matching / affirmation should the Client fail to provide sufficient funding on settlement date.

A Securities Services Provider, considering the extension of contractual settlement services, must take into account applicable laws and regulations. These may vary by jurisdiction and regulator (e.g., UK CASS rules, U.S. federal banking law and regulations, etc.).

13.4.4 Contractual Income

A Securities Services Provider may also offer contractual income date accounting in certain markets. Again, the Securities Services Provider takes a decision based largely on the country risk of a particular market to reflect posting on the Client account at the expected value date income payment date rather than the income posting date. In this situation, a Securities Services Provider is taking a credit risk on the Issuer for receipt of the monies.

Again, all applicable law and regulation should be considered in the context of the provision of contractual income.

13.5 Credit Protection Clauses

A Securities Services Provider will typically have recourse to client assets, including (often) cash accounts. Such recourse typically protects against the risk of loss from client failure to fund settlement or to pay the Securities Services Provider's fees and are framed as security against debt and/or in satisfaction of a debt. This recourse generally is set out in the contract with the client but can also arise under law. In addition to addressing credit risk concerns, the presence or absence of recourse may affect regulatory capital considerations for Securities Services Providers.

Applicable local law (usually the law governing the securities - or cash - account at the Securities Service Provider) may stipulate requirements that must be met in order for this recourse to be effective and may also limit the effective recourse actually available. Therefore, it is important to consider the possibility that the exercise of recourse may be limited by law, regulation or regulatory guidance. For example, if cash accounts are included, there could be regulatory constraints on the Service Provider's ability to utilise "set off" as well as other requirements intended to protect clients (see, e.g., UK CASS 7).

Recourse to assets typically comprises two aspects: a right of retention and a right of sale.

13.5.1 A Right of Retention

This is where the Securities Services Provider that is holding or controlling Client assets, despite not being the owner of the assets, can retain either specific Client assets (e.g. assets connected with a particular transaction) or assets whose value corresponds to the debt. Retention of assets at a greater value - or held outside the scope of the service being provided - may be challenged for effectiveness under local laws or compatibility with regulation. In any case, the permissibility of such additional rights should be reviewed carefully.

In and of itself, a right of retention does not give a right to sell the assets, so will not discharge the debt. However, it can be used to secure payment by the debtor Client (a lien is an example of a right of retention).

13.5.2 A Right of Sale

This is where the provider can dispose of Client assets and retain the proceeds of sale in satisfaction of a debt and typically permits the Securities Services Provider to assume ownership of the assets prior to the exercise of the right of sale. The Securities Services Provider will also usually have a right of retention which may have been (or may be required to be) exercised prior to the exercise of the right of sale.

Local laws may create mechanisms providing for the availability and exercise of both rights, but each right may need to be specifically provided for in the contract.

Generally, all parties to an arrangement providing for recourse to assets should consider:

- Applicable legal or regulatory requisites such as whether a collateral arrangement must be evidenced in writing (and how) and whether and how collateral is 'provided' to, "controlled" by or in the "possession" of the Securities Services Provider
- Certainty in describing the securities or securities accounts which are the subject of either or both rights
- Compliance by the parties with requirements to ensure the rights are effective (e.g., any requirement to register the rights)
- Any other rights relating to the securities or accounts (including underlying client rights, or rights already given by the client to third parties (e.g., financing arrangements) and whether the rights (of retention or of sale) remain effective
- Prior steps and mechanics necessary to give effect to either or both rights

13.6 Credit Risk Threats

The table below highlights the key credit risk threats that could impact a Securities Services Provider and / or Client.

Illustration 13.6 Credit Risk Table

Risk Description	Risk Mitigation
Client defaults on credit facility due to inability or unwillingness to meet its financial obligations	▪ Credit risk strategies (Risk Appetite Framework) should be established for Clients including lending strategies, regularly reviewed credit ratings and limits to industries / countries ▪ Ongoing monitoring of overall exposures should be implemented ▪ Prudent underwriting ▪ Prudent past due loan management, collection and workout ▪ Proper management of intraday credit risk facilities (minimizing potential exposure per borrower and in general in e.g. large exposure (lending not to exceed jurisdictional allowed percentage of eligible capital)) should be in place ▪ Technology capabilities to immediately stop any cash debits and securities deliveries in the event of a trigger event
Credit loss during the course of settlement of a transaction arising from failure to receive cash or assets after already delivered having cash or assets to the second party	▪ Credit assessment of counterparties ▪ Implementing limit facilities with counterparties for counterparty credit risk and settlement purposes
Client is no longer able to obtain foreign exchange (FX) to service its external debt (for example as a consequence of convertibility restrictions)	▪ Continuous monitoring of individual countries ▪ Continuous monitoring of Clients and where they have business ▪ Termination of further business in case of triggering events, risks

