THE EVOLVING PRUDENTIAL TREATMENT OF BANKS' CRYPTOASSET EXPOSURES

REPLY AVANTAGE

AGENDA

1 Background and regulatory landscape

2 Evolution of Basel crypto standard

3 Diving into the core of the prudential requirements

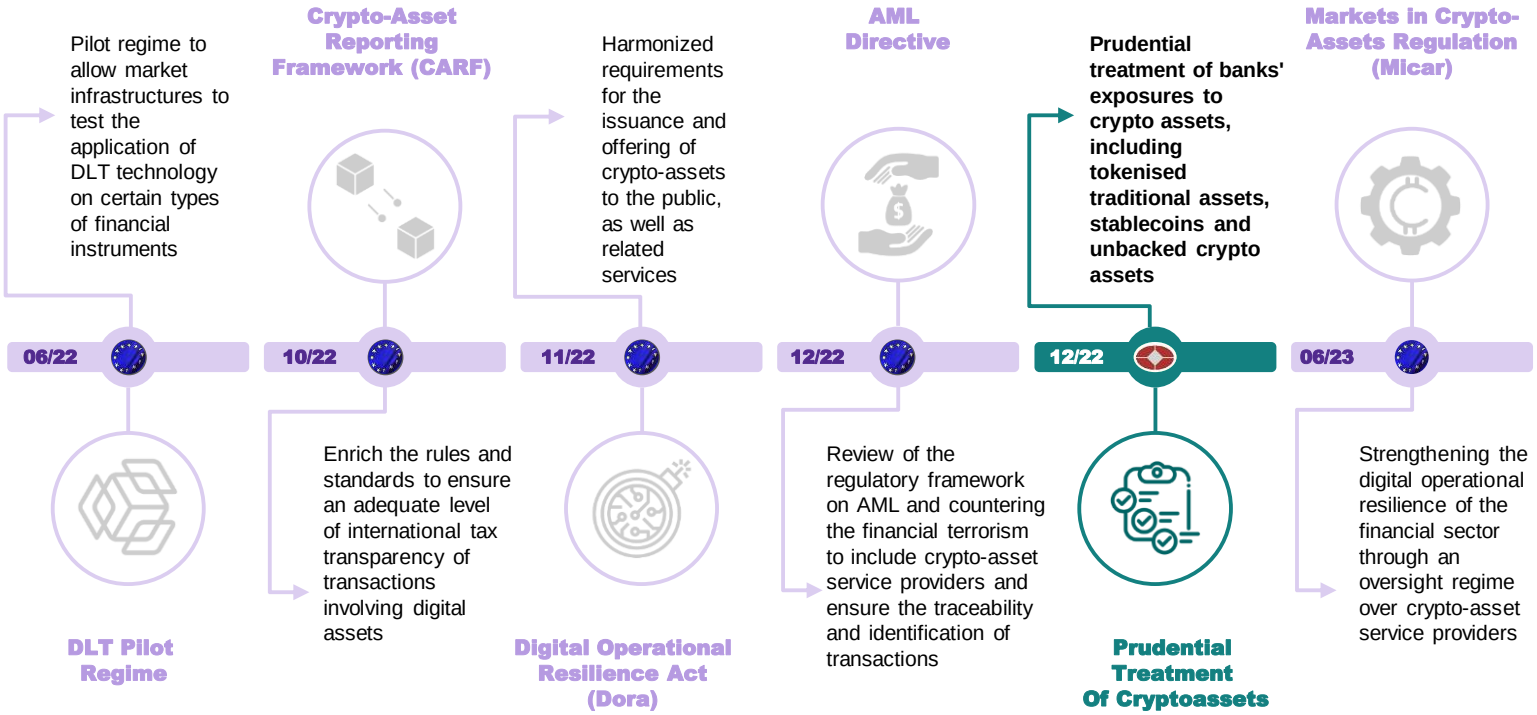
4 Industry impact and challenges

5 Why Avantage Reply

BACKGROUND AND REGULATORY LANDSCAPE

BACKGROUND AND REGULATORY LANDSCAPE

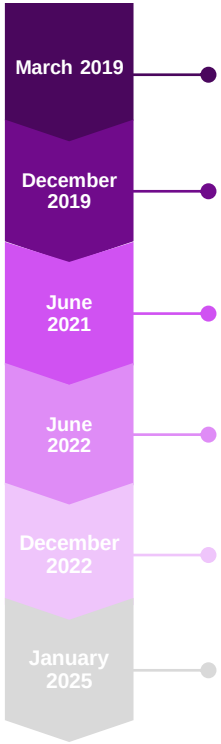
The increasing development of cryptoassets and their high degree of volatility has promoted regulators to define standards to manage this immature, non-standardized asset class that can present concerns for financial stability and increase the risks faced by banks



