3 de novembro de 2026

20/2026-BSM

U P D A T E D S U P E R V I S I O N S T A N D A R D

Participants in B3's Listed and OTC Markets

Re: **Publication of the Updated Supervision Standard on Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing (AML/CFT)**

BSM Market Supervision ("BSM"), in the exercise of its duties, hereby informs the market of the publication of the updated Supervision Standard No. 18/2025 on AML/CFT, which incorporates the amendments introduced by the Brazilian Securities and Exchange Commission ("CVM") Resolution No. 245/2026, as well as the enhancements identified during BSM's regulatory review process. The update includes: (i) greater emphasis on continuous and enhanced monitoring requirements; (ii) reinforcement of the obligation to assess the maintenance of client relationships throughout the business relationship, in accordance with the Risk-Based Approach and the criteria established by each Participant; (iii) further detailing of beneficial owner identification and verification procedures, including compliance with restrictive lists; and (iv) enhancements to the provisions applicable to Politically Exposed Persons ("PEPs").

The provisions contained in the updated Supervision Standard are not intended to exhaust all regulatory obligations relating to this matter, and it is the duty of each Participant to verify the requirements applicable to the activities it conducts in the securities market.

This Supervision Standard shall become effective on November 3, 2026, and shall revoke Supervision Standard No. 18/2025, published on October 9, 2025.

Additional information may be obtained by calling +55 (11) 2565-6200 (option 1) or by e-mail at bsm@bsmsupervisao.com.br.

3 de novembro de 2026

20/2026-BSM

S U P E R V I S I O N S T A N D A R D

Participants in B3's Listed and OTC Markets

Re: **Update to the Supervision Standard on Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing (AML/CFT)**

BSM Market Supervision ("BSM"), in the performance of its functions, hereby issues this update to the Supervision Standard ("Supervision Standard") with the purpose of strengthening the monitoring and reporting duties that must be observed by Participants in the Listed and OTC market segments regarding Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing ("AML/CFT"), considering the regulations and guidelines in force issued by the Brazilian Securities and Exchange Commission ("CVM"), as well as the rules issued by B3 S.A. - Brasil, Bolsa, Balcão (“B3”).

This Supervision Standard is not intended to exhaust all regulatory obligations related to the matter. It is the responsibility of each Participant to verify the requirements applicable to its activities, taking into account its size, transaction volume, complexity, activities carried out in the securities market, and the risks identified in its Internal Risk Assessment ("IRA").

The Participant's duties relating to client registration, although referenced in this Supervision Standard, are addressed in detail in the Supervision Standard on Client Registration.

The terms defined in this Supervision Standard are consistent with the BSM Glossary[1] or are defined throughout this document.

This Supervision Standard is divided into three (3) sections and their respective subsections: (I) Participant's duties; (A) AML/CFT Policy; (A.1) Know Your Customer Process; (A.2) Know Your Employee, Know Your Relevant Service Provider and Know Your Investment Advisor Processes; (B) Senior Management and Responsible Officer; (C) Risk-Based Approach; (C.1) Minimum Requirements; (C.2) Risks; (C.3) Financial Capacity and Assets Monitoring; (C.4) Monitoring and risk classification of Non-Resident Investors; (D) Internal Risk Assessment; (D.1) Internal Risk Assessment Report; (D.2) Effectiveness Indicators; (E) Monitoring, analysis and reporting of atypical situations; (E.1) Analysis of atypical situations; (E.2) Alert analysis; (E.3) Reporting obligation; (E.4) Monitoring of restrictive lists; (F) Training and capacity building; (G) Documentation and evidence; (II) BSM Supervision; and (III) Enforcement.

I. Participant's duties

[1] Available at: https://www.bsmsupervisao.com.br/normativos-bsm?section=glossario-bsm.

1.1. Participants in organized markets administered by B3 must, within the scope of their responsibilities, identify, assess, understand and mitigate the risks of money laundering, terrorist financing and proliferation financing ("ML/TF"), pursuant to the applicable regulations, adopting a Risk-Based Approach ("RBA") to ensure that prevention and mitigation measures are proportionate to the identified risks and that regulatory requirements are duly observed.

1.2. Participants, their officers, employees and representatives must understand that terrorist financing and proliferation financing involve risks and characteristics that differ from those associated with money laundering and therefore require the establishment of rules, processes, controls and mechanisms for continuous and enhanced monitoring to ensure proper compliance with regulatory obligations.