Risk Description	Risk Mitigation
Securities Services Provider and / or Client are negatively impacted due to a global or regional geopolitical event or developments in a country's economy (e.g. sovereign debt default)	▪ Credit risk strategies (Risk Appetite Framework) on institution level setting up lending strategies and limits to industries, countries ▪ Ongoing monitoring of overall exposures per country / region ▪ Prudent underwriting, strict limit management to countries ▪ Continuous monitoring of individual countries ▪ Termination of further business in case of triggering events leading to risk outside appetite

14. Liquidity Risk

14.1 Introduction

From the perspective of a Securities Services Provider, fulfilling the settlement obligations of its Client with the CSDs, central banks and Sub-custodians may give rise to liquidity risk where a Securities Services Provider cannot access funding. A Securities Services Provider may also experience liquidity challenges where cash going out significantly exceeds cash coming in (e.g. significant RvP transactions processed above DvPs).

14.2 Definition

Liquidity is defined as the ability to access funding, convert assets to cash quickly and efficiently or to roll over / issue new debt - especially during periods of market stress - in order to meet short-term obligations.

14.3 The Intra-Day Credit Risk Landscape

A Securities Services Provider is especially exposed to intra-day liquidity risk. Intra-day liquidity risk, and its measurement, has been a significant area of focus by the Securities Services community - and their regulators - driven by the significant increase in exposure values as well as by the complexity of managing intra-day liquidity needs arising from settlement activities in different time zones.

Moreover, with the trend towards a reduction of settlement cycles from two to one business day, liquidity processes are being compressed into a shorter timeframe which will be particularly challenging for cross-currency transactions having an FX component.

The following funding requirement changes have been noted:

- Changing credit appetite (particularly for intra-day credit), and reduced access to cheap credit, has increased pre-funding requirements by many market participants
- Changes to settlement timelines has also increased the need to fund the night before settlement date (e.g. T2S, T+1)

14.4 Liquidity Risk Threats

The table below provides the liquidity risk threats for Securities Services Providers, as well as their Clients.

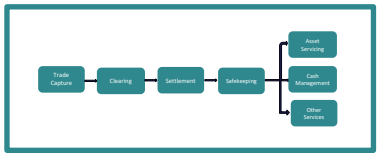
Illustration 14.4 Liquidity Risk Table

Risk Description	Mitigation
Services not maintained by Securities Services Provider due to lack of liquidity	▪ Complete a comprehensive internal liquidity adequacy assessment process (ILAAP) ▪ Implement a liquidity management system

Risk Description	Mitigation
Funding by Securities Services Provider cannot be accessed on time	▪ Ensure access to accurate liquidity management ▪ Ensure access to Central Bank funding lines where appropriate
Increased collateral requirements from Securities Services Provider not recognized by Client	▪ Securities Services Provider and Client to manage and monitor intra-day credit requirements together an ongoing basis
Funding by Client cannot be accessed on time	▪ Implement a liquidity management system by Client to manage flows (to assure it works during periods of market stress as well) ▪ Select a financially strong Securities Services Provider

15. Systemic Risk

15.1 Introduction



The Securities Services industry is key to the functioning of the broader financial system. The Securities Services value chain also implies interconnections and interdependencies between multiple Securities Services Providers and FMIs. This chapter focuses on the risk of a breakdown of the entire financial system - rather than a failure of one or more institutions - and the measures that can be taken to mitigate the impact of this risk materializing.

15.2 Definition

The International Monetary Fund (IMF), the Financial Stability Board (FSB) and the Bank for International Settlement (BIS) formally define Systemic Risk as the risk of widespread disruption to the provision of financial services that is caused by an impairment of all or parts of the financial system and which can cause serious negative consequences for the real economy. A financial system is considered stable when financial institutions are able to provide households, communities and businesses with the financing they need to invest, grow, and participate in a well-functioning economy.

Among these financial institutions, there are systemic institutions, the so-called Systemically Important Financial Institutions (SIFIs). The FSB defines a SIFI as a financial institution whose distress or disorderly failure, because of their size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity. Due to FMIs being at the heart of the financial system - and having a major role to play to ensure its stability - FMIs are de facto regulated as systemic entities.

15.3 Assessing Systemic Importance

In practice, there are two ways of measuring the systemic importance of a financial institution or infrastructure in the system. The first approach relies on information on positions and risk exposures, which is typically confidential and only shared externally with regulators. The second approach relies on public market data, such as stock returns, option prices, or credit default swaps, as they are believed to reflect all information about publicly traded firms.

