AM TW Risk Management Framework

Classification	Internal	
Document administrator	AM TW Risk Officer	
Approved by	AM TW Board	Date of approval: Oct 1, 2024

UBS

Table of Contents

Introduction

This section describes the purpose of UBS AM TW Risk Management Framework and the entities in scope.

1.1. **Purpose**

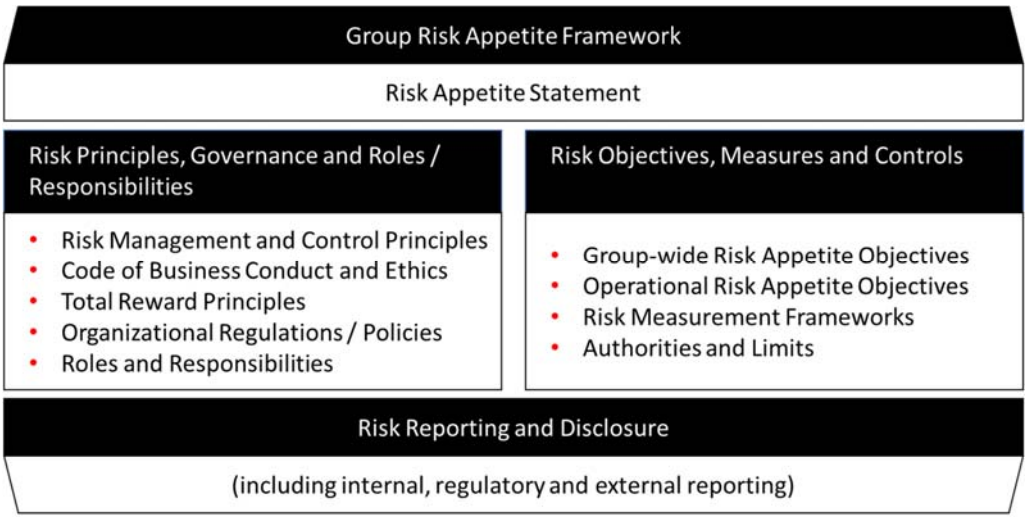
The purpose of this document is to set out the approach to risk management within UBS Asset Management Taiwan Limited (herein referred to as 'AM TW') including

- the overarching risk management systems in place, which address strategic, governance, operational, market, investment and liquidity risk at both fund operator and fund level;
- the key processes for identifying, assessing and managing risks; and
- the risk management framework for AM TW.

AM TW adopts the approach established by Group UBS in respect of risk management and this Framework additionally sets out the key processes applicable to UBS AM TW, as part of its obligations under *SITE Risk Management Principle,*

The AM TW Risk Management Framework is designed to ensure risk-taking at every level of the organization is in line with our strategic priorities, capital and liquidity plans, as well as our pillars, principles and behaviors.

In respect of risk appetite for AM TW, the framework is formulated in line with the UBS Risk Appetite Framework (1-C-005068), with which legal entities and divisions must comply. A schematic overview of the Group Risk Appetite Framework and its components is shown below.



Risks are an inherent consequence of being in business, and the taking, managing and controlling of risk are core elements of AM TW's business activities. Our aim is not to eliminate every source of risk,

but rather to identify and understand the risks and potential risk concentrations and to achieve an appropriate balance between risk and return while adhering to our principles and behaviours at all times.

1.2. **Scope**

This document applies to UBS Asset Management Taiwan Limited.

As noted above, this framework forms part of the broader UBS Group risk management framework and Additional Key Documents for reference are set out in section 5.1.

Governance

The purpose of this section is to describe the role that the Board, the AM TW F2B and Risk Forum, 1st line, 2nd Line and 3rd line of Defence play in the governance of UBS AM TW Risk Management Framework.

2.1. Roles and Responsibilities of the AM Taiwan Board of Directors

The AM Taiwan Board of Directors (herein referred to as "the Board") is responsible for monitoring the effectiveness of AM TW Risk Management Framework including satisfying itself through appropriate reporting and oversight by the UBS Asset Management Taiwan Front-to-Back and Risk Forum. After due consideration, it is the Boards' responsibility to formally approve TW Risk Management Framework

The Board should be aware of all risks (i.e. market, credit, liquidity, operation, legal, reputation, climate, economic and political and other risks) and take the accountability of the risk management

Specific Responsibilities of the Board within the context of owning the Risk Management Framework:

- The Board should supervise the implementation of risk management framework, monitor the climate risk strategy and review the impact on reputation due to climate risks,
- Consider escalations from the TW F2B; and
- Challenging the executive on actions proposed and implemented as a result of breaches, or where there is risk acceptance impacts on the company and
- Supervise the implementation of sustainability and climate risk management and plan and review the impact on reputation.
- Ad-hoc Review and approval of AM TW Risk Management Framework

2.2. Roles and Responsibilities of the AM TW F2B and Risk Forum

The UBS Asset Management Taiwan Front-to-Back and Risk Forum (herein referred to as "TW F2B") supports the AM Taiwan Location Head in his/her mandate to oversee the local operational environment and facilitate a sound and comprehensive alignment of the business and business support/control functions, towards the implementation and maintenance of the AM agreed business strategy.

