Digital Assets Risk Management Policy ("DA Policy")

Version No	2.1
Document Type	Policy
Parent Document	Enterprise Risk Management Framework
Parent Framework	Enterprise Risk Management Framework
Document Approver Name	Jason Pierpoint Forrester
Document Approver Job Title	Co-Head-CRO CIB,Global Head-ERM,Dep CRO,SC Bank
Document Owner Name	Gwenda Marian Phillips; Amitav Borkakoty
Document Owner Job Title	CRO SCV & GH Cryptoasset Risk Mgt; Global Head, Risk Governance and Enterprise Risks
Document Contact Name	Maria Zameer
Document Contact Job Title	Executive Director, Digital Assets Risk
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	GLOBAL
Approval Date	14/03/2023
Effective Date	01/09/2023
Next Review Date	01/09/2025

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Maria Zameer	Migration to Inline format- Non Material Change(No change to document content)	Non-Material	Jason Pierpoint Forrester	2.1	14/03/2023	01/09/2023

The full version history is included at the end of the document.

1. PURPOSE AND SCOPE

This policy sets out the minimum requirements for the management of risks including identification, assessment and monitoring of associated with Digital Assets ("DA") activities, services and exposures (collectively referred to as "Activities" for the course of this document) arising from the Group's Businesses[1] across our Clients[2], Products and Projects.

The policy is mapped to the Enterprise Risk Management Framework ("ERMF") and applies to all businesses and operations of the Group. Risks associated with DA activities arise across multiple Principal Risk Types ("PRTs"). Existing Principal Risk Type Frameworks ("RTFs"), and their associated policies and standards must continue to be adhered to in addition to stipulations contained in this policy.

For the purposes of the scope of this document, DA is the Group's preferred term to collectively refer to "digital assets", "cryptoassets", "virtual assets" or "tokens". These terms are used interchangeably in the context of Group's Businesses and their associated operations.

There is currently no universal definition of a "cryptoasset" ("CA") or related terms such as a "digital asset" or "virtual asset". However, there is increasing consensus on the basic elements of the definition in the United Kingdom ("UK") and other jurisdictions, and in global standards.

The definition adopted for the purposes of this policy is taken from the UK Financial Services and Markets Bill[3], where DA means any cryptographically secured digital representation of value or contractual rights that:

(a) can be transferred, stored or traded electronically, and

(b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)."

DA activities include DA exchange providers (including DA Automated Teller Machine, peer-to-peer providers, issuing new DAs, etc), custodians, and business models such as DeFi ("Decentralised Finance"). Other use cases of Digital Ledger Technology ("DLT"), for instance Central Bank Digital Currencies and the use of DLT for operational effectiveness, will be evaluated on a case-by-case basis if they include the risks of DA.

Digital Assets Risk Statement

DA Risk is defined as the "potential for regulatory penalties, financial loss and/or reputational damage to the Group resulting from DA related activities from the Group's Businesses across Clients, Products and Projects.

Digital Assets Risk Management Approach ("DARMA")

The DARMA is the denoted term used to refer to a formal and robust governance structure for the risk management of DA. This includes but is not limited to DA specific risk appetite metrics; the DA Policy; DA Risk Committee ("DRC"); Financial Crime Compliance Cryptoassets Interim Control Framework ("CAICF"), and evaluation tools and guidelines. It enables the Group to apply a consistent approach for the management of DA related risks including, but not limited to identification, assessment and monitoring, to meet regulatory expectations relating to the appropriateness of risk assessments and oversight of DA related activities.

The Approach applies across the Group's Businesses and is governed through the DRC. As DA-related risks are cross-cutting in nature and may materialize through the PRTs, existing PRTs policies, standards and risk assessments must continue to be adhered to in addition to requirements under the DARMA.

---

[1] Businesses refers to Corporate, Commercial and Institutional Banking ("CCIB"), Consumer, Private and Business Banking ("CPBB") and Standard Chartered Ventures ("SC Ventures" or "SCV").

[2] Examples of Client review assessment are:
- a) Portfolio level credit exposure to clients whose principal business is DA. For Ventures, the Venture Governance Model would apply for escalations or consultation with DRC.
- b) Portfolio level retrospective review of onboarded clients classified as DA exposed by the Client Business.
- c) Specific Client risk events escalated to DRC from client oversight committees.
- d) Notification of updates in relation to client Customer Due Diligence ("CDD") or portfolio risk metrics from the Businesses.

[3] Financial Services and Markets Bill, Section 65, https://bills.parliament.uk/bills/3326.

Out of Scope Activities for the Policy

The Group has clarified with the Prudential Regulatory Authority ("PRA") and Financial Conduct Authority ("FCA") that these activities are outside the scope of the policy requirement.

- Distributed Ledger Technology ("DLT") solutions where DLT solutions are applied purely for operational efficiency, including where there may be a transfer of rights
- Operating expense accounts for DA entities: Operating expense accounts to manage activities such as rent, and employee wages where existing Client Due Diligence requirements will apply.

2. MANDATORY POLICY STATEMENTS

Approach to Managing risks associated with DA exposure or activities

2.1. Risk Management

The Group applies a three Lines of Defence ("LOD") model to the day-to-day management of risks associated with DA activities, services or exposures. As a practical approach to address the cross-cutting risks arising from DA, enhanced due diligence (as evaluated against the DA Higher Risk Activities Framework) is to be conducted for Clients, Products or Projects based on applicable PRTs prior to inducting or onboarding any DA activities. Existing governance and approval authority structures will continue to apply as per normal course of business.

The risk management practices and principles outlined in this policy are guided by various regulatory initiatives and guidance. This includes but is not limited to:

- "Dear CEO" letter[4] from the Prudential Regulatory Authority ("PRA") 28 June 2018 and further notice on 24 March 2022[5]
- "Dear CEO" letter[6] Financial Conduct Authority ("FCA") 11 June 2018 and further notice on 24 March 2022[7]
- Basel Committee on Banking Supervision publication on the prudential treatment of cryptoassets issued on 16 Dec 2022[8]

2.2. Senior Managers Regime

a. **Risk Management Framework.** The Group Chief Risk Officer ("GCRO") is responsible for second line oversight responsibilities for the Risk Management Framework for DA as stated in the Statement of Responsibilities. These responsibilities are discharged through the PRT Risk Framework Owners ("RFOs") and DA Subject Matter Experts ("SMEs") and through the Global Head, ERM and CRO, SC Bank for DA.

b. **Risk assessment attestations**. The Senior Management Function ("SMF") of the relevant Businesses are responsible for reviewing and signing off on the overall risk assessment for any planned Higher Risk DA Activities. This approach is in line with consultations with the PRA and FCA.

[4] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2018/existing-or-planned-exposure-to-crypto-assets.pdf

[5] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2022/march/existing-or-planned-exposure-to-cryptoassets.pdf

[6] https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-Digital Assets-financial-crime.pdf

[7] https://www.fca.org.uk/news/statements/notice-regulated-firms-exposure-cryptoassets

[8] https://www.bis.org/bcbs/publ/d545.htm

2.3. Higher Risk DA Activities

The Group has identified and assessed specific DA related activities as Higher Risk ("HR"). These activities are derived from regulatory consultations, industry papers and advice from PRT RFOs and DA SMEs and have been shared with the PRA and FCA.

The demarcation between entities that are directly involved in DA related activities and those that support them can be unclear and change over time. Some may present higher or lower risk and therefore the risk assessment may differ in scope and depth according to the level of risk presented. The list of activities is non-exhaustive at present due to the rapidly evolving nature of the DA industry. The DA HR Framework is refreshed annually. Out of cycle and relevant updates can be made to the DA HR Framework on request by the DRC.