While several prominent examples of such measures have been proposed over time (the Marginal Expected Shortfall, the Systemic Expected Shortfall, the Systemic Risk Measure, the Delta Conditional Value-at-Risk), they can, more simplify, be categorized as two different types:

- Measuring the expected capital shortfall of an institution conditional on a financial crisis occurring
- Measuring the Value-at-Risk of the financial system conditionally on a specific event affecting a given firm

In other words, all attempts to formally measure systemic risk, so far, have:

- Been structured around the interactions between a firm and the system it is a part of

- Distinguished between the impact of the firm (in distress) on the system and the impact of the system (in distress) on the firm

15.4 Key Concepts of Systemic Risk

For a Securities Services Provider, apart from the quantitative measures, systemic risk can also be articulated around several key concepts. These include:

- Inbound and outbound systemic risk
- Contagion and amplification
- Concentration and Interconnectedness

15.4.1 Inbound and outbound systemic risk

This notion of directionality is important. Indeed, as part of the very system whose risk is being assessed, a Securities Services Provider needs to distinguish between the risk the system poses to it (inbound) and the risk it poses to the system (outbound). This distinction between the risks taken (and thus the resilience to systemic stress) and the risks posed (and thus the contribution to systemic stress) is fundamental. This is also why there is a need to distinguish between “stress” and “vulnerability”. When systemic risk materializes, the organization at the origin of the problem is deemed to be releasing stress (outbound) that other industry players need to absorb (inbound), which they will do if they do not suffer from material vulnerabilities.

15.4.2 Contagion and Amplification

Contagion and amplification are mechanisms at work during events which can have a systemic impact. Contagion can turn an isolated incident into a widespread incident and amplification can turn a minor incident into a severe incident. Both mechanisms are typically at work in systemic events, which impact a significant number of Securities Services participants in a material way.

Contagion can take several forms. It can be direct (e.g. bilateral exposures) or indirect (e.g. information spillovers). Amplification can also take several forms, such as negative feedback loops or pro-cyclicality.

15.4.3 Concentration and Interconnectedness

By their scale and interconnectedness, a large Securities Services Provider spares other market participants the need to establish more bilateral relationships than they already have. Concretely, by leveraging the Securities Services value chain to access one or several markets, Securities Services participants avoid the need to set up multiple other bilateral arrangements with other participants in the different markets. So, while a Securities Servies Provider supporting the Securities Services value chain concentrates the risk of Securities Services participants (who become more dependent on them), they simultaneously reduce the level of interconnectedness in the market. There is thus a trade-off between concentration and interconnectedness.

15.5 Systemic Risk Threats

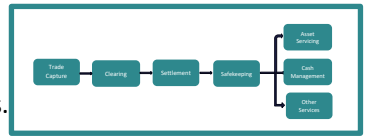
The following table shows the key system risks and how they can be mitigated:

Illustration 15.5 Systemic Risk Table

Risk Description	Risk Mitigation
Policy not in place at Securities Services Provider for handling systemic risk events	▪ Implement suitable internal senior management policy covering key systemic risk factors and approach ▪ Ensure that both inbound and outbound risks are documented and understood ▪ Have a comprehensive suite of management reporting tools on systemic risks
Outbreak of war in a systemically relevant country	▪ Identify and assess countries where high-risk probability of war ▪ Limit exposure to high-risk markets, activities and Clients should an event appear imminent ▪ Terminate contracts, or make alternative arrangements, in the event of war
Market crash occurring	▪ Monitor and assess continuously the state of global markets ▪ Ensure processes in place to manage a market crash
SIFI or FMI failure	▪ Assess and document concentration risks against other Securities Services participants and have in place arrangements to move to other participants in the event of a fundamental issue or failure ▪ Incorporate training to ensure that staff understand their responsibilities and the action and escalation requirements should a failure occur

16. Geopolitical and Geoeconomic Risk

16.1 Introduction



The geopolitical and geoeconomic landscape, for financial institutions, has changed significantly in recent years. Geopolitical events and geoeconomic goals can threaten financial stability and can cause major disruption to both organizations and countries. Multiple risks can occur when geopolitical and geoeconomic events occur which impact financial firms, such as sanctions, uncertain and changing global alliances as well as capital outflows. Therefore organizations need to be constantly assessing the geopolitical climate.

This chapter explores the changing geopolitical and geoeconomic landscape and highlights some of the key events that have occurred over recent years that have impacted the Securities Services industry. It also identifies the different risks to a Securities Services Provider that could arise in the event of a geopolitical and / or geoeconomic issue arising and what mitigants are available to minimize the impact of these risks.

16.2 Definition

Geopolitics is where a country or organization uses political power and influence to secure national interests. On the other hand, geoeconomics is the use of economic activities and resources in order to gain economic benefits.