The TW F2B escalates issues as appropriate to the AM APAC F2B Forum and/or the Board, in accordance with the UBS Group-wide Escalation Framework (1-C-010170). The AM TW F2B members will raise relevant topics related to the operational environment, to enable effective information sharing, discussion, and challenge.

The TW F2B is responsible for updates, risk overview, High-level minutes and action log and does not have decision-making authority. Actions will be determined by the AM Taiwan Location Head, supported by inputs and contribution from the AM TW F2B members.

2.3. Roles and Responsibilities of AM TW Risk Management

AM TW Risk Management should establish AM TW Risk Management Framework, take the lead in the implementation of risk measurement, monitoring and assessment of risk management on annual basis upon the approval of AM TW Risk Management Framework from the Board.

2.4. Roles and Responsibilities of the 1st Line of Defence

Activities are performed by the business or function management. The business or function owns its risk exposures and is accountable for maintaining effective processes and systems to manage its risks, including robust and comprehensive internal control, documented procedures, in compliance with applicable laws, regulations and policies and escalate and propose remedial action whenever the risk is observed and report the action status to the TW F2B until the risk returns to green.

2.5. Roles and Responsibilities of the 2nd Line of Defence

Compliance and Operational Risk (C&ORC) are a member of the TW F2B and play a role to provide an independent oversight and challenge of financial and non-financial risks arising from the firm's business activities and to protect against non-compliance with applicable laws and regulations.

2.6. Roles and Responsibilities of the 3rd Line of Defence

The third line of defence activities are performed by Group Internal Audit (GIA) and Taiwan Statutory Internal Audit (SIA). GIA/SIA are responsible for evaluating the overall effectiveness of governance, risk management and the control environment, including the assessment of how the first and second lines of defence meet their objectives.

Principles

The purpose of this section is to describe the AM TW Risk Management Framework in the context of the Group, to provide an overview of risk identification, assessment, monitoring and reporting.

3.1. Risk Culture

Our commitment to risk management begins with risk culture and setting the right 'tone from the top'. Risk culture involves in our day-to-day job making good decisions for the interest of our clients and shareholders, treating others the same way you would like to be treated, and speaking up without fear of retaliation on matters which do not exemplify our high standard.

With the help from our functional partners, the following key risk culture themes are identified for AM Taiwan.

Accountability – Sense of ownership to ensure correct outcome for firm and clients (e.g. Proactively follow up on risk items and issues).

Behaviour – Exercising diligence when complying with risk standards and risk supervision. Identifying and address risk flags on a timely basis. (e.g. Holistic risk assessments, fact-checking).

Challenge – Critically and constructively assess information as presented and speak up when something does not look right (e.g. Challenge line managers/business instructions and clients' response, escalate potential red flags).

3.2. Consideration of relevant Group policies, frameworks and risk appetite statements

AM TW has designed this Risk Management Framework to demonstrate compliance with SITE Risk Management Principle. In developing the AM TW Risk Management Framework all relevant Group policies and frameworks have been taken into consideration, particularly the Group Risk Appetite Framework (1-P-005068) and Risk Control Framework – UBS Entities (1-P-001915) with which UBS legal entities and Business Divisions must comply. Employees of AM TW must affirm on an annual basis, compliance with key policies and frameworks applicable to it. AM TW is not defined by the Group as a Significant Entity or a Significant Regional Entity and as such these policies do not require the entity to have defined Limits, Triggers and Targets for certain Primary risks and have exposure monitoring in-place against these risks and do not require it to establish risk appetite statements. However, AM TW has given consideration to local regulatory guidance, SITE Risk Management Principle and has designed a Risk Management framework to include both qualitative statements and quantitative assessments along with group internal thresholds to ensure that the framework complies with all relevant Group policies.

As per the Risk Control Framework – UBS Entities policy, entities must align their quantitative risk appetite statement with the business division and so AM TW has reviewed both the Asset Management Primary Risk Appetite Statement and the Asset Management Operational Risk Appetite Statement and ensured that where relevant the quantitative risk appetite statements are aligned and set within the divisional tolerances.

AM TW has defined Risk Taxonomies as applicable to AM TW to classify all of the risks that it has identified as being relevant to the entities based on their business activity, leveraging Group taxonomies (such as the Operational Risk Taxonomy) where relevant.

3.3. Risk Identification, Assessment and Management

UBS AM TW has implemented a comprehensive approach to the identification and assessment of the risks AM TW is exposed to, based on the various Group, Divisional and local policies/processes in place across different risk types and business functions. This approach enables the TW F2B and the Board to have confidence that all risk types have been considered in the identification stage, and that there is a framework in place to ensure a consistent approach to the assessment of the risks that are relevant to AM TW.