Governance Framework and Regulatory Obligations

2.4. Governance Framework

a. **DRC**. Digital Assets Risk Committee ("DRC") is established under the Group Risk Committee ("GRC") to oversee the implementation of risk management for DA under the Group ERMF within the Businesses. The DRC oversees and is to be consulted on the assessment of DA related risks and provides decision (from a DA risk perspective) to support, not support or support with conditions the risk assessment. The risk assessment will provide coverage on:

   i. Clients and third parties in relation to the DA services that they will be providing to any of the Businesses. Clients are counterparties who may also be service providers and include brokerages, custodians, and exchanges

   ii. Products; and

   iii. Projects.

b. **Existing Governance Structure**. Existing approval governance structures continue to be required for the holistic review of the risks arising from Clients, Products and Projects. The recommendations from the DRC oversight and consultations must be taken into consideration by the governance fora for Clients, Products and Projects with regards to DA-related risks prior to approval from the BAU Committees.

c. **Updates to Senior Management**. As per normal course of business, the Business Leads or First Line of Defence ("1LOD") must keep the Board and Senior Management informed of the DA activities in the Group through periodic updates to the Group Risk Committee, DRC and any other request-based Forum/ Committee. Similarly, overall updates on the DA strategy will be provided by the DA Centre of Excellence ("DA COE"). The DA COE, as a central point of contact, must work with the respective Business Leads for reporting on DA related exposures across the Group.

d. **Updates to Group Governance Committees on DA risk management**. Enterprisewide, strategic updates related to DARMA will be provided by the DA Risk Team or DA SMEs, in consultation with the relevant PRT RFOs and SMEs. Conversely, PRTspecific updates (whether internal or external) on DA to respective approval or governance committees[9] will be provided by PRT RFOs and SMEs in consultation with the DA Risk team and DA SMEs. In both cases, prior consultation with the respective parties is recommended.

[9] BAU approval committees include but are not limited to Business Risk Committees including Group Risk Committee, CCIB Risk Committee and CPBB Risk Committee. Governance Committees include, but not limited to the Non-Financial Risk Committees, Regional Risk Committee, or PRT specific Committees

2.5. Regulatory Obligations

a. **Identification of relevant regulatory trends**: For DA thematic regulations, Compliance will identify new and amended regulations as and when issued by the relevant financial authorities. In addition, DA COE must collaborate with Group Public and Regulatory Affairs ("GPRA") to assess major DA regulatory and policy trends that impact the Group to form a strategic view about new and developing risks in the regulatory and policy environment.

b. **Implementation**:

   i. The Business Leads or 1LOD in conjunction with DA COE are responsible for the overall implementation of the DA related policies and standards (as the standards become available) under oversight and review of the Global Head, DA Risk Management, RFOs and DA SMEs.

   ii. The respective PRT RFOs are responsible for overseeing and reviewing the implementation of DA related policies specific to their PRTs in consultation with the Global Head, DA Risk Management and DA Risk team.

c. **Notification to Regulators**: Regulatory engagement is managed through Group Public and Regulatory Affairs ("GPRA") or Group Regulatory Liaison ("GRL") teams as per standard practice within the Group. Business SMF jointly with the DA COE and other relevant stakeholders, in collaboration and on advice from GRL, are responsible for giving advance notifications as applicable or where requested (Refer to Section 2.2 for related information).

d. **Regulatory Engagement**: The DA COE, working jointly with GPRA and Country Heads of Compliance, Financial Crime and Conduct ("CFCC") for host regulators, is responsible for designing and executing a regulatory engagement strategy on DA topics and updates to the DRC. Business Leads and the DA COE are responsible for business inputs and representation at regulatory engagements on DA topics and updates to the DRC. DA COE must collaborate with GRL, which is responsible for coordinating all engagements with the PRA/FCA, with Country Heads of CFCC for engagements with host regulators. From time to time, the DRC is to be apprised by the Business Leads or DA COE with the summary and outcomes of such engagements.

e. **Risk Assessments**. Risk assessments must include the inherent and residual risk, and the relevant Group and DA specific risk appetite metrics and monitors across the applicable PRTs. DRC must review the risk assessment prior to submission to the relevant regulatory authority and may request the Business Heads ("BH")/ Relationship Manager ("RM")/ Accountable Executive ("AE") for additional supporting information during the oversight, review and consultation process undertaken with the PRT RFOs or DA SMEs for the respective PRTs. Risk assessments will follow the appropriate standards, guidelines and procedures issued under existing governance as well as any additional DA specific governance.

f. **Inventory**. DA COE must maintain an inventory of Clients, Products (including specific DA approved for on-boarding) and Projects identified for the purpose of informing the DRC, the PRA and other regulators as applicable. For avoidance of doubt, theinventory must include DA initiatives that have been internally approved, initiatives not classified as Higher Risk DA Activities as well as new initiatives that are in the pipeline and not yet approved. Specific client inventory will be jointly reported by Client Coverage.

2.6. Risk Appetite

a. **Responsibility**: DRC is responsible for review, recommendation and oversight of the Group's DA risk appetite (in consultation with DA SMEs and Group Risk Appetite) and indicators for risks associated with DA. The recommendation will then follow the Group's Risk Appetite review process (refer to the Risk Appetite Policy) and be presented to Group Risk Committee and Board Committees as required. The respective PRT RFOs are responsible for reporting on the risk appetite metrics per the standard

BAU process in collaboration with the respective DA SMEs, and in consultation with the Global Head, DA Risk Management and DA Risk team. The respective Business Heads /Relationship Managers /Accountable Executives are responsible for providing data to report on the metrics as part of their business and revenue generating activities.

b. **Strategic Planning Development**: DA Risk Appetite is an explicit input into development of the Group Strategy and Corporate Plan, driving proactive risk management.

c. **Breaches of Risk Appetite and/or escalation triggers**: 1LOD and 2LOD must ensure immediate escalation and prompt mitigation of breaches of DA Risk Appetite and/or escalation triggers, following the standard Risk Appetite reporting process with tracking to completion of the remediation actions. Monitoring, reporting and escalation of breaches is to follow the requirements in the Risk Appetite Policy and include notification by the Business to the DRC.

d. **Metrics**: Metrics must provide insight into the key drivers of the Group's DA profile (refer Appendix 3), monitored through both the Group Risk Appetite metrics and monitors, and the DA specific risk appetite metrics and monitors[10].

2.7. Position Statements

a. **Approval**. New Position Statements ("PSs"), Summary of Approach ("SoA") and Risk Acceptance Parameters ("RAPs") or changes to existing to PSs, SoAs and RAPs must be accepted and endorsed by the DRC prior to submission to the Group Responsibility and Reputational Risk Committee ("GRRRC"). The GRRRC has final authority to approve or reject new proposals or changes to existing documents.

b. **Review**. DA PSs, SoAs and RAPs must be assessed by Reputational Risk, the DA COE and the DA Risk team every two years or earlier where material changes arise.

Risk Identification, Assessment and Monitoring

2.8. Identification of DA Risks and exposure

a. **Clients**. All RMs must consider client's DA exposure and/or activities at the time of onboarding for new-to-bank clients and on-going reviews of existing clients. This includes consideration of source of wealth for Private Banking.

b. **Products (including specific DA)**. All Business Heads at Group and Country level, and SC Ventures Accountable Executives and/or SCB Appointee Directors to Ventures (collectively known as "Business Heads" or BHs for the purpose of this policy) must consider risks associated with DA Activities as part of the business case to be prepared for new products and as part of the on-going review process for identification of changes of existing products.

c. **Projects (Projects / Partnerships / Ventures / Investments)**. Accountable Executives ("AEs") or equivalent must consider risks associated with DA Activities as part of the project plan, including from external stakeholders.

d. **Suppliers and Third Parties.** BHs and AEs must consider DA related risks arising from suppliers and third parties who are identified to provide DA related services including technology, arising from Products or Projects identified, where applicable. Third Party Risk Management ("TPRM") needs to be adhered to with completion of Vendor and Non-Vendor Risks Assessments, prior to signing a

[10] More information on Group Risk Appetite is present in the Group Risk Appetite Policy available on GovPoint.

contract and going live with suppliers and third parties. Relevant RFOs and DA SMEs are to be consulted, where applicable, as part of the risk assessments. BHs and AEs must monitor suppliers and third parties in accordance with TPRM requirements and DA COE standards and guidelines.

e. **Registration with DA COE**. RMs, BHs and AEs must register all identified Clients, Products and Projects with DA COE. This registration must be prior to inducting or onboarding DA related Activities by the Businesses; Business line authority approval for funding or progressing into Proof of Concept ("POC") for products; relevant Business line authority approval for funding or progressing a project into POC.