Geopolitical and geoeconomic risks therefore consist of exposure to the effects of:

- Political instability
  This includes changes in government, political unrest, or conflicts
- International relations
  International relations includes diplomatic tensions, military conflicts, or alliances between nation states or supranational blocs
- Social unrest
  Social unrest comprises protests, strikes, or social movements
- Economic policies
  These include policies such as financial relationships, trade restrictions, tariffs, sanctions, or changes in economic policy

By nature, the Securities Services industry is a global one, involving the holding assets in one jurisdiction in order to support participants in others. Securities Services Providers are therefore inherently sensitive to geopolitical and geoeconomic risk which can have the following adverse effects:

- Service disruption
  The service delivery to Securities Services Providers is interrupted
- Loss of securities, cash, or cash entitlements
  Securities Services Providers are subject to losses resulting from conflicts of law, moratoria, and asset seizure / countermeasures to sanctions
- Enforcement penalties
  Securities Services Providers could be subject to penalties, fines and voluntary settlements relating to AML failures and to sanctions violations

- Security failures
  There could be a loss of physical assets, data and IP, and physical threats to senior staff
- Reputational risk
  Damage relating to a Securities Services Provider's reputation could arise from doing business with regimes with poor human rights, environmental and political track records and damage arising from a perceived or actual failure to protect Investors' assets in the event of conflict

16.3 The Geopolitical and Geoeconomic Landscape

The geopolitical and geoeconomic landscape is constantly changing as country alliances shift, political, business and criminal issues arise and conflicts occur. These changes do not just impact individuals or countries, they can also impact financial institutions and the way that they do business. Below are highlighted just some examples of the geopolitical and geoeconomic risks that are current at the time of writing of this report.

16.3.1 US-Chinese relations

A geopolitical risk, that has come to the fore over the last decade, is the relationship between two of the world's largest economies – the US and China. The relationship between these two nations is both an opportunity and a threat to global financial markets. Trading between these two economic power houses, along with the EU, has led to strong economic growth. However, there has also been a notable push for less globalization and a de-coupling of the relationship to alleviate the concern of a reliance on foreign markets where there is a level of uncertainty around ongoing supply models. The recent implementation of tariffs has also shown that geoeconomic risk can cause market disruption. Should these tensions boil over, there could be risk to global trade and interrupted supply chains which could impact financial markets and cause significant risks. Securities Services Providers should be aware of the risks that could arise if these tensions increase and ensure there are robust mitigants in place to counter these.

16.3.2 Russia / Ukraine war

The Russia / Ukraine war has caused significant disruption to people's lives in the geographical region. However, it has also had a significant impact on the financial industry and, specifically, on the Securities Services industry. The introduction of sanctions by regulators required Securities Services Providers to comply with strict sanctions regimes introduced by multiple countries (such as the US, EU and UK). The industry has had to deal with the challenge of complex, and changing, sanctions regulations and ensure that both new and existing business is closely monitored to ensure compliance with the rules.

16.3.3 Tensions in the Middle East

The heightened tensions in the Middle East between Israel and Gaza - and more recently the escalation with Lebanon – is causing instability in the region. Whilst the geopolitical impacts are currently limited to the immediate region, there is the risk of further escalation should other countries become directly involved. This could have wider repercussions with a potential impact on supply chains, health and increased migration of people looking to escape the conflict.

16.3.4 Sustainability

An emerging geopolitical and geoeconomic risk is that of sustainability with an increasing focus by politicians and regulators on climate change, natural resources and energy security. As strategic country alliances change and emerge, the need for robust measures to manage the potential risk of these changes, will become ever more necessary. Securities Services Providers are already having to consider ESG measures when looking at new business. The theme of sustainability, and its impact, on business, is likely to grow as policies and regulations evolve.

CASE STUDY: Geoeconomics and the Covid-19 Pandemic

The cross-border Securities Services industry - and the infrastructure that supports it - was born in the 1970s and grew exponentially with deregulation and globalization from the 1980s. Retrenchment from globalization - by economically significant nation states - therefore challenges the fabric on which the industry is built.

The commitment to deregulation and globalization was undermined by the financial crisis and, more recently, the Covid-19 pandemic. When it hit, in early 2020, the pandemic caused significant disruptions to economies and financial markets. These disruptions – such as supply and distribution problems, productivity concerns as well as a serious health emergency – led to government interventions in many markets with changes to fiscal and monetary policy. The Securities Services industry, as part of the financial system, was also impacted with significant levels of instability and volatility. Securities Services providers were left juggling high trading volumes at the same time that employees were suddenly required to work remotely.

Whilst the markets bounced back relatively quickly, and the financial markets showed their resilience in dealing with the pandemic, the impact of such an unexpected geoeconomic event – and the need for broad, all encompassing, risk management processes – has never been clearer.

16.4 Geopolitical and Geoeconomic Risk Threats

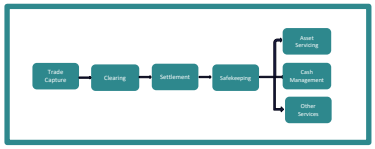
The table below highlights potential geopolitical and geoeconomic risks that could occur as well as how these risks can be mitigated.