When risks are identified as being relevant for AM TW they are assessed for materiality and managed through a variety of different mechanisms, including by independent functions, depending on the type of risk and reported to the TW F2B. This includes

- the front-to-back control environment of UBS AM Taiwan
- the business, regulatory and operational risk environment of UBS AM Taiwan
- service level quality and scope, operational KPIs
- potential risk and impact of the issues escalated by various operational change related steering Forums and provide input for perceived operational risks mitigation.
- client related Cross-border, Conflicts of Interest business matters
- Financial Risk
- Investment Risk
- Fair Client Treatment
- Client Complaints
- Climate Risks including but not limited to physical and transition risks
- Sustainability Development

3.4. Monitoring and Reporting

TW F2B will monitor and manage the identified risks. Each Owner is responsible to provide relevant management information to TW F2B and any other relevant functional committee or forum. TW F2B will ensure that:

- appropriate management actions are triggered.
- escalation process is followed.
- remediation plan, including target dates and tolerances are adhered to; and
- relevant reporting is timely provided to the Board if required.

AM TW Risk Management should report the climate risk management implementation and the impact to reputation and legal obligation for the Board's assessment on quarterly basis.

3.5. Disclosure

- AM TW should disclose the risk management information including but not limited to policy, qualitative and/or quantitative measure, the supervision of climate change management in term of

risk and opportunity by the Board, and oversight and assessment of climate risk on sustainability report or public website periodically since June, 2024.

3.6. Risk definitions and descriptions

Risk type	Description
Market Risk	Market risk is the risk of loss resulting from adverse movement in market variables such as rates, FX, equities, credit spreads and other measures.
Credit Risk	Credit risk is the risk of loss that may occur from the failure of any party to abide by the terms and conditions of any financial contract. Credit Risk Framework – UBS AM (4-P-001148) defines how AM fulfil its fiduciary duty to clients and demonstrates compliance with UBS risk management and control standards regarding Credit Risk. AM typically acts as authorized agent in entering investment and hedging transactions on behalf of clients with brokers and counterparties. Credit transactions subject to the policy include: - Securities and loan trading that do not qualify as cash/non-credit transactions - Securities financing (including securities lending, repos, reverse repos) - Bilateral and cleared OTC derivatives (including forwards and FX) Exchange traded derivatives - Prime brokerage - Participation notes Standard credit terms are defined for ISDA Master Agreements, Schedules, Credit Support Annexes (CSA) and ancillary documents. These establish baseline terms that are acceptable from a Risk Control perspective.
Liquidity Risk	Liquidity risk is the risk that a Fund cannot meet client redemptions at current prices while fulfilling obligations to remaining shareholders in line with the Fund's stated objective. The primary goal of a fund's liquidity program is to meet redemption obligations without incurring substantial cost or unfair treatment to investors. The AM Liquidity Manual (Global Liquidity Risk Management (LRMP) describes the framework of role and responsibilities. Additionally, AM Liquidity Escalation Playbook (Liquidity Management Event Playbook) is to provide guidance when considering liquidity risks and protocol during a crisis
Operation Risk	Operational risk is defined as the risk of a loss resulting from inadequate or failed internal processes, people or systems, or from external causes (deliberate, accidental or natural). As a result of AM TW's business model, operational risk is the most material risk to which AM TW is exposed. The specific operational risks managed by AM TW are outlined in more detail in operational risk taxonomy which is aligned with the Group's Operational Risk Framework.
Legal Risk	Legal Risk is defined as the risk of a loss resulting from regulation violations, breaches, overlooking or invalid contracts.
Strategy risk	Strategy Risk is defined as the risk of a loss resulting from wrong decision, inappropriate execution, lacks of response to the competitors or to change of industry.
Sustainability and Climate Risk	Sustainability and climate risk (SCR) is defined as the risk that UBS is negatively impacted by or negatively impacts climate change, loss of biodiversity, human rights infringements, and other environmental, social and governance matters. Climate risks can arise from either changing climate conditions (physical risks: Economic costs and financial losses resulting from the increasing severity and frequency of extreme climate events) or from efforts to mitigate climate change (transition risks: The risks related to the process of adjustment towards a low-carbon economy). SCR may manifest as credit, market, liquidity and operational risks for UBS, resulting in potential adverse financial, liability and reputation impacts. They may also negatively impact the value of investments. Sustainability and Climate risk management process will follow the group principles of APAC climate risk management and Sustainability and Climate Risks which are met the standard of SITE Risk Management Principle in term of principles, procedures and disclosure.