2.9. Assessment, Management and Escalation of risks

a. **Scope of Higher Risk DA activities or Client Types**. 1LOD with the DA COE must review and evaluate whether the Clients, Products and Projects are within the scope of the Higher Risk DA Activities or relevant Client types. The assessments may be reviewed and challenged by the DRC, relevant RFOs, DA SMEs and the DA Risk Team. Those assessed as Higher Risk are to be subjected to an enhanced due diligence assessment of DA related risks for the applicable PRTs before taking on the Activities. This assessment must include third parties identified in 2.8 (d). The DRC will assess the need for notification to the PRA or relevant regulator(s).

b. **Management of Higher Risk DA activities or Client Types**. Based on section (a), 1LOD must complete the DA specific enhanced due diligence assessment for the applicable PRTs for Clients, Products and Projects and obtain sign-off from the respective PRT RFOs or delegates. The DA specific risk assessment is complementary to the risk assessments specified by the PRT RFOs under their respective policies and standards.

   1LOD must present the DA specific risk assessment to the DRC and obtain the DRC's recommendations to support, not support, or support with conditions. The assessment must clearly provide the 1LOD view of the inherent risk posed to the Group, the proposed controls to manage the risks, and the expected residual risk. Where a residual risk is elevated, the 1LOD must comply with relevant Group requirements to accept or treat the elevated residual risk. The assessment must also consider the inherent and residual risk profile against the Group's Risk Appetite and assess whether the activity is within appetite.

   As part of the risk assessment, the Business is to consult with the DA COE to ensure relevant controls in relation to assessment of DA risks required for testing scenarios, objectives, business cases and/or minimum entry/exit criteria for testing phases are outlined in the relevant documentation for the Client, Product or Project (where known) by the Business, with controls and residual risks reviewed by the relevant PRT RFOs, and DA SMEs.

c. **Onboarding of specific DA coins or tokens**. Where a specific DA coin or token is being assessed for onboarding or trading, BHs must complete an additional assessment to admit the specific DA with the DA COE and Product Services against the Group DA Admission Guidelines. The DA admission assessments must be presented to and supported by the DRC and DA SMEs, prior to onboarding of the specific DA coins or tokens.

   i. For SC Ventures[11] onboarding of DA is subject to the Group's DA Admission Guidelines or the DA Assessment standard approved at Go-Live of the Venture, provided that there are no material gaps from the Group's DA Admission Guidelines. The approval to onboard DAs resides with the relevant SC Ventures/ Ventures Committee/Forum, with notifications to the DA COE and DA Risk teams, including copies of the DA assessments and approvals.

[11] SC Ventures here specifically refers to the SC Ventures Business Unit, SC Ventures Investments or Funds undertaking DA related Activities, or commercially live Ventures.

d. **Updates to DA related Products**. DA related activities with respect to financial instruments must be against a Product Programme Guide ("PPG") under the Group Product Governance Policy and Standard managed through Product Services. PPGs and associated risk assessments for Products where there are new or changes to existing Products containing DA specific elements must be reviewed under the oversight and consultation of the DRC for DA related risks in addition to the BAU governance and oversights requirements.

e. **Escalation to GRRRC**. For cases registered with the DA COE, a Higher Risk Framework Assessment is carried out to identify Higher Risk cases for enhanced due diligence. From there, a Consolidated Risk Assessment is submitted to the DRC, and cases might be further escalated to GRRRC as required. For cases assessed as not Higher Risk, where potential reputation or stakeholder perception risk is identified in accordance with the Reputational and Sustainability Risk Materiality Assessment, the risks must be assessed and accepted by the authorities set out in Risk Authority Matrix for Stakeholder Perception Risks in the Reputational Risk Policy, with potential escalation to GRRRC. Escalations of non-Higher Risk cases to GRRRC must be noted to the DRC.

f. **Escalation to GRC**. DA products, projects or clients may be referred to or escalated to GRC as part of BAU process or on recommendation from DRC.

g. **Environmental Risk**. In cases where potential environmental and social risks are identified or when advised by the Committee, the Client, Product or Project must refer to Reputational and Sustainability, and Climate Risk teams for further considerations. The risk must be assessed and accepted by the authorities set out in the respective risk policies.

h. **Implementation of controls.** 1LOD must ensure that for each applicable PRT, the inherent risk, mitigants or controls, and residual risk is clearly documented and obtain sign-off from relevant PRT RFO or delegates in consultation with relevant DA SMEs in line with the requirements as stated in the Group Operational Risk Policy. This includes the implementation and monitoring of controls through the RCSAs as delegated by the Policy/ Standards Owners.

2.10. Monitoring

a. **All DA exposures**. 1LOD for clients, products and projects must monitor adherence to conditions underlying the DRC's support and changes in clients, products and projects which require re-assessment to be conducted. 1LOD is to keep the DA COE informed on the progress of conditions.

b. Processes must be implemented by Process Owners to adequately monitor changes in the risks for the applicable PRTs posed by the clients and their commercial activities.

2.11. Risk Data Aggregation, Data Quality and Reporting

a. Requirements outlined in the Group's ERMF on Risk Data Aggregation, Risk Reporting and Data Quality apply to this policy.

2.12. Stress Testing and Internal Capital Adequacy Assessment Program (ICAAP)

b. **Assessment**. The respective BH/ AE in conjunction with DA COE must ensure DA Activities from Clients, Products and Projects are assessed in accordance to the requirements set out in the Enterprise Stress Test Policy, ICAAP and as well as relevant standards and policies. Assessment to be presented to DRC.

c. **Review**. DRC will review and challenge the Businesses' DA risk considerations in collaboration with the relevant Group RFO or delegates.

2.13. Skills training

a. All relevant staff must be trained with appropriate skills, knowledge and capability to undertake their roles and responsibilities. DA COE, in consultation with the DRC, is responsible for designing, developing and delivering an appropriate level of training to enable Group wide domain knowledge. Businesses, RFOs and Functions are responsible for role specific training for their teams.

2.14. Risk Culture and Insurance Coverage Review

a. **Risk culture**. The respective Businesses with the DA COE, working jointly with Reward Governance, must ensure that DA activities are considered through the relevant remuneration processes as overseen by the Group Performance Remuneration Committee so that the incentives provided for engaging in this activity do not encourage excessive risk-taking.

b. **Insurance Coverage Review**: The respective Businesses with the DA COE must engage with Insurable Risk annually to ensure that the Group's strategy and exposure to DA-related Clients, Products, or Projects are reviewed as part of the Group's annual insurance renewal process and the need for further considerations on the appropriateness of the coverage under the relevant insurance policies appropriately assessed.

3. RESPONSIBLE ROLES FOR IMPLEMENTING THE MANDATORY POLICY STATEMENTS

Roles and Responsibilities

The following roles are critical for the implementation of the policy:

Lines of Defence ("LOD")	Roles	Primary Responsibility
First Line of Defence ("1LOD")	**For Clients:** Relationship Managers ("RMs") **For Products:** Business Heads ("BHs") **For Projects:** Accountable Executives ("AEs") or Chief Product Owners under New Ways of Working	• Responsible for identification, assessment, monitoring and escalation of risks associated with DA Activities arising from Client, Product and Projects. This includes the notification requirement to DA COE • Responsible for the submission of DA-related risk assessments alongside approval documentation to the DRC and existing Governance fora • Responsible for the DA risk assessments for notification to the PRA and regulators (where applicable) • Responsible for providing data and information under reporting requirements including risk appetite metrics and monitors, risk information reporting and stress testing.
	Business Senior Manager	• Responsible for reviewing and oversight of the overall

Lines of Defence ("LOD")	Roles	Primary Responsibility
	Function (SMF) within CCIB, CPBB and SC Ventures (SCV)	risk assessment for any planned Higher Risk DA Activities including confirmation that they understand the DA related risks and that the DA SMEs have been appropriately engaged • Responsible for reviewing and signing-off on attestations and risk assessments for DA related Activities as part of regulatory submissions.