Illustration 16.4: Geopolitical and Geoeconomic Risk Table

Risk Description	Risk Mitigation
Policy approach on geopolitical risk lacking	▪ Ensure market risk assessments address political risk broadly and are not restricted narrowly to legal risks
New and emerging geopolitical and geoeconomic risks not identified	▪ Allocate clear management responsibility for monitoring emerging geopolitical and geoeconomic risks ▪ Assess Securities Services networks for political risks on a continuing basis
Assessment and monitoring of existing geopolitical risks failure	▪ Ensure that Securities Services Providers and Clients have adequate access to security and political intelligence ▪ Establish mitigation and contingency plans to address emerging threats, including but not limited to exit plans ▪ Ensure that customer contracts appropriately distribute the risk between the provider and its customer for both direct and indirect losses ▪ Consider prompt communication and information sharing with industry peers, including industry-wide crisis cells to deal with conflicts and other geopolitical events
Required regulatory change, as a result of a geopolitical or geoeconomic risk, not complied with	▪ Ensure that Client contractual arrangements facilitate risk-based compliance with foreign sanctions regimes where a jurisdictional nexus might exit or where secondary sanctions are foreseeable ▪ Allocate clear management responsibility for monitoring potentially relevant sanctions programmes and associated screening (Note: this is especially important when sanctions compliance is outsourced to group functions) ▪ Ensure that compliance functions are appropriately trained in Securities Services products

17. Digital Assets Risk

17.1 Introduction



The risks outlined in the previous chapters of this report have focussed on assets held in a traditional Securities Services model. However, over the last five years the financial industry has seen the creation and growth of digital assets, which may utilize different operating models and technology platforms.

In this chapter, the focus is on digital assets that are held by Clients and utilize a service provider. It does not consider the option of self-custody, nor does it look at digital assets that would not normally be held in a Securities Services environment such as wine tokens or non-fungible tokens (NTFs).

The chapter looks at the key principles that should be considered to mitigate risks when servicing digital assets. It defines the two key types of digital asset – tokenized assets and native digital assets - and distinguishes the key risks of each. It should be recognized, however, that the digital asset marketplace is still evolving and will therefore continue to change and develop. There will therefore be a requirement for both Clients and Securities Services Provider to actively assess these ongoing developments to mitigate risks as they change.

17.2 Definition

A digital asset can, most broadly, be defined as any asset that is created and kept in digital form. From a Securities Services industry perspective, digital assets encompass two key types:

- Tokenized Assets
  Tokenized assets are created to represent traditional securities that are already held in an existing Securities Services environment. A tokenized asset is sometimes referred to as a digital twin as it is a digital representation of an asset that exists, in an immobilized form. As tokenized assets have an underlying real-world equivalent, no new assets are created

- Native Digital Assets
  Native digital assets - sometimes known as native on-chain assets, virtual assets or crypto assets - are purely digital assets that only exist on a digital platform. Native digital assets may be similar to assets that exist in the real world or may be new asset types (such as cryptocurrencies and NTFs)

17.3 The Digital Asset Landscape

Over the last ten years, there has been a slow, but significant, change in the financial landscape. Traditional centralized models for transacting cash and securities, with a strong regulatory oversight and controls, have been joined by the advent of digital assets.

As with anything new, there were initially concerns over the risks involved in investing in digital assets. However, more recently, this has changed as regulators have come to grips with this new world and started to implement new, or

modifications of existing, regulations to support their use. Driven by the introduction of regulations and high returns, digital asset adoption - particularly investment in cryptocurrencies - has been significant and it is anticipated that the digital asset market will continue to grow in the future.

17.4 Servicing Digital Assets

As with traditional assets, a Client wishing to invest in digital assets will require a service provider to hold and safekeep its assets. Whilst it may be a traditional Securities Services Provider that offers this service, there are also new participants- known as VASPS (Virtual Asset Service Providers).

The servicing of digital assets will depend on the type of digital asset as well as the type of operating model and technology platform that is adopted. Below are highlighted the key areas for consideration when looking at servicing digital assets.

17.4.1 Technology Platform

A traditional custody model, as outlined in the chapters above, utilizes a technology model that is a private and centralized technology platform. Tokenized assets can be supported utilizing this traditional custody model.

However, the majority of digital assets utilize different technology platforms which leverage a decentralized database and utilize a distributed ledger – known as Distributed Ledger Technology (DLT). A DLT is a digital system that records, validates and updates transactions immutably whilst enabling simultaneous access to the network across multiple locations. The technology allows for STP and transparency across different organizations in real time.