EVOLUTION OF BASEL CRYPTO STANDARD

EVOLUTION OF BASEL CRYPTO STANDARD

The Basel Committee on Banking Supervision (BCBS) introduced a harmonized standard for the treatment of cryptoasset based on the capital requirements set by the Basel framework:



- **March 2019**: The BCBS published a **newsletter** outlining the minimum supervisory expectations for banks that acquire cryptoassets and/or provide related services
- **December 2019**: The BCBS released a **discussion paper** to gather stakeholders' views on a number of issues relating to the prudential regulatory treatment of cryptoassets
- **June 2021**: The BCBS published a **public consultation** on preliminary proposals for the prudential treatment of banks' cryptoasset exposures
- **June 2022**: The BCBS published a **second public consultation** on the prudential treatment of banks' cryptoasset exposures built on the proposals contained in the first consultation issued in June 2021
- **December 2022**: The BCBS released the **standard** on the prudential treatment of banks' exposures to cryptoasset[1]
- **January 2025**: The **standard** will be **implemented** by January 2025

(1) For more details: Prudential treatment of cryptoasset exposures (bis.org)

DIVING INTO THE CORE OF THE PRUDENTIAL REQUIREMENTS

DIVING INTO THE PRUDENTIAL REQUIREMENTS

SCOPE AND PERIMETER OF THE REGULATION

The **scope** of the Prudential Treatment of Cryptoassets Regulation include three **main aspects**:

1

Management of **critical topics** as consumer protection, money laundering, terrorist financing, and the carbon footprint of cryptoasset

2

Monitoring of cryptoasset's growth since many typologies of digital assets have shown a **high degree of volatility**. Cryptoassets could be a source of risk to financial stability and worsen the risks faced by banking institutions

3

Treatment of cryptoassets that fall into these categories[1]:

- **Tokenised traditional assets** (e.g. security token)
- **Stablecoins**
- **Unbacked cryptoassets** (e.g. cryptocurrencies)

(1) The prudential treatment of central bank digital currencies (CBDCs) is not described within the Basel Framework

DIVING INTO THE PRUDENTIAL REQUIREMENTS

THE «PRINCIPLES» OF PRUDENTIAL TREATMENT OF CRYPTOASSETS

SAME RISK, SAME ACTIVITY, SAME TREATMENT

The cryptoasset that provides the same functions and has the **same risks of a "traditional asset**", should be subject to the **same capital, liquidity and other requirements as a traditional asset**

SIMPLICITY

The prudential treatment of cryptoassets should be **easy and cautious**, as the cryptoasset market, technologies and related services are still evolving

MINIMUM STANDARDS

Any prudential treatments of cryptoassets indicated by the Committee constitutes a **minimum standard for banks**. Banks may apply additional and/or more conservative measures, where justified

DIVING INTO THE PRUDENTIAL REQUIREMENTS

GROUPS CLASSIFICATION AND KEY ELEMENTS

The prudential treatment of a bank's cryptoasset exposure depends on whether, based on its characteristics, they will be included in **Group 1** or **Group 2 cryptoasset**

GROUP 1

Cryptoassets that satisfy all **four classification criteria** will be classified as **Group 1**

Based on the asset type, a distinction can be made between:

- **Group 1a**: Tokenised traditional assets[1]
- **Group 1b**: Cryptoassets (Stablecoins) with stabilisation mechanisms

GROUP 2

The **Tokenised traditional assets** and **stablecoins** that **don't meet** the **classification conditions** and the **unbacked cryptoasset** will be included in **Group 2**

A distinction can be made between:

- **Group 2a**: Cryptoassets[2] that pass the Group 2a hedging recognition criteria
- **Group 2b**: All other cryptoassets[2] that fail the Group 2a hedging recognition criteria

(1) Traditional assets are those assets that are captured within the Basel Framework that are not classified under this chapter as cryptoassets
(2) Tokenised traditional assets, stablecoins and unbacked cryptoassets

DIVING INTO THE PRUDENTIAL REQUIREMENTS

CLASSIFICATION CONDITIONS FOR GROUP 1 CRYPTO ASSETS

FIRST CONDITION

TOKENISED TRADITIONAL ASSETS will only meet classification condition 1 if they satisfy all of the following requirements:

- They **are digital representations of traditional assets** using cryptography, DLT or similar technology to record ownership
- They pose the **same level of credit and market risk** as the traditional asset

CRYPTOASSETS THAT HAVE A STABILISATION MECHANISM will only meet classification condition 1 if they satisfy all of the following requirements:

- **The cryptoasset is designed to be redeemable for a predefined amount of a reference asset or assets or cash equal to the current market value of the reference asset**(s). The value of the reference asset(s) is referred to as the "peg value"
- The **stabilisation mechanism is designed to minimise fluctuations in the market value of the cryptoassets** relative to the peg value. Banks must have a monitoring framework to verify that the stabilisation mechanism is functioning
- The **stabilisation mechanism enables risk management similar to the risk management of traditional assets**, based on sufficient data or experience
- There exists **sufficient information that banks use to verify the ownership rights of the reserve assets** upon which the stable value of the cryptoasset is dependent. Banks may use the assessments of independent third parties for the purposes of verification of ownership rights only if they are satisfied that the assessments are reliable
- **The cryptoasset passes the redemption risk test and the issuer is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements**. Cryptoassets with stabilisation mechanisms have to meet a "basis risk test", but as yet has chosen not to implement this test

DIVING INTO THE PRUDENTIAL REQUIREMENTS

CLASSIFICATION CONDITIONS FOR GROUP 1 CRYPTO ASSETS

SECOND CONDITION

All **rights, obligations** and **interests** arising from the cryptoasset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed. In addition, the applicable legal framework(s) ensure(s) settlement finality. Banks are required to conduct a legal review of the cryptoasset arrangement to ensure this condition is met, and make the review available to their supervisors upon request

To meet classification condition 2, at all times the cryptoasset arrangements must ensure:

- **Full transferability** and **settlement finality**. In addition, cryptoassets with stabilisation mechanisms must provide **a robust legal claim** against the issuer and/or underlying reserve assets and must ensure **full redeemability at all times and at their peg value**. In order for a cryptoasset arrangement to be considered as having full redeemability, it must allow for **the redemption to be completed within 5 calendar days of the redemption request at all times**
- **Adequacy of documentation**. For cryptoassets with stabilisation mechanisms, cryptoasset arrangements must clearly define **which parties have the right to redeem**; the **obligation of the redeemer** to fulfil the arrangement; the **timeframe for this redemption** to take place; the **traditional assets in the exchange**; and how the **redemption value** is determined. **These arrangements must also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the cryptoasset is issued and redeemed**. **This information must be made public by the issuer of the cryptoasset**. The public offering of the cryptoasset must be approved by the **relevant regulator** on the basis of this **public disclosure**. Otherwise, an **independent legal opinion would be needed**

DIVING INTO THE PRUDENTIAL REQUIREMENTS

CLASSIFICATION CONDITIONS FOR GROUP 1 CRYPTO ASSETS

THIRD CONDITION

The functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are **designed and operated to sufficiently mitigate and manage any material risks**

To meet classification condition 3, the following requirements must be met:

- The functions of the cryptoasset, and the network on which it runs, do not pose any material risks that could impair the transferability, settlement finality or, where applicable, redeemability of the cryptoasset. To this end, entities performing activities associated with these functions must follow **robust risk governance and risk control policies and practices to address risks including**
- **All key elements of the network must be well-defined such that all transactions and participants are traceable**. Key elements include: the operational structure; degree of access; technical roles of the nodes and the validation and consensus mechanism of the network