	Digital Asset Centre of Excellence
	("DA COE")
		• Responsible as the business partner and the Group's 'single point of contact' for the Group-wide view on DA across Business Segments
		• Responsible for supporting the alignment of strategy across the business lines and providing advice across Business and Functions.
		• Responsible for industry engagement with industry groups and supporting regulatory engagement.
		• Responsible for the following frameworks and processes across Group:
		  • DA Admission Guidelines and Questionnaire
		  • Inventory of DA initiatives.
		  • Evaluation of DA initiatives against the DA Higher Risk Activities Framework to determine enhanced due diligence.
		• Responsible for providing subject matter expertise across the Group in support of the following activities:
		  • Regulatory Engagement
		  • Engagement with third parties to provide DA domain education to the Group.
		  • Business line strategy and planning as it relates to DA
		  • Investments into Digital Asset related firms or tokens.
		• Responsible for coordinating and working with RM, BH, or AE to carry out responsibilities as stated in this policy

Second Line of Defence ("2LOD")	Group Chief Risk Officer ("GCRO")	• Senior Manager Function responsibilities to define the Group's framework for managing DA related risks
	Global Head, ERM and Deputy CRO SC Bank, Global Head, DA	• Delegated responsibility from GCRO to define the Group's framework or approach to managing DA related risks, including setting and reviewing policies for DA risk considerations • Responsible for working with Group RFOs to propose and review DA Risk Appetite for consideration and

Lines of Defence ("LOD")	Roles	Primary Responsibility
	Risk Management; DA Risk Team	reviewing reporting on compliance with the DA Risk Appetite metrics • Responsible for review, challenge and advice on the Group DA Risk Profile, DA risk assessments and submissions overseen by the DRC in conjunction with the PRT RFOs and DA SMEs • Responsible for supporting Group Committee and regulatory engagements on the DARMA
	PRT RFO and PRT Subject Matter Experts ("PRT SMEs")	• Responsible for providing the overall end-to-end signoffs for DA initiatives under BAU governance and approval models under oversight and consultation with DA SMEs and Global Head, DA Risk Management. This is to support the identification, assessment and monitoring of DA risk associated with Clients, Products and Projects. • Responsible for updates to relevant and interconnected policies, standards and guidelines to provide oversight, review and challenge to DA related initiatives. • Responsible for setting and maintaining Risk Appetite metrics, to ensure that DA-related risks impacting or arising within their Risk Type are understood and considered, including the main drivers of risk and potential mitigants • Responsible for the advice on the need for further review and notification prior to execution where Higher Risk DA Activities are being undertaken • Responsible for responses to provide a consistent assessment of DA-related risks across the Group, with review of documented evidence of identified risks and recommended controls.
	Digital Assets Risk Committee ("DRC")	• Responsible for oversight and consultation to Support/ Not Support/ Support with conditions, for Clients, Products and Projects for DA related Activities based on DA risk assessments presented by RM/BH/AE • Responsible for review and recommendation of the Group's DA risk appetite • Responsible for providing access to PRT and DA SMEs to assist in the identification, assessment and endorsement of DA-related risks to enable existing Business authorities to derive comfort that DA-related risks have been appropriately assessed by the relevant expertise • Responsible for monitoring the Group's planned and actual DA-related exposure for notification to regulators and evaluation in balance sheet management activities

Lines of Defence ("LOD")	Roles	Primary Responsibility
		such as ICAAP.
1LOD and 2LOD	Existing governance fora and authorities for approval of Clients, Products and Projects	• Responsible for the overall review and approval of the Client, Product and Projects, taking into consideration the DA risk assessment and recommendation from DRC, for approval per existing authorities. • For avoidance of doubt, all SC Ventures (SCV) initiatives are within the scope of this policy and will follow the SCV specific governance process, taking into consideration the DA risk assessment and recommendation from the DRC.
Third Line of Defence ("3LOD")	Group Internal Audit	• Responsible for ensuring the Third Line of Defence duties have been carried out as required in the Enterprise Risk Management Framework

4. POLICY RELATED AUTHORITIES

Global Head Enterprise Risk Management ("ERM") and Deputy Chief Risk Officer ("CRO") SC Bank, maintains the overall approval authority on the DA policy and associated dispensations. Through this policy, the Global Head, DA Risk Management is delegated approval authority for non-material changes to the DA policy and its associated dispensations, which may include but not limited to, minor updates to the DA Higher Risk Activities Framework, minor updates to processes and minor updates to any standards, artefacts or guidelines mapped to this Policy. Such approvals granted have to be ratified post-facto with Global Head ERM and Deputy CRO SC Bank.

5. CONNECTED PROCESSES AND ACTIVITIES

The following key processes as per the Group Process Universe are impacted by the above policy requirements.

a. Processes for Anti Money Laundering and Client Due Diligence for CCIB, CPBB and SCV. This included processes for Client On-boarding and Account management and periodic reviews.

b. Product management and review and approval processes for Global Banking, Retail Banking, Wealth Management, Financial Markets, Transaction Banking and Corporate Finance including SC Ventures

c. Processes for Transaction Screening and Transaction Processing

d. Processes for Onboarding of Third Parties and Vendors, and Third-Party Risk Management

e. Processes for protecting the integrity of the market and maintaining proper market conduct standards

6. POLICY EFFECTIVENESS REVIEW

The management of Digital Assets Risk manifests across the PRTs. The Policy Owner is responsible for monitoring and affirming the overall effectiveness of this Policy. The Policy effectiveness review will consider the following:

- Review of the output of oversight activities conducted by DRC
- Effectiveness of the policies and standards interconnected with this Policy and performed by the respective Policy Owners as per the Framework and Policy Governance Standards.
- Review of control monitoring results, residual risk assessment and any applicable risk acceptances or root cause reviews for the processes connected to this policy
- Evidence of gaps or inefficiencies gathered from stakeholders through use of the process connected to this policy
- Review of relevant management information and risk assessment presented to DRC
- Processes for protecting the integrity of the market and maintain proper market conduct standards
- Annual confirmation to the Global Head, DA Risk Management on the effectiveness of their policies and standards for DA risk management as part of the annual effectiveness review process.

7. INTERCONNECTED POLICIES & STANDARDS

Policy Name	Risk Type & Risk sub-type	Policy Owner	Area of connection
Credit Policy for CCIB Client Coverage	Credit Risk – CCIB	Head Credit Policy CCIB	Credit guidelines for lending to DA related counterparties.
CPBB Credit Risk Management Policy	Credit Risk - CPBB	Global Head of Wealth Lending Risk	Credit policy establishes the credit underwriting rules for PvB clients for the source of wealth from DA
Enterprise Stress Testing Policy	All principal risk types as defined in ERMF	Head, Capital Risk Oversight	Stress testing and capital requirements arising from DA related activities
Group Antimoney Laundering and Counter terrorist Financing Policy	Financial Crime – Anti Money Laundering (and Terrorist Financing)	Global Head, AML	The AML/CTF Policy refers to and relies on Group CDD Standards and relevant Appendices to fulfil regulatory requirements for Client due diligence (“CDD”) and Know Your Client (“KYC”) obligations at onboarding and on an ongoing basis.
Group Operational Risk Policy	Operational Risk	Global Head, Operational Risk	The Group Operational Risk Policy refers to and sets out the mandatory policy statements for managing operational risk. In this instance, it would include Operational Risk Appetite, Risk and Control Self-Assessment, Response Management, Governance, Reporting

Policy Name	Risk Type & Risk sub-type	Policy Owner	Area of connection
			Requirements and Scenario Analysis.
Group Fraud Risk Management Policy	Financial Crime – Internal Fraud Financial Crime – External Fraud	Global Head – Fraud Risk Management	The Group has considered the requirements of the UK Fraud Act 2006 and those Financial Conduct Authority (FCA). In this instance, going by the UK Fraud Act 2006, Fraud can be committed by: i. making false and or misleading statements regarding DA transactions and or by conduct (fraud by false representation); ii. deliberate concealment of what should have been disclosed e.g. By clients having a DA nexus (fraud by failing to disclose information); and iii. abuse of position /and or power.
Risk Appetite Policy	All principal risk types as defined in ERMF	Global Head, Risk Appetite and Stress Testing	Governance of the Group-level Digital Assets Risk Appetite Statement and Risk Appetite Metrics is conducted in line with the Group Risk Appetite policy and standards.
Group AntiBribery and Corruption ("ABC") Policy	Financial Crime - Anti Bribery and Corruption The Global CoHeads, FCC, have delegated the Global Head, ABC as the risk framework owner for Anti-Bribery and Corruption risk.	Global Head, ABC	Potential for loss due to failure by SCB Staff, or Associated Persons acting on behalf of the Bank, to comply with Bribery and Corruption laws or regulations, pursuant to dealings with Digital Asset transactions or products. Risk of Digital Assets used to pay or conceal bribes.
Group Sanctions Policy	Financial Crime – Sanctions	Global Head FCC Sanctions, High Risk Clients and Emerging Threats	Requirements for complying with all applicable sanctions and mitigating sanctions risks.
Group Information and	ICS. (Confidentiality,	Head, Information and Cyber	Requirements for risk identification and mitigation of data risks including key