17.4.2 Operating Model

Whilst tokenized assets may be held by a Securities Services Provider using the traditional operating model outlined in previous chapters, the majority of tokenized assets, and all native digital assets, utilize a different model known as Digital Asset Custody (DAC). As outlined in the Global Digital Finance (GDF), ISSA and Deloitte Report entitled 'Digital Asset Custody Deciphered': "Some activities required for DAC are recognized in traditional Securities Services as roles performed by a Securities Services Provider. However, it is broadly recognized that - in relation to digital assets - new operating models, capabilities and controls may be required to provide these services effectively." Digital Asset Custody Deciphered.

In summary, the operating models for digital assets comprise:

- Rather than holding the asset in a traditional omnibus or segregated account with a Securities Services Provider, the digital assets are held in 'wallets' within the DLT system and the movement of the digital assets from one party to another is dependent on authorization using the private keys for the asset's wallet
- A transaction protocol - known as a smart contract - directly and automatically controls the transfer of digital assets between the buyers and sellers of the assets based on agreed conditions
- Digital assets and smart contracts allow for committed atomic settlement, which enables settlement to be accelerated or delayed from market-agreed time frames. The settlement process for digital assets is therefore flexible and can occur at any point during the day with final settlement.

17.4.3 Information Security

Specific physical and system access, and segregation controls for safeguarding private keys, must be highly secure to ensure the security of information and limit vulnerabilities to threats, such as theft or misuse. Security methods include hot storage (where the private key is held in a location connected to the internet – i.e. less secure from cyber-attacks but advantageous from a timeliness of transaction completion perspective) or cold storage where the private keys are not connected to the internet) therefore more secure although more time consuming to complete transaction processing.

17.4.4 Regulatory and Legal Frameworks

Regulatory and legal frameworks around digital assets are still evolving. Whilst some jurisdictions have created a regulatory framework in many markets this still does not exist. Additionally, regulations have been implemented in multiple ways, with some markets creating digital asset specific regulations and others adapting their current financial frameworks to incorporate these assets. Where new regulations have been implemented, they tend to be unique to the jurisdiction which has oversight which also leads to challenges when a Client wishes to invest in digital assets in multiple markets.

It is therefore critical that both Securities Services Providers look at regulatory considerations such as:

- Determining how legal title and transfer of legal title can be assured for DAC (for example, for traditional securities legal title may be recorded as the Securities Services Provider holding legal title on behalf of its Client whereas, for digital assets the Securities Services Provider may be deemed to hold possession, while title remains directly with the Client)
- Where a digital asset regulatory framework has already been implemented, that the regulations implemented reflect that a Securities Services Provider holding control over private keys is conceptually similar to traditional custody model
- That the jurisdiction's asset safety regulations consider the digital asset to be a financial instrument (and therefore covered by asset safety regulation) or not
- Understanding the confluence of the Client, Securities Services Provider and the "location" of the Digital Asset and the regulatory uncertainty where those differ

With respect to technology platforms, regulators have considered that the regulatory status of an asset or activity is not impacted by the use of alternate technologies, such as DLT, provided that doing so does not change the risk characteristics of the asset or the legal title to the underlying asset.

17.5 Digital Assets Risk Threats

For tokenized assets, the risks are predominantly the same as, or similar to, the risks associated with a traditional Securities Services model. The main difference, and risks, is linked to when a different technology model is utilized. However, for native digital assets, there are key differences around the operating model, the custody of the assets, security as well as confidentiality. This results in different, and / or additional, risks which need to be assessed and mitigated when considering a DAC service.