FOURTH CONDITION

Entities that execute redemptions, transfers, storage or settlement finality of the cryptoasset, or manage or invest reserve assets, must: (i) be **regulated and supervised**, or subject to appropriate risk management standards; and (ii) **have in place and disclose a comprehensive governance framework**

Entities subject to condition 4 include **operators of the transfer and settlement systems for the cryptoasset, wallet providers and, for cryptoassets with stabilisation mechanisms, administrators of the stabilisation mechanism and custodians of the reserve assets**. Node validators may be subject to appropriate risk management standards as an alternative to being regulated and supervised

DIVING INTO THE PRUDENTIAL REQUIREMENTS

RECOGNITION CRITERIA FOR CLASSIFICATION OF CRYPTO ASSETS IN GROUP 2a

1° HEDGING RECOGNITION CRITERIA

The bank's **cryptoasset exposure** is one of the following:

- A direct holding of a spot Group 2 cryptoasset where there exists a derivative or exchange-traded fund (ETF)/exchange-traded note (ETN) that is traded on a regulated exchange that solely references the cryptoasset
- A derivative or ETF/ETN that references a Group 2 cryptoasset, where the derivative or ETF/ETN has been explicitly approved by a jurisdiction's markets regulators for trading or the derivative is cleared by a qualifying central counterparty (QCCP)
- A derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion above
- A derivative or ETF/ETN that references a cryptoasset related reference rate published by a regulated exchange

2° HEDGING RECOGNITION CRITERIA

The bank's cryptoasset exposure, or the cryptoasset referenced by the derivative or ETF/ETN, is highly liquid. Specifically , both of the following must apply:

- The **average market capitalisation was at least USD10 billion over the previous year**
- The **10% trimmed mean of daily trading volume** with major fiat currencies **is at least USD50 million over the previous year**

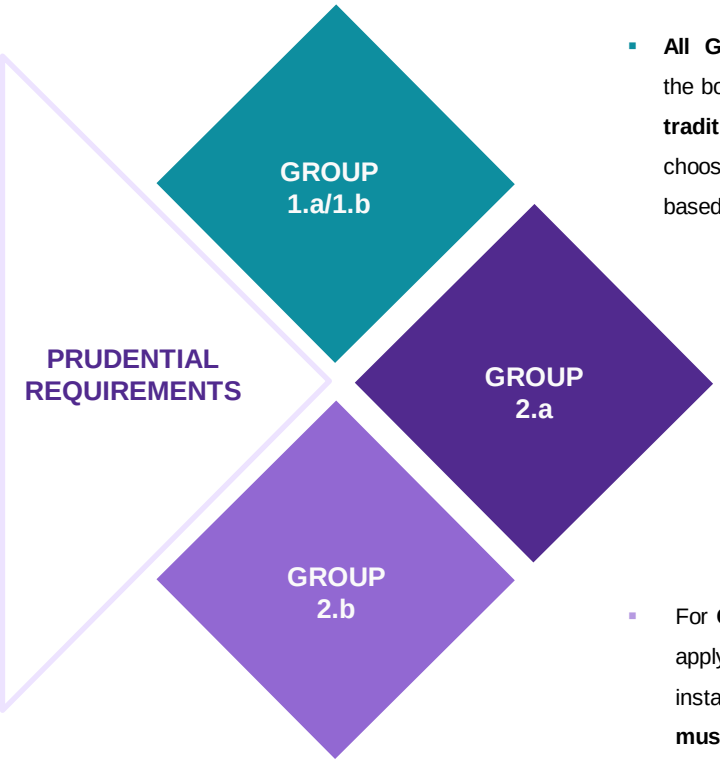
3° HEDGING RECOGNITION CRITERIA

Sufficient data is available over the previous year. Specifically, both of the following must apply:

- There are at least **100 price observations over the previous year**. The price observations must be "real"
- There are **sufficient data on trading volumes and market capitalization**