Policy Name	Risk Type & Risk sub-type	Policy Owner	Area of connection
Cyber Security Policy	integrity and Availability of Information Assets, Information systems and technical infrastructure)	Security Policy	management associated with DA. Key Management is covered under Enterprise Key Management Technical Information Security Standard ("EKM TISS")
Product Governance Policy	Operational Risk - Product Mismanagement	Global head, Operational Risk	Requirements for product considerations
Change Governance policy	Operational Risk - Change Mismanagement	Global head, Operational Risk	Requirements for managing DA change initiatives
Group Tax Policy	Operational Risk - Tax Risk	Global Head, Tax & Functions Finance	Tax requirements arising from DA activities or exposures
Group Third Party Risk Management Policy	Operational Risk - Third Party Risk Mismanagement	Executive Director, Third Party Risk Management	Role and responsibilities in business/ functions and minimum risk and due diligence requirements
Corporate Action and new market entry policy	Operational Risk - Governance	Global Head, Corporate Development	Requirements when selling investments in Digital Assets through SCV etc
End User Computing Policy	Operational Risk - Transaction Processing	Global Head, Governance & Change	Use of manual applications (including spreadsheets) in the recording, monitoring, and reporting of Digital Assets activities
Sustainability Risk Policy	Reputational and Sustainability - Sustainability	Global Head, Risk Governance and Enterprise Risks	Impact on environment arising from high energy required to support the DLT technology employed in Digital Assets activities
Reputational Risk Policy	Reputational and Sustainability – Stakeholder Perception	Global Head, Risk Governance and Enterprise Risks	Implication to the Group's reputation when carrying out Digital Asset or having crypto exposure
Group Data Management Policy	Compliance – Data Risk	Global Head, Strategy, Governance and Core Compliance	Data must be clearly defined and understood before it is Group18ed in model development. Any data quality issues identified mist be escalated in line with the DM Policy.
Capital Management Policy	Treasury Risk – Capital Risk	Global Head, Treasury Capital	Requirement for DA activities and exposure to be considered in ICAAP
Group	Compliance Risk	CFCC Global	Conduct should comply with the

Policy Name	Risk Type & Risk sub-type	Policy Owner	Area of connection
Competition and Anti-trust Policy	– Market Conduct	Head, CFCC, CPBB & AME	requirements in the policy on how to manage potential anticompetitive conduct.
Group Conflict of Interest Policy	Compliance Risk - Conflict of Interest	Global Head of Frameworks and Policies	Activities giving rise to conflicts of interest arising from transactions must be identified, assessed and managed in accordance with the policy.
Group Market Conduct Policy	Compliance Risk - Market Conduct	Global Head, CFCC, CCIB & EA	This policy provides the requirements to protect the integrity of markets and sets out the proper market conduct standards and expectations for all Staff.

8. STANDARDS MAPPED TO THIS POLICY

Note: Currently there are no direct standards mapped to this policy. Various artefacts including guidelines and assessment frameworks are available on the Digital Assets Centre of Excellence Bridge page.

Standard Name	Risk Type	Standard Owner	Standard Approver

9. APPENDIX

Appendix 1: Terminology and Glossary

Definitions and terminology for DA are not standardised across markets or regulatory frameworks. For comparative purposes and consistency this document uses the following commonly found terms:

Term	Description
Alpha testing	Early test of the new product internally within the organisation
Beta Testing	A test of a product by outside users before the product goes live. Occurs after an internal alpha test, but before commercial launch
Central Bank Digital Currency (“CBDC”)	Central bank digital currency – A digital asset for payments issued by a central bank and denominated in the national unit of account. A direct liability of the central bank. Specific design choices will be localised.
Cryptoassets (“CA”) or Digital Assets (“DA”)	Cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology (“DLT”) and can be transferred, stored and/or traded electronically
Distributed	DLT is the underlying technology behind most cryptocurrencies. It

Term	Description
Ledger Technology ("DLT")	provides chronological history of transactions, on a peer-to-peer network of nodes. Blockchain is a type of DLT; but not all DLT is blockchain.
DA exchange providers	Businesses that allow customers to trade DA for other assets including conventional fiat money or different digital currencies. They can also be market makers that take bid-ask spreads as transaction commissions for their services or charge fees as a matching platform
Custodian wallet providers	entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies
Decentralised Finance (DeFi')	A system by which financial products become available on a public decentralized blockchain network, making them open to anyone to use, rather than going through middlemen like banks or brokerages. DeFi refers to a system by which software written on blockchains makes it possible for buyers, sellers, lenders, and borrowers to interact peer to peer or with a strictly software-based middleman rather than a company or institution facilitating a transaction
Exposure - Direct	Examples include the Group's projects in providing custodian services of DA For the purpose of this policy, for planned direct exposure to DA Activity, there is a requirement to notify PRA who may request submission of a risk assessment covering both financial and non-financial risks associated with the intended exposure.
Exposure - Indirect	Examples of indirect exposure include minority equity investment in the entities dealing in DA For the purpose of this policy, for planned indirect exposure to DA Activity, there is a requirement to notify PRA.
E-money Tokens	This category refers to any token that is electronic money ("e-money"). E-money is defined as electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which is issued on receipt of funds for the purpose of making payment transactions and is accepted by a person other than the electronic money issuer. Examples: Stablecoins that reference underlying fiat currency like a USD coin.
Exchange token	May be called 'cryptocurrency'. Also known as 'cryptocurrencies', 'crypto-coins' or 'payment tokens'. Used as a means of buying and selling goods and services without traditional intermediaries. Decentralised; not issued or backed by a central authority. These tokens are designed to provide limited or no rights for tokens holders, and there is usually not a single issuer to enforce rights against. Currently outside the regulatory perimeter in most cases.
Privacy Coins	Privacy Coins are not traceable or linkable by way of transaction history on the blockchain. This type of coins usually have privacy features such as stealth addresses and ring confidential transactions. Stealth addresses feature enables the recipient to receive multiple payments through a single address, while at the same time ensuring there are no links on the blockchain between their address and any other address. Ring confidential transactions (RingCT) is a cryptographic tool that

Term	Description
	conceals the amount being transacted, while still allowing for the network to verify the amount without having to reveal any actual details.
Privacy enhancing tools	Privacy-enhancing tools that obfuscate transactions and/or identify of the owners such as • Mixers or tumblers; • Obfuscated ledger technology; • Internet Protocol (IP) anonymisers; • Ring signatures; • Stealth addresses; • Ring confidential transactions; • Atomic swaps executed outside of Exchanges; • Non-interactive zero-knowledge proofs; • Shielded privacy coins
Stablecoin	Aims to maintain its value relative to a specified asset or basket of assets; intended to be used as a means of payment or store of value. May meet security or e-money definitions. Some with sufficient scale may be 'global stablecoins' and subject to enhanced regulatory scrutiny.
Security token	A token with specific characteristics that provide rights and obligations akin to a share or a debt instrument. Generally subject to existing securities frameworks and fully regulated. If a token has any of the following characteristics, it is likely to be considered a security token: ➢ it provides access to voting rights or represents ownership or control; ➢ it represents money owed to the token holder; ➢ it provides a right to subscribe for other specified investments, such as shares; ➢ it confers a contractual or property right over other investments; ➢ it acts as a vehicle through which profits or income are pooled; and/or ➢ it represents a right in a specified investment, such as a share. Examples: Equity Tokens; Debt Tokens; or Real Asset Tokens; Real estate fractional interest tokens; Asset backed tokens.
Utility token	Grants holders access to current or prospective products or services, but without the same allocation of rights as security tokens. May meet the definition of e-money in some cases, and may be regulated as such.