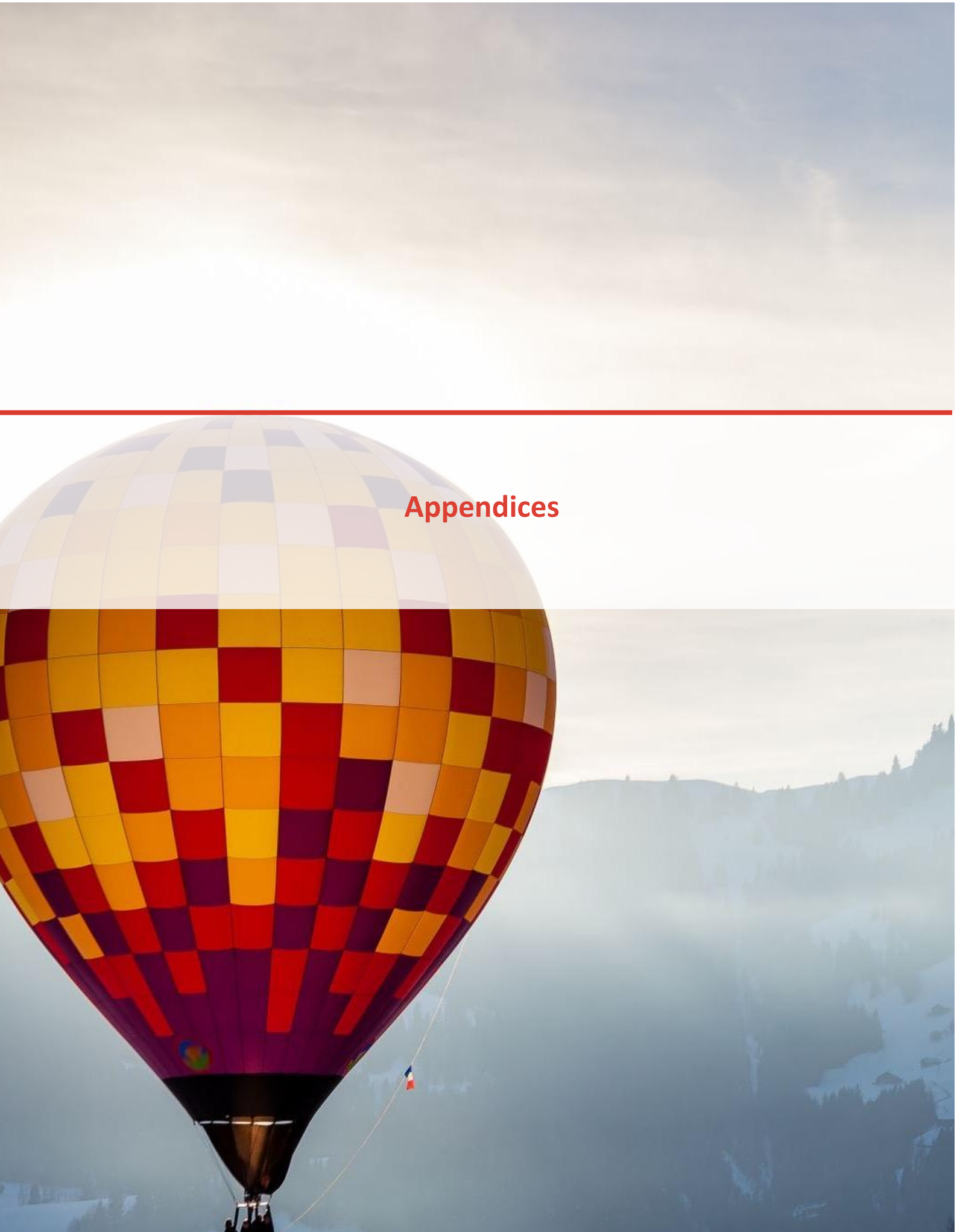
The table below provides a summary of the key digital asset risks that should be reviewed by Securities Services providers and Clients when considering digital assets. These risks should be considered in conjunction with the risks that are outlined in the previous chapters of this report.

Given the relative newness of digital assets, it should be noted that technology, operational and regulatory frameworks are still evolving and therefore the risks will also be likely to change and additional risks may emerge.

Illustration 17.5 Digital Assets Risk Table

Risk Description	Risk Mitigation
▪ Lack of regulatory framework for digital assets	▪ Ensure that any jurisdiction where a Securities Services Provider offers a digital assets service recognizes the construct and has implemented a regulatory framework ▪ Implement active monitoring at the Securities Services Provider of digital asset regulations / laws changes
▪ Lack of asset protection for digital assets	▪ Ensure that jurisdiction's asset safety regulations consider a digital asset to be a financial instrument ▪ Validate that regulations and laws governing asset protection for digital assets are in place in the jurisdiction of service offering ▪ Ensure that Securities Services Provider has control over the private keys and not a third-party
▪ Insufficient or incomplete due diligence of Securities Services Provider	▪ Assess Securities Services Provider to ensure that appropriate licences are held to provide a DAC service
▪ Lack of operational controls or oversight	▪ Confirm that securities transaction mechanisms adopt monitoring controls to check for unusual, suspicious and sanctioned information of digital assets ▪ Implement Know your transaction (KYT) and Know your asset (KYA) monitoring that can provide rapid analysis of the validity of transactions and the asset's history
▪ Insufficient information and / or data security	▪ Implement a DLT solution with specialist security features covering security keys and smart contracts
▪ Lack of a robust DLT solution	▪ Undertake a detailed review of DLT technology to ensure that the platform meets business needs and regulatory requirements ▪ Implement validation of the platform during testing and on an ongoing basis
▪ Third-Party Provider	▪ Ensure that detailed due diligence of third-party providers is undertaken, particularly around applicable regulatory and legal frameworks, systems security and asset protection

ISSA International Securities Services Association



Appendices

Section 4: Appendices

Key High-Level Terms and Definitions

The following table provides a list of the key terms and definitions utilized in this report.