Operational Risk Taxonomy	Risk Themes	Taxonomy Description
1.Employment or Licensing Practices	- Employment or Licensing Practices	The risks arising from acts inconsistent with laws, rules and regulations or the firm's human resources policies governing employment practices, discrimination, compensation, employee related taxes and benefits. Risks arising from loss of key staff, excessive turnover, and failure to implement comprehensive succession plans for key positions. Failure to perform an appropriate pre-employment screening process including stringent due diligence and background checks in order to ensure on-boarded staff are fit and proper. Failure to ensure employees are where required appropriately registered or licensed. Applies to both full-time employees, contractors and temporary staff.
2. Market Conduct	- Insider dealing and misuse of market sensitive information - Standards for fair and orderly markets - Fair and appropriate client pricing - Other Market Conduct	Failure to maintain appropriate standards of market conduct to ensure a fair and effective market and meet applicable laws, rules and regulations and regulatory expectations governing activities undertaken on or through a market or in pricing/ transaction related bilateral interactions between counterparties. UBS needs to take appropriate measures so that our own actions do not amount to abuse, distortion of the market or uncompetitive/ unfair pricing and, where UBS facilitates transactions with clients, to take reasonable steps to ensure these standards are applied for clients' actions. The risk includes failure to take appropriate steps to prevent or detect misuse of market sensitive or confidential client transactional information, or inappropriate communication of pending research, and of failure to prevent or detect arrangements or behaviour that restrict, distort or prevent competition or the abuse of a dominant position or failure to prevent tying.
3. Product and Service Lifecycle	- Product and Service Lifecycle	The risks arising from failures, flaws, or mistakes in the design, development, approvals, understanding of the risk characteristics (including sustainability and climate risk), investment management, tax reporting requirements , of UBS manufactured ('in-house') and/or 3rd party products and services (including electronic trading), both at launch and through the product/service lifecycle, and compliance with applicable standards, laws, rules and regulations.
4. Investment Suitability	- Investment Suitability	The risks arising from an inability to demonstrate adherence to applicable Client Suitability standards, laws, rules and regulations.

Operational Risk Taxonomy	Risk Themes	Taxonomy Description
5. Cross-border Business Conduct	- Cross-border Business Conduct	The risk arising from the failure to identify and comply with laws, rules and regulations and policy requirements applicable to cross-border business conduct and provision of financial services to clients, prospects or the collaboration with external service providers as well as from the failure to adhere to the firm's restrictions to prevent local permanent establishment. The risk that the firm fails to take appropriate measures to adequately manage and control cross-border business conduct when providing financial services during cross-border travel or non-travel related interaction with clients or prospects. The risk arising from the failure to establish the clients' fiscal compliance status and to comply with client-related reporting obligations based on regulations such as Foreign Account Tax Compliance Act or Automatic Exchange of Information.
6. Internal and External Fraud	- Internal fraud - External fraud	The risk of employees (including contractors / temporary employees) or third parties engaging in actions intended to defraud or misappropriate assets (including through cyber enabled channels) from clients, prospective clients, and/or the firm, or failure to timely detect or comply with applicable laws, rules and regulations in regard to fraud.
7. AML and KYC	- AML and KYC	The risk that UBS fails to conduct appropriate due diligence when establishing client relationships and throughout the life of the business relationship including performing enhanced due diligence where the relationship indicates the potential for a higher level of AML risk including AML related reputational risk, e.g. politically exposed person, sensitive country affected party, sensitive industries and other AML risk categories related to the Money Laundering regulation. In addition, the risk that UBS fails to comply with applicable Anti-Money Laundering (AML) laws, rules and regulations and policy requirements to prevent the financing of illegal activities (including terrorism) through financial systems and failure to report suspicious activities or responds to requests from relevant authorities.
8. Sanctions or Embargo Violations	- Sanctions or Embargo Violations	The risk that UBS fails to comply with any measure or restriction (including those often referred to as "embargoes") taken by one or more countries (or their respective government agencies) or international organizations under laws, rules, or regulations, which is aimed at restricting dealings of any kind (including the import and export of goods, capital or services) with or involving another country, specific persons, legal entities, organizations or goods.
9. Bribery and Corruption	- Bribery and Corruption	The risk that UBS fails to identify and comply with laws, rules, regulations and policy requirements applicable to bribery and corruption and to take appropriate steps to prevent an employee or UBS Entity from making, offering, promising, receiving, soliciting or arranging for a bribe in any form (e.g. payments, gifts, business entertainment or anything of value), be it directly or indirectly (e.g. through an intermediary), or to detect any such activity. Risks associated with such failure are particularly pronounced, where a Public Official (including a state-owned enterprise) is involved.