Appendix 2 – Higher Risk Activities Framework

INTERNAL

DA Higher Risk Framework ("DAHRF") – Scope and application

The Scope of the DA Higher Risk Framework aligns with the scope of the DA Risk Management Policy ("DARMP"). Out of scope of the policy, in line with the DARMP, are the following activities:

- Distributed Ledger Technology ("DLT") solutions where DLT solutions are applied purely for operational efficiency, including where there may be a transfer of rights
- Operating expense accounts for DA entities: Operating expense accounts to manage activities such as rent, and employee wages where existing Client Due Diligence requirements will apply.

Application of the DAHRF is set out in the DARMP which includes the following:

Scope of Higher Risk DA activities or Client Types

- 1LOD[1] with the DA COE must review and evaluate whether the Clients, Products and Projects are within the scope of the Higher Risk DA Activities or relevant Client types.
- The assessments may be reviewed and challenged by the DRC, relevant RFOs, DA SMEs and the DA Risk Team.
- Those assessed as Higher Risk are to be subjected to an enhanced due diligence assessment of DA related risks for the applicable PRTs before taking on the Activities. This assessment must include third parties identified in 2.8 (d) of the DARMP.
- The DRC will assess the need for notification to the PRA or relevant regulator(s)[2].

Management of Higher Risk DA activities or Client Types

- 1LOD must complete the DA specific enhanced due diligence assessment[3] for the applicable PRTs for Clients, Products and Projects and obtain sign-off from the respective PRT RFOs or delegates.
- The DA specific risk assessment is complementary to the risk assessments specified by the PRT RFOs under their respective policies and standards.
- 1LOD must present the DA specific risk assessment to the DRC and obtain the DRC's recommendations to support, not support, or support with conditions. The assessment must clearly provide the 1LOD view of the inherent risk posed to the Group, the proposed controls to manage the risks, and the expected residual risk.
- Where a residual risk is elevated, the 1LOD must comply with relevant Group requirements to accept or treat the elevated residual risk. The assessment must also consider the inherent and residual risk profile against the Group's Risk Appetite and assess whether the activity is within appetite.
- As part of the risk assessment, the Business is to consult with the DA COE to ensure relevant controls in relation to assessment of DA risks required for testing scenarios, objectives, business cases and/or minimum entry/exit criteria for testing phases are outlined in the relevant documentation for the Client, Product or Project (where known) by the Business, with controls and residual risks reviewed by the relevant PRT RFOs, and DA SMEs.

[1] 1LOD refers to relevant Line of Business (LOB) leading with proposal or initiative

Digital Asset Risk Management Policy (DARMP) can be found here on GovPoint

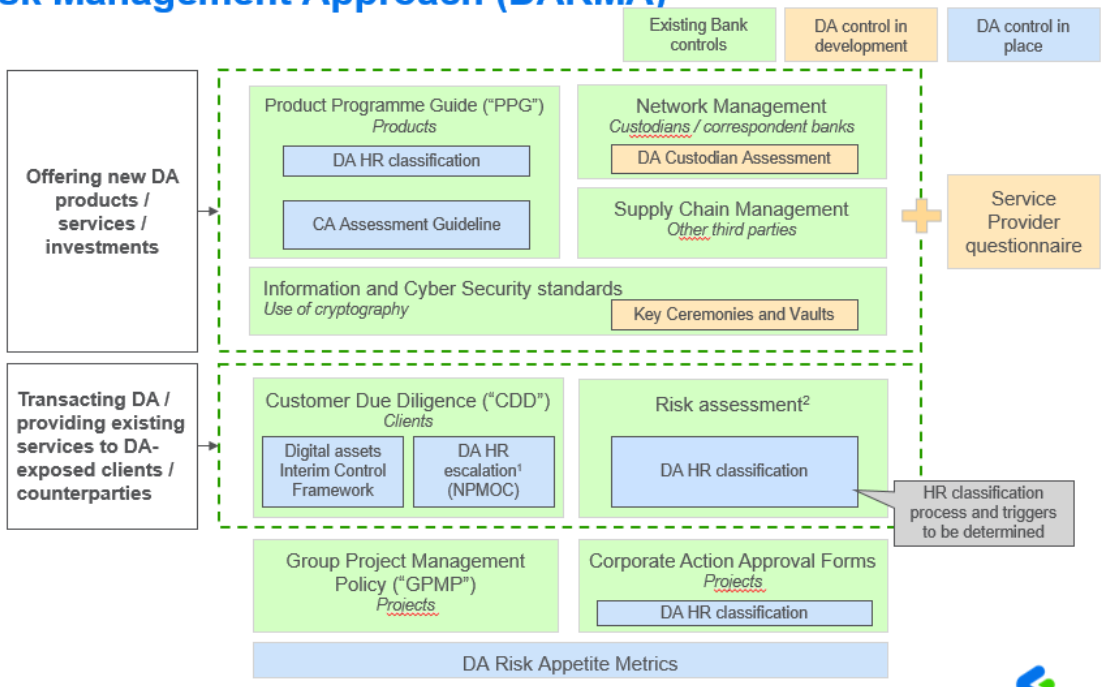
[2] In the PRA's Dear CEO letter (2018), firms were reminded to .." (iii) deal with regulators in an open and co-operative way, and disclose appropriately anything relating to your firm of which we would reasonably expect notice." The approach to notifying regulators is set out in the DARMP.

[3] This is the 'New Initiatives Consolidated Risk Assessment (NICRA)'

INTERNAL

Role of Digital Asset ("DA") Higher Risk ("HR") Framework within the Digital Asset Risk Management Approach (DARMA)

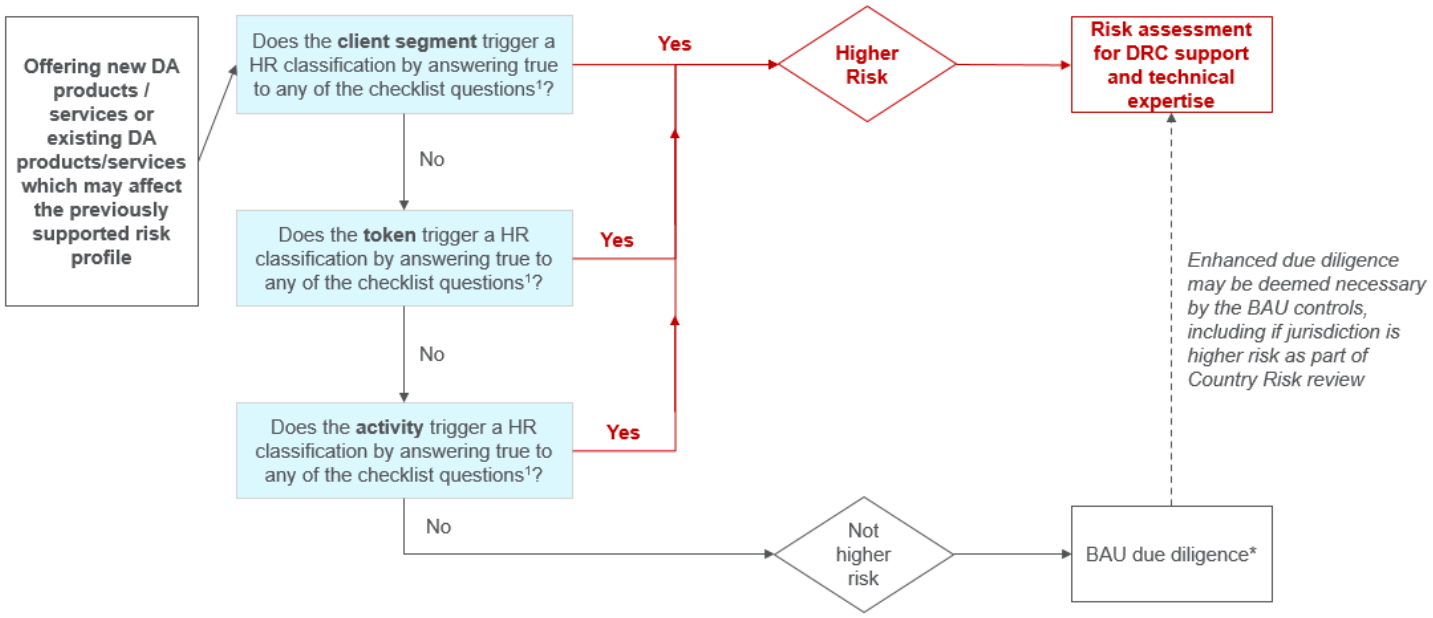
- Product approvals and client onboarding should be conducted via Business As Usual ("BAU") controls, e.g., CDD for clients, PPG for products and services
- The DA HR Framework includes a delineation between entities and products:
  - HR process and triggers for transacting DA and / or providing existing services to DA-exposed clients / counterparties;
  - HR process and triggers for offering new DA products / services / investments;
  - In addition there should be an HR process and triggers as part of Credit Assessment (to be developed in future)
- In target state, BAU controls should be enhanced to capture the HR Framework classification requirements