DIVING INTO THE PRUDENTIAL REQUIREMENTS

PRUDENTIAL REQUIREMENTS



- **All Group 1 cryptoassets** must be assigned to the **banking book or trading book** based on the application of the boundary criteria. **All risks** resulting from **cryptoasset activities** are **generally** treated in the **same way** as **traditional assets** in the current Basel Framework. In addition, to manage Group 1 cryptoassets, authorities can choose an **infrastructure risk add-on**. The add-on will initially be set at zero and increased by the authorities based on any **weaknesses** observed in the infrastructure used

- **Group 2.a cryptoassets** must be treated according to the proposed market risk rules, **independent** of whether they stem from trading or banking book instruments. **Capital requirements** for Group 2.a cryptoassets are generally calculated with a **modified version** of the models currently used in the Basel Framework. However, for some risks, **models-based approaches must not be applied**

- For **Group 2.b cryptoassets** there is **no separate trading book and banking book treatment**. Banks must apply a **risk weight of 1250%** or adopt a **narrower approach** compared to the current Basel Framework for instance by using a **modified version of the model.** However, for some risks, **models-based approaches must not be applied**

DIVING INTO THE PRUDENTIAL REQUIREMENTS

PRUDENTIAL REQUIREMENTS

RISK TYPOLOGY	GROUP 1	GROUP 2
1 CREDIT RISK	**Group 1a**: The tokenised traditional assets held in the banking book will generally be subject to the same rules to determine credit RWA as non-tokenised traditional assets. However, banks must evaluate some characteristics of the cryptoassets of the Group 1a as the liquidity of the tokenized asset compared to the non-tokenized one or if the market liquidity characteristics and market values of tokenized assets meet the requirements for credit risk mitigation under the standards of the credit risk **Group 1b**: Banks that have banking book exposures to Group 1b must analyse their specific structures of the crytoassets and identify all risks that could result in a loss. Each capitalized credit risk must be separately assessed by banks using credit risk standards (the list is non-exhaustive and can include risks of default from the redeemer or from the reference asset)	**Group 2.a**:The capital requirements may be calculated according to a modified version of the Simplified Standardised Approach (SSA) or a modified version of the Standardised Approach (SA). The Internal Models Approach is not applicable to Group 2a cryptoassets. The modified versions will include a separate risk class with its capital requirements based on the specifications set in the standards **Group 2.b**: For each separate Group 2b cryptoasset to which they are exposed, banks must apply a risk weight of 1250% to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoasset
2 MARKET RISK	The minimum capital requirements applied to **Group 1a** and **Group 1b** cryptoasset exposures are regulated by: ▪ Standardised Approach ▪ Semplified Standardisied Approach ▪ Internal Models Approach However, it will be necessary to take into consideration a series of specifications for the application of each model as reported in the regulation	
3 CREDIT VALUATION ADJUSTMENT RISK	Derivatives and Securities financing transactions SFTs on **Group 1a** and Derivatives on **Group 1b** will generally be subject to the same rules to determine CVA RWA as non-tokenised traditional assets	**Group 2a**: Cryptoassets will be only subject to the rules set out in Basel Framework. The use of SA-CVA is not permitted for derivatives and SFTs referencing Group 2a cryptoassets **Group 2b**: For each separate Group 2b cryptoasset to which they are exposed, banks must apply a risk weight of 1250% to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoasset

DIVING INTO THE PRUDENTIAL REQUIREMENTS

PRUDENTIAL REQUIREMENTS

	RISK TYPOLOGY	GROUP 1	GROUP 2
4	COUNTERPARTY CREDIT RISK	**Group 1a**: Derivatives on Group 1a cryptoassets will generally be subject to the same rules to determine CCR as non-tokenised traditional assets, which includes the application of the Internal Models Method **Group 1b**: Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CCR RWA as non-tokenised traditional assets	**Group 2a**: Derivatives on Group 2a cryptoassets will be subject to the SA-CCR, but with specific changes in relation to the calculation of the potential future exposure (PFE) for which a new "crypto" asset class will be created. **Group 2b**: In the Group 2b, the changes concern both the replacement cost (RC), for which netting is allowed only between exposures in cryptoassets of Group 2b, and the PFE for which 50% of the notional amount per transaction
5	OPERATIONAL RISK	The operational risk resulting from cryptoasset activities should generally be captured by the operational risk standardised approach through the Business Indicator, which should include income and expenses resulting from activities relating to cryptoassets, and through the Internal Loss Multiplier, which should include the operational losses resulting from cryptoasset activities. In case these approaches don't capture operational risk, banks should take further steps to ensure capital adequacy	
6	LIQUIDITY RISK	For the liquidity coverage ratio and net stable funding ratio requirements, the cryptoasset exposures must generally follow a treatment that is consistent with existing approaches for traditional exposures with economically equivalent risks. The treatment must also appropriately reflect the additional risks that these assets hold in comparison to traditional assets, and the relative lack of historical data. The document specifies which cryptoassets can qualify as QHLAs (es. Group 1a)	
7	LEVERAGE RATIO	Cryptoassets are included in the leverage ratio exposure measure according to their value for financial reporting purposes, based on applicable accounting treatment for exposures that have similar characteristics. In case the cryptoasset exposure is an off-balance sheet item, the credit conversion factor set out in the leverage ratio framework will apply in calculating the exposure measure	
8	LARGE EXPOSURE	Cryptoasset exposures that give rise to a credit risk exposure are included in the large exposure measure according to their accounting value. The bank must identify and apply the large exposure limits to each specific counterparty or group of connected counterparties to which it is exposed under the risk-based capital framework. If the cryptoasset exposes the bank to the risk of default of more than one counterparty or to the default risk of the reference asset, these risks should be considered for the purpose of the large exposures framework. Cryptoassets that do not expose banks to default risk do not give rise to a large exposures requirement	

DIVING INTO THE PRUDENTIAL REQUIREMENTS

ADDITIONAL KEY ELEMENTS

KEY ELEMENTS	GROUP 1	GROUP 2
Add-on for infrastructure risk	The authorities must have the **power to apply an add-on to the capital requirement for exposures to Group 1 cryptoassets**. The add-on for infrastructure risk will initially be set as zero but will be increased by authorities based on any observed weakness in the infrastructure used by Group 1 cryptoassets	**Not Applicable**
Group 2 exposure limit	**Not Applicable**	**A bank's total exposure to Group 2 cryptoassets must not exceed 2% of the bank's Tier 1 capital** and should generally be lower than 1%. Banks breaching the 1% limit will apply the more conservative Group 2b capital treatment to the amount by which the limit was exceeded. Breaching the 2% limit will result in the whole Group 2 exposures being subject to the Group 2b capital treatment.
Deduction requirement	**Cryptoasset exposures are not subject to the deduction requirement that applies to intangible assets** set out in [CAP30.7] and [CAP30.8][1], even in cases where the cryptoasset is classified as an intangible under the applicable accounting standard	

(1) For more details: CAP30 - Regulatory adjustments (bis.org)

DIVING INTO THE PRUDENTIAL REQUIREMENTS

DISCLOSURE & SUPERVISORY

1 DISCLOSURE

Banks must provide **qualitative information** that sets out an **overview of the bank's activities** related to cryptoassets and **main risks** related to their cryptoasset exposures, including descriptions of:

- ***Business activities*** *related to cryptoassets, and how these business activities translate into components of the risk profile of the bank*
- ***Risk management policies*** *of the bank related to cryptoasset exposures*
- ***Scope and main content of the bank's reporting*** *related to cryptoassets*
- ***Most significant current and emerging risks*** *relating to cryptoassets and how those risks are managed*

Banks must **disclose information** regarding any cryptoasset exposures on a **regular basis**, including for each specific type of cryptoasset exposure information on:

- *The direct and indirect exposure amounts*
- *The capital requirements*
- *The accounting classification*

2 SUPERVISORY

National Competent Authorities (NCAs) evaluate how efficiently banks assess their **capital needs**. Supervisors should:

- ***Review the appropriateness of banks' policies and procedures*** *for identifying and assessing those risks*
- ***Exercise their authority*** *to require banks to address any deficiencies in their identification or assessment process*
- ***Recommend that banks undertake stress testing or scenario analysis*** *to assess risks*

The types of response that supervisors may consider include the following:

- ***Additional capital charges*** *for risks not sufficiently captured under the minimum capital requirements for operational risk, credit risk, or market risk*
- ***Provisioning*** *of losses related to cryptoassets where such losses are foreseeable and estimable*
- ***Supervisory limit or other mitigation measures****, such as requiring a bank to establish an internal limit to contain the risks not adequately identified or assessed in the bank's risk management framework*