Operational Risk Taxonomy	Risk Themes	Taxonomy Description
10. Corporate Governance and Frameworks	- Corporate Governance and Frameworks	The risk of failing to have a robust Corporate and Legal Entity Governance structure in place including the implementation of effective governance and policy frameworks. This also includes the failure to ensure the adequate set-up, oversight, management, approval and reporting of UBS entities and failure to set standards, authorities and limits including responding to an increase in loss potential for primary risks (Treasury, Market and Credit risks) and Sustainability and Climate Risk (SCR), in accordance with the firms risk appetite. The risk of failure to comply with Laws, Rules and Regulations in respect of the aforementioned risks.
11. Financial and Regulatory Reporting	- Financial Reporting - Regulatory Reporting	The risk of failing to ensure financial and regulatory reports required to be produced by UBS and submitted to external authorities are materially complete, accurate, and submitted in a timely manner. The scope of this taxonomy covers UBS's mandatory regulatory reporting obligations to external regulatory authorities under laws, rules and regulations, as well as UBS's financial reporting under IFRS, local accounting and local corporate tax requirements. Financial and regulatory reporting requirements exist at UBS Group (consolidated) level, as well as at individual country, jurisdiction and entity levels. This risk also includes internal financial management reporting and financial planning. A regulatory authority is defined as one of the following types of financial industry regulators: (i) Banking and securities regulators; (ii) Self regulators in the banking and securities industry; (iii) Central banks; and (iv) Exchanges. A financial authority may include financial industry regulators, as well as Tax Authorities, International and National Accounting Standard Boards and Companies Registers.
12. Model Risk	- Model Risk	The risk of adverse consequences resulting from inadequate model governance (including a failure to comply with applicable laws, rules and regulations), model development, model implementation, model use or model validation processes. The taxonomy risks apply to both internally developed or vendor models used by UBS to conduct its business, for purposes including (but not limited to); identifying and measuring risks, valuing exposures, valuing instruments or positions, conducting stress testing, assessing adequacy of capital, managing client and own assets (e.g. tactical or strategic asset allocation in client portfolios), algorithmic trading, measuring and monitoring compliance with rules and regulations (e.g. financial crime analytics), identifying patterns in data, surveillance activities, or meeting financial (e.g. IFRS 9/CECL) or regulatory reporting requirements (Pillar 3) and issuing public disclosures.

Operational Risk Taxonomy	Risk Themes	Taxonomy Description
14. Data Management	- Data Management	The risk of firm's data not being properly managed and/or not meeting the required quality in terms of completeness, correctness and timeliness. The taxonomy covers risks arising from: • using or maintaining incorrect and/or incomplete data or providing data on a non-timely basis, that creates errors and/or might negatively impact processes within the firm and/or internal/external reporting; • inadequate or missing governance/control of the data, resulting in an inability to satisfy business requirements, and applicable laws, rules and regulations. As well as an inability to effectively measure whether data is fit for its intended purpose.
15. Technology Failure or Disruption	- Technology Failure or Disruption	Impact from outage, degradation and /or inaccurate data within (i) internal applications and infrastructure or (ii) technology used by 3rd parties in the services consumed by the firm. This could be caused by accident or by intent. This risk also includes the failure to identify and comply with laws, rules and regulations relevant to technology failure or disruption (e.g. non adherence to regulatory reporting of incidents).
16. Transaction Processing and Execution	- Transaction Processing and Execution	The risks associated with the lifecycle of a transaction from its capture, execution, and processing. The taxonomy covers risks arising from: • primary risk adherence to transactional limits; • initial capture and execution of trade/transaction; • All subsequent processing of trade/transaction (i.e. the lifecycle of pre-settlement, lifecycle management, settlement and post-settlement activities) and failure to comply with applicable laws, rules and regulations. All types of trade/transaction booked in the Front Office or processed by Operations are included.
17. Third Party Management and Inter-entity Outsourcing	- Third Party Management and Inter-entity Outsourcing	This taxonomy covers risks arising from the procurement and consumption of services, including outsourcing provided by third parties, their subcontractors and / or other UBS governed legal entities. Service delivery is based on contractual arrangements. The taxonomy includes risks associated to ineffective frameworks, policies and / or execution of procurement and Third Party Risk Management (TPRM). It also covers risks arising from failure to comply with laws, rules and regulations. Only services consumed and / or processed by one or multiple UBS governed legal entities qualify as service under this taxonomy. The TPRM policy (1-P-008361) and TPRM Reference Guide cover the definition of third party type, applicability of risk domains per third party type, consistent approach of risk assessment and monitoring, the end-to-end risk management process of lifecycle of a third party engagement, and annual risk assessment review by 12 risk domains for risk assessment and monitoring of Third Parties across UBS. Detailed information on the scope of this Taxonomy is covered by TPRM Policy (1-P-008361) and TPRM Reference Guide at goto/tprm.
18. Business Continuity, Resilience and Crisis Management	- Business Continuity, Resilience and Crisis Management	The risk that UBS, when faced with an operational disruption, can not respond or recover its critical activities, processes or important business services within established continuity and resilience requirements (including any as defined by applicable laws, rules and regulations).