1 - Virtual Asset Service Providers (VASPs, or CASPs) are currently a prohibited client type under the current OneBank CDD standard. An interim approach has been approved to onboard select CASP clients into the CCIB FI FinTech segment under the CASP CDD Standard experiment, which has been supported by the CCIB Client Lifecycle Non-Financial Risk Committee. VASP/CASP client relationships are still subject to dispensation approval by the Global Head of AML and classified as higher risk clients from a group CDD perspective, but are not classified as higher risk under the DA HR Framework if using standard fiat products. VASPs are subject to oversight by the New Payments Methods Oversight Committee ("NPMOC"), which can escalate to other Committees including the CCIB Client Risk Committee (CCIB CRC) or Digital Asset Risk Management Committee (DRC) as appropriate. Non-standard use of products e.g. for Stablecoin reserve management will trigger DA HR classification.
2 – Risk assessment: key PRTs including Credit / Traded / Treasury.

Decision tree to determine HR classification for offering new DA services

The Business Leads with the DA COE recommend the HR classification which is reviewed by the relevant DA Subject Matter Experts and Risk Framework Owners to determine whether the initiative is to be classified as an HR DA Activity.

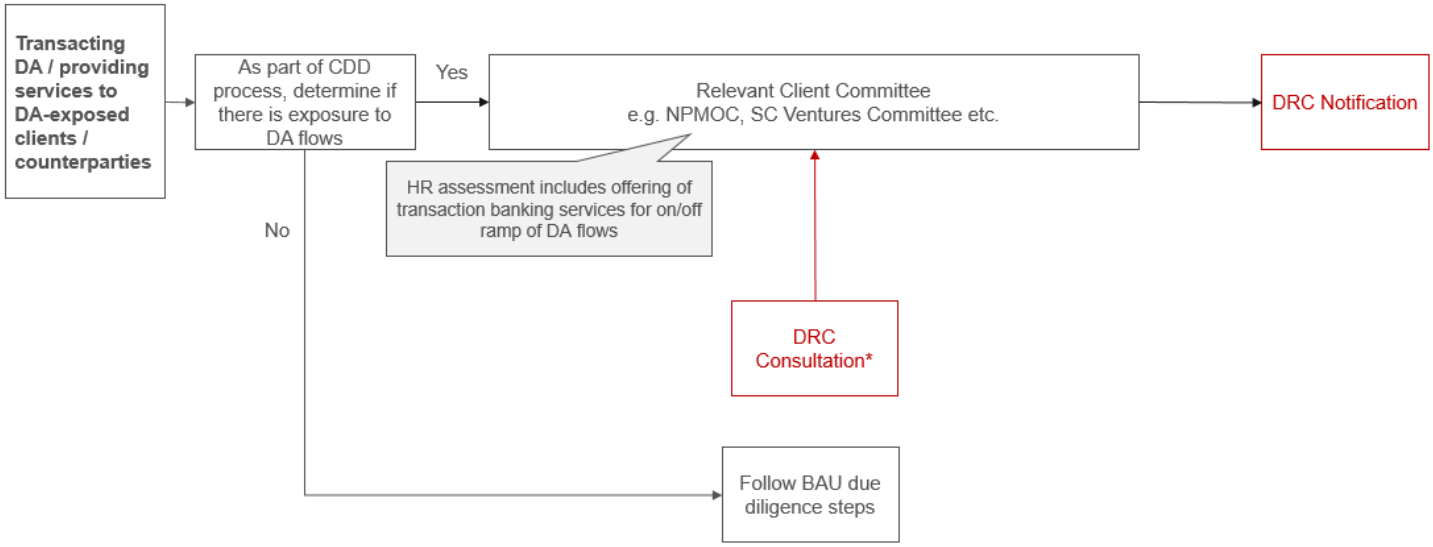


[1] Checklist questions can be found on Slide 7 and further details on Slide 13

* Instances may arise where a proposal is first assessed as 'Lower Risk, but subsequent incidents or changes / refinements to the proposal update the classification to "Higher Risk". In such instances, DA enhanced due diligence is to be followed which includes review/support by DRC.

INTERNAL

Decision tree to determine HR classification for providing existing services to DA-exposed clients



6 *DRC review and support is requisite to the approval of the DA activity by the BAU Approving Committee. As part of the consultation DRC may request confirmation from Subject Matter Experts engagement.

INTERNAL

Offering new DA products / services: HR classification is triggered if answer to any of the below is True

	Questions	True?
Client checklist	DA products / services are provided to retail[1] consumers and/or clients	☐
Token checklist	Transactions and coin provenance cannot be reliably established, and block explorer infrastructure is not easily accessible	☐
	The project and associated entities have pending investigations or regulatory / legal action in any of the jurisdictions relevant to the project or in the United Kingdom ("UK"), European Union ("EU"), United States ("US"), Hong Kong ("HK"), Singapore ("SG") or the United Arab Emirates ("UAE")	☐
	The issuer of asset backed tokens / stablecoins does not have independent, reputable audit reports on reserves is not regulated by a strong regulator, and/or issues tokens in a different jurisdiction to where the services are provided	☐
	The protocol has known exploits over the past 36 months[2]	☐
	Network operations has known network wide incidents in the past 12 months[2]	☐
Activity checklist: Key handling / on-chain transactions	Activity for SCB own purposes, or fulfillment or delivery of product or service to client requires on chain transactions on permissionless networks directly by the Group or its vendor	☐
	There is evidence of significant Financial Crime Risk or inherent limitation to monitoring Financial Crime Risk	☐
	Transactions include from and to un-hosted wallets	☐
	The initiative involves interaction with an automated, smart contract cross-chain bridge as part of product / service	☐
Activity checklist: On/off-balance sheet exposure*	Material leverage is provided to clients for DA activities	☐
	Exposure includes material[3] DA balances at trading venues or dedicated custodian	☐
	Exposure includes DA yield generating products	☐
	Exposure includes investments[4] in DA-focused firms with principal risk exposure to DAs	☐
	Exposure includes Decentralised Finance ("De-Fi") participation, e.g. via Decentralised Exchanges ("DEX") with Automated Market Maker ("AMM"), smart-contract-lending or staking	☐

[1]Retail client means all CPBB clients and includes bank initiatives that provide services to a group of retail type equivalent individuals where they are not directly clients of the bank; e.g. a venture business providing DA services to such retail type equivalent individuals.
[2] Minimum requirement to assess in consultation with ORM and ICS to screen using relevant tools. [3] Criteria relating to materiality of DA balances will be communicated in due course.
[4] Criteria relating to DA investments and materiality will be communicated in due course.
*See definition on following slide

7

Appendix 3 – DA Risk Appetite

INTERNAL

DA RA metrics (1/3)

UPDATED

Full list of newly/new subset approved metrics at the MT RA Level

This is the complete list of four MT RA for Committee noting, as well as eight MI plus six MI metrics which are still under consideration and will be monitored to assess viability.