Term	Definition
Asset	Also known as a financial asset or financial instrument, a – usually - non-physical asset that has value as a contractual claim or ownership right
Asset lifecycle	A cycle reflecting the different stages of an asset, from its inception through its purchase, use and maintenance and on to its final disposal
Asset lifecycle participant	Organizations or individuals that provide or utilize any of the components outlined in the lifecycle of an asset
Asset Manager	An organization which acts on behalf of an Investor. It may be an Investment Manager (that focuses primarily on individual investments) or Fund Manager (that works with funds comprised of multiple assets which are often tailored to a particular market sector)
Asset Servicing	The function of servicing a Client's assets typically includes: ▪ Corporate actions (e.g. rights issues, stock splits) ▪ Proxy Voting ▪ Class Actions ▪ Income processing (e.g. dividends, interest /redemptions) ▪ Tax services (e.g. withholding tax relief at source or through reclaim)
Broker Dealer	A party that trades financial transactions on behalf of its Clients (Broker) or on its own behalf (Dealer)
Cash Management	The function of providing cash account facilities to support the movement of securities and asset servicing related monies is known as cash management. These services may include credit facilities to support intraday liquidity and Foreign Exchange (FX) capabilities
Central Bank	The provider of Central Bank money for the settlement in the CSD

Term	Definition
Central Counterparty (CCP)	A party that acts as the central counterparty for all clearing members with the CCP becoming the buyer to every seller and the seller to every buyer
Central Securities Depository (CSD)	A market infrastructure holding securities and enabling securities transactions to be processed by means of electronic book entry. The CSD typically operates a securities settlement system and provides central maintenance of securities accounts and/or notary functions in a specific market
Clearing	This function is an optional step - between trading and settlement - whereby certain transactions are processed together, typically on a clearing venue
Client	An Asset Manager or Investor that appoints a Trade Execution and / or Securities Services Provider is known as the Client of the Securities Services Provider
Custodian	A financial institution which is authorized and supervised by the financial services / bank prudential regulator to provide Securities Services
Depositary / Depotbank	An organization appointed by certain types of EU domiciled fund to oversee the investments made into the fund
Financial Market Infrastructure (FMI)	A provider or operator which clears or settles securities between Securities Services participants
Fund Administrator	An organization responsible for independently verifying the assets in a fund and valuing the fund on behalf of the Client
Fund Services participants	The parties involved in providing services to a fund, which includes a Fund Administrator, Depositary / DepotBank and Transfer Agent
Global Custodian	A Custodian that provides services with respect to securities traded in multiple markets or jurisdictions
Investor	An individual or organization that invests in assets. An Investor may be the actual owner of the assets or be an intermediary holding assets on behalf of other Investors
Issuer	The creator of an asset is known as an Issuer
Registrar	A party responsible for maintaining a registry of the Investors and number of securities held for a fund, bond or equity issuance and to ensure that the quantity of securities in circulation equates to the quantity issued.
Regulator	The organization that governs the operation of the financial market for the jurisdiction for which they are responsible.
Safekeeping	The function of holding of securities owned by a Client is referred to as Safekeeping.

Term	Definition
Securities or Prime Broker	A party that offers services to hedge funds and other professional Clients including securities lending, leveraged trade execution and cash management
Securities Services	A combination of financial services that consists of trade capture, clearing and settlement as well as the safekeeping and administration of assets on behalf of Clients (also sometimes referred to as post-trade services)
Securities Services Provider	An umbrella term for Securities Services participants, such as Custodians, Financial Market Infrastructures (FMIs) and other participants that provide Securities Services to a Client
Settlement	The function of settlement refers to the process of transferring the ownership of securities between counterparts. Settlement is usually against cash which is referred to as Delivery versus Payment (DVP) or Receipt versus Payment (RVP). However, the settlement may also be free of payment
Stock Exchange	A venue where Broker Dealers can buy and sell securities, such as stocks, bonds and other financial instruments
Sub-custodian	A Custodian that provides services with respect to securities traded in a particular market or jurisdiction
Third-Party Provider	A specialist firm that offers external services to Securities Services Providers
Trade Capture	The function of trade, or instruction, capture is the process whereby the Securities Services Provider receives an instruction from its Client (or Trade Execution participant)) to 'settle the trade' on their behalf
Transfer agent	A party appointed by a fund or the Issuer of an asset to issue and cancel fund units and securities in physical or dematerialized form as well as reflect changes in the ownership of an asset

Working Group Participants

ISSA would like to thank the following member organizations for their participation in this project:

- ABN AMRO
- BNP Paribas S.A
- BNY
- Deutsche WertpapierService Bank AG
- Digital Asset Holding, LLC
- Euroclear
- HSBC Holding Plc
- Intesa Sanpaolo Group / Privredna Banka
- JP Morgan Chase & Co.
- Rand Merchant Bank – Custody Services
- SEB Group
- Standard Chartered Bank
- The Depository Trust & Clearing Corporation