19. Privacy, Data Ethics and Records Management	- Privacy, Data Ethics and Records Management	Risks arising from not processing UBS data in line with applicable privacy, data ethics and records management requirements, and notably related to : • not processing personal data (collection, storage, creation and / or subsequent processing including data transfers) in line with applicable data privacy laws, rules and regulations (Data Privacy) • engaging in CID and Personal Data processing activities involving the use of Models or Data Analytics which do not meet data ethics principles and requirements (Data Ethics) • not categorizing information, not identifying and managing UBS records, and not adhering to storage limitation (disposal) requirements in accordance with applicable laws, rules and regulations (Records Management)
20. Cyber and Information Security	Cyber and Information Security	The risks arising from: • Cybersecurity or Information Security deficiencies, resulting in (i) inadequate protection of UBS information assets (UBS owned or third party owned information hosted by UBS) against theft, leakage, unauthorized cross-border data exposure (Data Confidentiality); (ii) cyber disruption of UBS technology estate leading to compromise of its availability and/or integrity. • Failure to identify and comply with laws, rules and regulations relevant to cyber and information Security (incl. non-adherence to regulatory reporting of incidents) • Failure to accurately identify threats from malicious cyber actors

Statements

The purpose of this section is to describe the qualitative statement and quantitative assessment, including the associated risk drivers, calculation measures and risk mechanism.

4.1. Financial Risk

Risk type	Assessment
Market Risk	APAC Risk Control utilizes quantitative techniques to identify and measure market risk through a combination of risk metrics and tools, including but not limited to ex-ante Tracking Error (TE), Value-at-Risk (VaR), stress scenarios profit or loss, early warning triggers, and red flag assessments to alert AM and Risk Control Management when PMs are approaching regulatory or operational Risk Control guidelines, through a number of internal and external risk systems including but not limited to GRS, MSCI Risk metrics and AM Atlas Limit Monitoring Tool.. APAC Risk Control reports key exposures and summarizes its independent view on emerging risks, including ad-hoc stress loss results, in Monthly F2B and risk forum. Market Risk identification, measurement, monitoring, reporting and limits will follow Market Risk and Liquidity Policy for Client Assets (4-P-003081) supplemented with UBS Asset Management Risk Control Handbook and Global Minimum Standards – UBS AM Market Risk.
Credit Risk	On a monthly basis, AM Credit Risk Control monitors compliance with the approved counterparty list adhering to the Credit Risk Framework – UBS AM (4-P-001148). Counterparties are approved for traded products (e.g., OTC, FX, ETD etc.), and in certain instances, restricted to specific business areas or instruments. Leveraging Credit Aggregation Tool (CAT) and AM Atlas limit monitoring tool, counterparty exposure concentration is monitored on a daily and monthly basis at the fund level against an internal threshold of 5% (or other % exceptionally approved) per Fund per Counterparty, calculated as the ratio of net exposure to AuM (or total exposure to AuM for cleared trades). Any breaches will be investigated and follow actions as listed in AM Credit Risk Framework. This will also be highlighted in Monthly Financial Risk Report and TW F2B. AM Credit Risk Control also reviews periodically the brokers used for Credit Transactions (except for directed brokerage). Risk-based approach is employed to determine the review frequency based on the credit worthiness of the brokers. Higher-risk (rated BBB+ / Baa1 or below, or unrated) brokers will be reviewed annually while low-risk (rated A- / A3 or above) brokers will be reviewed every 3 years. AM Credit Risk Control follows UBS AM Credit Risk Framework (4-P-001148) for the control and limit for credit risks.
Liquidity Risk	APAC Risk Control utilizes the Global Liquidity Risk Management (GLRM) platform and GRS to measure liquidity risks on a fund's asset and liabilities such as liquidity costs, redemption coverage ratios, stress scenarios, Liquidity horizons, and shareholder concentration Liquidity Stress tests are used in regular risk reporting and risk meetings. Historical and hypothetical scenarios are considered on a periodic basis to ensure stress testing remains current with active risks in the market. The liquidity risk analysis for TW funds in scope is included in the Monthly Financial Risk Report and presented to the TW F2B Liquidity Risk identification, measurement, monitoring and reporting will follow Market Risk and Liquidity Policy for Client Assets (4-P-003081) supplemented with UBS Asset Management Risk Control Handbook and Global Minimum Standards – UBS AM Market Risk.

Risk type	Assessment
Sustainability and Climate risk	At fund level: APAC Risk Control identifies, measures and monitors sustainability risks at portfolio level through a combination of risk at portfolio level including but not limited to UBS Consensus Scores, Weighted Average Carbon Intensity, UBS ESG Risk Flag and Climate Risk metrics (Physical and Transition Risks). These metrics are visible through GRS into tableau dashboards, monitored and reported at least on a monthly basis for all tradeable asset classes. Any funds identified with elevated risk in at least one of the metrics will be notified to portfolio managers and highlighted at TW F2B and board meetings. At entity level: AM TW will follow Sustainability and Climate Risks policy (1-P-004081). Our sustainability and climate risks are managed through the following SCR framework which is in line with the multi-year roadmap to integrate sustainability and climate risk into our financial and non-financial risk frameworks and related processes. There is a data model and a business process for scoring sustainability and climate risk at the company and asset levels, across a range of materially relevant types. 