PRT	New metrics to specifically set tolerances for the DA business or as a DA subset to existing metrics	Rationale	Risk Appetite	Escalation Level	Phase	Category
Reputational and Sustainability	•Very High DA cases (initiatives) for approved projects, clients, products and transactions (rolling twelve month basis)	Under the Reputational and Sustainability Risk Type Framework and where applicable: clients, transactions, products and strategic coverage decisions require a Reputational and Sustainability Risk Materiality Assessment. High/Very High cases require approval by the Group Responsibility & Reputational Risk Committee and represent those decisions that carry a heightened potential to cause a high degree of reputational damage to the franchise. The DRC also has authority to escalate matters to GRRRC where there are material reputational concerns.	~~5~~ 2	~~3~~ 1	A	2
Operational and Technology	•Last 12 months Operational Risk ("OR") losses including stress events related to DA	Cumulative OR losses over last 12 months related to Digital Assets including stress events defined as events leading to losses greater than USD2m	$2 MM	$1 MM	B	2
	•Elevated Residual DA Risks (Very High/High)	Very High and High residual risk related to Digital Assets	3	2	B	2
	•New DA Product releases and assets without appropriate and justified approvals in a month1	# of new DA product releases without appropriate approvals recorded in M7. Monthly data sourced from M7 and manually assessed by Group SME. Events tagged to "Product Management" sub-type are shared by Reporting team with SME for manually assessment i.e. if event qualifies for reporting under the Risk Appetite metric.	0 (actual threshold)	-	A	2

Where a metric or management monitoring information (either Phase A or Phase B) applies for a DA activity, the Business will need to assess the activity against the metric or MI during the analysis phase and the Business will be required to produce the metric before the activity is permitted to Go-Live."

1 A Metrics which can be measured / data is available now (manual intervention may be required)

B Metrics which require infrastructure/feeds to gather data which may require new or enhancements to current systems.

INTERNAL

DA monitors (2/3)

NO CHANGE

Full list of newly/new subset noted metrics for Management Monitoring

Management monitoring where thresholds have been calibrated

PRT	New metrics to specifically set tolerances for the DA business or as a DA subset to existing metrics	Rationale	Management Monitoring	Escalation Level	Phase	Category
Information and Cybersecurity	•Contracted third parties with access to DA systems not assessed for security risk	DA management is increasingly dependent upon third parties where suppliers may/ will access the Group's DA. The Group will need to assure the information security controls are in place to. If third parties cannot meet or sustain the Group's security requirements, they may pose an unacceptable level risk as Group's reputation would be at stake and Group is accountable owner for the DA. This metric reports the percentage of contracted third parties with access to DA systems not assessed for security risk.	0 (actual threshold)	0 (actual threshold)	B	1
	•Instances of loss of client or SC private keys	Measures whether the Bank have a line of sight around the governance and deployment of cryptography keys and cryptography operations and of access management controls – for the DA services/products, vendor/partner/platform offered in collaboration with our Bank	0 (actual threshold)	-	B	1
	•Findings from design assurance reviews of DA partners / vendor products which are overdue /not remediated per agreed timelines	This metric measures whether the Group has a view of the ICS risks that have been identified on these 3rd party CA vendors / suppliers / partners/Products and the remediation status around it when SC partners go through third party security assessment.	1	0	B	1
	•Cases where TSPA or design review, SIA or equivalent have not been completed for DA partner / vendor products	If third parties/vendor/products cannot meet or sustain the Group's security requirements, they may pose an unacceptable level risk to the Group. This metric reports the percentage of DA partner /vendor/ products had not gone through Bank Security review or equivalent risk review.	5.00%	3.50%	B	1
	•High/Critical ICS incidents related to DA Partners / Vendors / Products that SC collaborates upon	Cyber threats will seek way to achieve their objective by exploiting trusted relationships and supply chains by seeking out vulnerabilities continuously. Hence designated Group authorized representative (and/or such other Group contact(s) notified in writing by Group to Third Party) and Group Cyber Defence Centre are notified of information security incidents involving Group Data within the timelines prescribed under the Agreement. This metric tracks the number of such High/Critical ICS incidents related to Products, DA Partners, Vendors that SC collaborates upon for their digital asset management reported to CDC (Cyber Defence Center).	1	0	B	2
Traded	•Trading Book DA Stress Loss	The metric captures the potential for market risk stress losses related to DA	$5M	$4.5M	A	2
	•Trading Book DA Value at Risk ("VaR")	The metric captures the potential for market risk losses in normal market conditions	$1M	$0.9M	A	2
	•Total DA Counterparty Credit Risk ("CCR") exposure (Potential Future Exposure)	New business where the risk exposure will be a small percentage to the overall PFE of our CCR Portfolio.	$200M	$180M	A	2

2 Where a metric or management monitoring information (either Phase A or Phase B) applies for a DA activity, the Business will need to assess the activity against the metric or MI during the analysis phase and the Business will be required to produce the metric before the activity is permitted to go-live.

A Metrics which can be measured / data is available now (manual intervention may be required)

B Metrics which require infrastructure/feeds to gather data which may require new or enhancements to current systems.

DA monitors (3/3)
Additional Management Monitoring Metrics Under Consideration

NO CHANGE

Management monitoring information under consideration

Subject to data availability and Business pipeline, metric performance trends will be monitored to assess viability as Monitoring Metrics. .

PRT	New metrics to specifically set tolerances for the DA business or as a DA subset to existing metrics	Rationale	Phase	Category
Operational and Technology	•$ value loss from inventory of coins which has been forked	A fork happens whenever a community makes a change to the blockchain's protocol, or basic set of rules. This metric monitors the changes in rules which could be interpreted positively (shift to proof of stake) or negatively (vulnerability patch) and has direct influence on the cryptocurrency value.	B	1
	•Instances of missed hard forking schedules	A hard fork happens when the code changes so much that the new version is no longer backward-compatible with earlier blocks. In this scenario, the blockchain splits in two: the original blockchain and new version that follows the new set of rules. This creates an entirely new cryptocurrency This metric monitors this divergence as historically the divergence has coincided with security vulnerabilities and often results in a corresponding divergence / devaluation of assets still trading on the older version of the blockchain.	B	1
Credit	•CCIB: DA exposure [Corporate]	Digital Assets exposure concentration in corporate portfolio. NOTE: the definition of DA exposure is under review	B	2
	•CCIB: DA exposure [FI/ NBFI]	Digital Assets exposure concentration in the financial institution portfolio. NOTE: the definition of DA Exposure is under review	B	2
Financial Crime	•Number of High-risk customers using digital assets	With the introduction of the new CDD standards, and the further refinement of the DA categorisations*, this metric supports the measurement of possible concentration of higher risk activities in higher risk clients as a lead indicator. (*Currently all DA-related customers are rated as higher risk.)	B	1
	•Fraud risk loss related to DA	This metric supports the measurement of impact of crystallised fraud events linked to digital assets, including external and internal fraud events. The delay in this KRI is due to the dependence on the manual identification of related incidents in M7(bank borne losses) and client related losses which are dependent on data gathering in the area operating the asset.	B	2

Where a metric or management monitoring information (either Phase A or Phase B) applies for a DA activity, the Business will need to assess the activity against the metric or MI during the analysis phase and the Business will be required to produce the metric before the activity is permitted to go-live.

3

A — Metrics which can be measured / data is available now (manual intervention may be required)

B — Metrics which require infrastructure/feeds to gather data which may require new or enhancements to current systems.

10. Version Control Table

Name	Changes made	Approved by	Version number
Maria Zameer **Francesco Roda**	The new Digital Asset Risk Management Policy has been introduced which defines the key principles for managing risks associated with Digital Asset activities. The Policy sets out the principles on the identification, articulation, and assessment of Principal Risk Types across clients, products, or projects.	Jason Forrester	1
Maria Zameer **Matthew Smith**	This version update adopts the new ERM Policy template. This version makes changes in the below areas: • includes the updated definition of Digital Assets as adopted from the UK Financial Services and Markets Bill issued in December 2022 • includes the DA Risk Statement as stated in the Enterprise Risk Management Framework • includes delegations of authorities for the Global Head, Enterprise Risk Management for approving material changes; and for the Global Head, DA Risk Management to approve non-material changes • clarifies on the roles and responsibilities. • clarifies on the updates to governance structures on DA risk management by PRT RFOs. This is current process and is now incorporated in policy as part of annual refresh.	Jason Forrester	2