INDUSTRY IMPACT AND CHALLENGES

INDUSTRY IMPACT AND CHALLENGES

All banks that decide to have **exposures in crypto assets** and **related services** will have an **impact on their functions** (e.g. Front Office, Back Office, Risk & Compliance) and will face **some important challenges**

1 DUE DILIGENCE

The bank should **consolidate** its **quantitative skills** to conduct analysis and **adequately assess** the risks arising from exposure to crypto assets or related services

2 GOVERNANCE & RISK MGMT

The bank should have a **clear** and **robust risk management framework.** The risk assessment process should be incorporated into the bank's **internal capital** and **liquidity adequacy assessment processes**

3 DISCLOSURE

The bank should **periodically disclose information** regarding the accounting treatment of crypto exposures, in accordance with national standards and requirements

4 SUPERVISORY DIALOGUE

Banks should promptly **inform supervisors** about crypto-asset activity and related services, evidence of the risk assessment process and the risk mitigation strategies

HOW TO GET STARTED

At Avantage Reply, the **experience gained** in both the **technology and financial sectors** and the **continuous learning** of the **Digital Asset phenomenon** are **key assets.** Our goal is to **support our clients** in identifying the **fundamental** and **critical actions** that **financial institutions** should take in this **disruptive phase of the market**, while remaining compliant with the new regulatory proposals of the Basel Committee

DUE DILIGENCE

Conduct **comprehensive analysis** using **quantitative** and technical skills in order to develop **new quantitative models** and ensure **efficient management of the risks** arising from exposure to cryptoasset

100%
Very High

GOVERNANCE & RISK MGMT

Change the **cultural mindset** and integrate the **new requirements** (Capital Requirements, Anti-Money Laundering, IT Resilience) set by regulators in the Digital Assets field into the organizations' framework and **redefine risk tolerance** in order to consider the new risks related to the crypto area

100%
Very High

DISCLOSURE

Define **adequate information flows** that included aspects, such as:

- Information on the **typology** of digital assets and related **services**
- **Accounting** for cryptoassets
- **Compliance** with regulatory requirements

75%
High

SUPERVISORY DIALOGUE

Open a **dialogue with regulators** by periodically disclosing **clear information** in line with the risk management strategies. In this way, authorities have the possibility to protect consumers and investors

75%
High

EFFORT NEEDED 25%

WHY AVANTAGE REPLY

TAKE ON THE NEW CHALLENGES OF DIGITAL ASSETS WITH AVANTAGE REPLY

HOW WE CAN HELP?

The introduction of **digital assets** within the financial institutions is not an easy climb, but with our help we can ensure that the summit will be reached in compliance with the new regulations and in line with the innovative context

Avantage Reply is the best guide you can get. We guide our clients towards an evolution of the risk framework starting from changing mind-set to ensure **new revenues opportunities** in the digital markets and the **creation of business value**

ADVISORY

Advisory on the regulatory landscape, business processes and IT technologies

PLAN&DESIGN

Planning of the project roadmap and design of new business processes and frameworks

IMPLEMENTATION

Governance and monitoring of the implementation and testing phases

CONTACTS

Danilo Mercuri
Partner, Avantage Reply
Via Castellanza, 11
20151 - Milano - ITALY

Phone: +39 02 535761
Mobile: +39 348 3064828
E-mail: d.mercuri@reply.it

Angelo Santarossa
Senior Manager, Avantage Reply
Via Castellanza, 11
20151 - Milano - ITALY

Phone: +39 02 535761
Mobile: +39 340 4603950
E-mail: a.santarossa@reply.it

Letizia Bucci
Lead, Avantage Reply
Via Castellanza, 11
20151 - Milano - ITALY

Phone: +39 02 535761
Mobile: +39 345 8602260
E-mail: l.bucci@reply.it

Michela Martella
Senior Consultant, Avantage Reply
Via Castellanza, 11
20151 - Milano - ITALY

Phone: +39 02 535761
Mobile: +39 342 7535893
E-mail: m.martella@reply.it