4.2. Operational Risk Taxonomies

The operational risk taxonomy is used by all lines of defence for reporting of the risk profile. Operational Risks are aligned with the Operational Risk Taxonomy as defined in the Group's Operational Risk Framework policy (1-P-000017). It is to implement effective governance and policy frameworks including the adequate set-up, oversight, management, approval and reporting, set-up standards and authorities in the policy. Any risk is identified will be reported, monitored, and assessed at TW F2B. We aim to implement effective controls to reduce operational risk exposures.

These 18 risk taxonomies will be assessed for inherent risk, control environment and residual risk in the RCSA annually.

Risk Type	Qualitative Risk Statement
1.Employment or Licensing Practices	**AM TW** aims to manage employment issues appropriately and handle them consistently, fairly and in compliance with relevant regulations. AM TW ensures staff are appropriately registered, competent, and that any employee related conflicts are appropriately disclosed. AM TW does not tolerate any member of staff wilfully disregarding their training obligations or inappropriate employee behaviour and conduct.
2. Market Conduct	**AM TW** does not tolerate employees intentionally violating the policies and controls that have been put in place to mitigate the inherent risk, as well as strong governance around best execution and fair allocation for each client.
3. Product and Service Lifecycle	**AM TW** will continue to consider customizing products to fit the needs of clients as well as develop complex products for sophisticated institutional clients when required. New business or initiate are sent to TRPA for preapproval process and gain the relative functions' approval.
4. Investment Suitability	**AM TW** will follow product governance, design, and distribution to ensure that products are transparent and meet customer needs. Intermediaries are subjected to due diligence.
5. Cross-border Business Conduct	**AM TW** will follow group well embedded cross-border frameworks.
6. Internal and External Fraud	**AM TW** has no tolerance for any internal or external fraud and actively promotes a culture of integrity, collaboration, and challenge. The Group Whistleblowing Policy ensures that any incidents of unethical behaviour can be safely escalated, and disciplinary action taken as required.
7. AML and KYC	**AM TW** acknowledges the risk of heightened regulatory scrutiny placed on Financial Crime. AM TW has robust AML and KYC processes in place to protect against facilitating financial crime and has in place a risk-based Financial Crime control framework to mitigate the risks. AM TW will continue to perform necessary due diligence checks on clients including clients from higher risk jurisdictions**.**
8. Sanctions or Embargo Violations	**AM TW** will follow global processes in place to ensure compliance.
9. Bribery and Corruption	**AM TW** has a strong ABC framework, processes and controls in place to mitigate bribery and corruption risks.
10. Corporate Governance and Frameworks	**AM TW** has corporate governance arrangements that support the effective long-term operation of the business and meet regulatory and ethical expectations.
11. Financial and Regulatory Reporting	**AM TW** intends to promptly remediate any regulatory reporting issues once identified and communicate openly with regulators where material deficiencies are noted. AM TW leverages the Group's Regulatory Process Management database to ensure there is clear ownership and transparency on the status and accuracy of all regulatory reporting.
12. Model Risk	**AM TW** leverages the Group's comprehensive and well embedded Model Governance framework including associated Key Model Performance indicators to identify any issues with the models that it relies on.

14. Data Management	**AM TW** follows group policies/procedures and there are access approval process and internal controls in place.
15. Technology Failure or Disruption	**AM TW** Our technology platform is complex and global in nature, however we actively look to avoid the risk associated with incidents that cause outages with a specialist Technology Operation Centre monitoring the platform at all times, and Group wide Software Development Lifecycle and Minimum Enterprise requirements to ensure standards are met prior to deploying software to production. There is a well embedded Group wide Program Management Framework that is used to ensure appropriate business sponsorship and transparency of progress for all technology change projects.
16. Transaction Processing and Execution	**AM TW** implements comprehensive control framework and increased review frequency have been established. There are robust event management process and governance for investigation of instances and taking the appropriate remediation actions to strengthen controls.
17. Third Party Management and Inter-entity Outsourcing	**AM TW** follows internal TPRM policy (1-P-008361) and TPRM Reference Guide and external regulation "Directions for Operations Outsourcing by Securities Investment Trust Enterprises and Securities Investment Consulting Enterprises" to govern the oversight of Inter-entity Outsourcing arrangements and external third party providers. The depth and formality of the TPRM Framework application depends on the criticality and risks to UBS due to engagements with Third Parties. Ongoing risk management monitoring proportionate to the risk segmentation and third party type for the duration of the contractual arrangement (minimum standards for control and oversight) should generally include: - Periodic assessment of contractual arrangement(s) and output of the assessment provided into the risk segmentation approach, if applicable - Appointment of adequate resources (UBS staff) with the necessary expertise, authority, and accountability to oversee and monitor the Third Party relationship commensurate with the level of risk and complexity of the relationship - Monitoring of the Third Party's activities and performance
18. Business Continuity, Resilience and Crisis Management	**AM TW** has a crisis management plan that is designed with the objective that critical systems and services can resume operations within a reasonable period of time following disruptive events. Not all scenarios can be foreseen and adequately planned for, and unknown elements will occur, however, AM TW will not tolerate repeated or substantial interruptions resulting from failure to reasonably maintain IT infrastructure. Meanwhile, AM TW follows Third Party Business Continuity & Resilience Guideline (1-G-005355) which outlines the processes, resources, roles & responsibilities and annual third party BCR plan test and also adheres with BCR Testing Guideline (1-G-004919). Third Parties which support an Important Business Services where UBS has a dependency on the Third Parties enhanced recovery solutions, must align to standards for Higher Inherent risk except for regulated institutions. Third Parties which are overseen by a regulator which sets out requirements for Operational Resilience are also required to complete an BCR Attestation.
19. Privacy, Data Ethics and Records Management	**AM TW** follows internal Records Management Policy (1-P-001004) to ensure we comply with law or regulation during the entire Lifecycle of Records and, where applicable Information, irrespective of their format and we adhere to the Code and provides the framework to identify, manage and control data usage by UBS in an ethical and responsible manner in accordance with Group Data Ethics Policy (1-P-011810). There are key procedure controls and assessments in place.
20. Cyber and Information Security	**AM TW** follows Cyber & Information Security Policy (1-P-000162). Cyber and Information Security (CIS) program uses the three lines of defence model to manage its implementation and operation in accordance with the Non-Financial Risk (NFR) Framework. Functions in first line of defence actively participate in CIS governance processes and operate in accordance with their functional mandate and within their governance parameters.

4.3 **Other Risks**

Risk type	Assessment
Legal Risk	Business Unit is required to follow the internal control/procedure and conduct the annual assessment to ensure in compliance with policies and regulations. (iv) all employees are requested to affirm accounts, disclosure, policy and regulatory compliance via goto/aol on annual basis or whenever necessary.
Strategy risk	New business or initiate are sent to TRPA for preapproval process and gain the relative functions' approval.

Appendix

5.1. Additional Documents

This document should be read in conjunction with the following documents:

- Risk Authorities: 1-C-000004
- Our Code of Conduct and Ethics: 1-C-001254
- UBS Risk Appetite Framework: 1-C-005068
- UBS Group-wide Escalation Framework: 1-C-010170
- Governance Documents Framework: 1-P-000011
- Non-Financial Risk Framework: 1-P-000017
- Market and Treasury Risk Framework: 1-P-000031
- New Business Enablement (NBE): 1-P-001339
- Liquidity and Funding Risk Management Framework: 1-P-000142
- Sustainability and Climate Risks: 1-P-004081
- Credit Risk Framework - UBS AM: 4-P-001148
- Market Risk and Liquidity Policy for Client Assets - UBS Asset Management: 4-P-003081
- NFR Taxonomy Guidelines: 1-G-007622
- Risk Control Self-Assessment Guidance: 1-G-007624
- Non-Financial Risk Appetite Guidance: 1-G-007626
- Group Model Risk Appetite Framework: 1-G-008602
- Transactions Requiring Pre-Approval (TRPA) Guideline & Process (4-G-005758)
- Data Management (1-P-005490)
- Outsourcing (1-G-004943)
- Third Party Risk Management (TPRM) policy Third Party Risk Management (1-P-008361)
- Third Party Business Continuity & Resilience Guideline (1-G-005355)
- Third Party Risk Management (TPRM) Reference Guide
- BCR Testing Guideline (1-G-004919)
- Records Management Policy (1-P-001004)
- Group Data Ethics Policy (1-P-011810)
- Cyber & Information Security Policy (1-P-000162)

Other internal documents:

Asset Management - risk management program: (https://intranet.ubs.net/en/asset-management/chief-operating-officer/know-your-risk.html)

- AM Liquidity Manual (Global Liquidity Risk Management (LRMP))
- AM Liquidity Escalation Playbook (Liquidity Management Event Playbook)

AM Risk Control Minimum Standards documents: (https://intranet.ubs.net/en/group-functions/group-risk-control/global-am-chief-risk-officer.html)

- UBS Asset Management Risk Control Handbook
- GLOBAL MINIMUM STANDARDS - UBS AM Market Risk
- GLOBAL MINIMUM STANDARDS - UBS AM Credit Risk