A. AML/CFT Policy

1.3. Participants must implement and maintain rules, procedures and internal controls for monitoring purposes aimed at identifying indications of ML/TF. Such rules, procedures and controls shall be described in detail in the Participant's AML/CFT Policy ("Policy") or in other internal regulations specifically dedicated to AML/CFT matters and expressly referenced in the Policy.

1.4. The Policy must be approved by Senior Management and duly implemented and widely communicated to all employees of the institution, including, when applicable, its branches and subsidiaries, as well as disclosed to service providers, as appropriate.

1.5. The Participant must ensure that Investment Advisors[2] and other representatives associated with it are subject to its Policy, as well as to the AML/CFT-related rules, procedures and internal controls required under applicable regulations. The Participant shall be responsible for monitoring compliance with such guidelines by these professionals. In the case of a legal-entity Investment Advisor, the responsible officer designated under the applicable regulation must act in an auxiliary, coordinated and subsidiary manner to support the Participant in supervising compliance with such guidelines by the advisers associated with it.

1.6. Without prejudice to the provisions of the regulations in force, the Policy must include, at a minimum:

(i) a description of the RBA process, taking into account the minimum criteria set forth in Section C.1 of this Supervision Standard;

(ii) Know Your Customer, Know Your Employee and Know Your Relevant Service Provider processes and, when applicable, the Know Your Investment Advisor process, as described in Sections A.1 and A.2 of this Supervision Standard;

(iii) a description of the IRA, considering the provisions of Section D.1 of this Supervision Standard;

[2] In the case of a non-exclusive Investment Advisor, the Participant must ensure that the Investment Advisor is aware of and complies with the terms of both policies, as well as with any other applicable rules and regulations of each Participant to which the Investment Advisor provides services.

(iv) the information obtained through the verification of the investor's suitability profile, when applicable, and how such information is taken into account for purposes of the RBA and AML/CFT procedures. The Policy must also describe the monitoring conducted and the procedures adopted by the Participant in connection with client registration, the maintenance of registration information and contact with clients whose risk-profile assessment and classification are conducted without the completion of a specific questionnaire, as well as clients presenting circumstances that require differentiated treatment and may result in the requirement to complete the investor profile questionnaire in full. Non-exhaustive examples include:

a. significant contributions of funds by the client;

b. unusual financial results; and

c. abusive use of the client's express acknowledgment that their suitability profile is missing, outdated or inadequate;

(v) materiality, recurrence and cumulative historical criteria, among others, for the selection and control of alerts, if the Participant does not analyze all alerts in full;

(vi) the roles and responsibilities of the areas and departments responsible for AML/CFT matters, including the duties of Senior Management;

(vii) the systems used by the Participant for AML/CFT purposes;

(viii) the manner in which external data sources are consulted, including restrictive lists relating to economic sanctions, terrorist activities, proliferation financing and other financial crimes; search engines;

databases; and regulatory authorities, for the independent verification of adverse information;

(ix) procedures describing the methodology and frequency of monitoring restrictive lists, which must be reviewed by Participants on a recurring basis;

(x) the procedures adopted to comply with mandatory asset freezing and unavailability requirements arising from resolutions issued by the United Nations Security Council ("UNSC");

(xi) the procedures adopted for mandatory and continuous monitoring intended to track UNSC resolutions and identify assets, rights and funds held or owned by natural or legal person clients subject to sanctions arising from such resolutions. These procedures must indicate the area responsible for such identification and describe how reports are submitted to the Ministry of Justice and Public Security ("MJSP"), as well as to the CVM and COAF, as applicable;

(xii) the procedures adopted for the differentiated, continuous and enhanced monitoring of clients included on restrictive lists;

(xiii) the procedures adopted for monitoring and assessing the AML/CFT program by Internal Audit, when applicable, and External Audit, as well as by Internal Controls, Compliance, Risk Management or an equivalent department that is independent from the AML/CFT area;

(xiv) the processes used to address instances of noncompliance or deficiencies identified through testing of the AML/CFT program, as well as the manner in which such matters are reported to Senior Management;

(xv) the processes used to test the effectiveness of the AML/CFT program, including the frequency with which such tests are conducted and the area responsible for conducting them; and

(xvi) the processes used for the retention and maintenance of information and records relating to AML/CFT analyses, in accordance with the retention period established by the regulations in force.

1.7. A single Policy may be adopted by institutions belonging to the same financial conglomerate. In such cases, the Policy must identify the institutions within its scope, describe the particular features of each institution and establish mechanisms for the exchange of information among the responsible areas within the conglomerate.

1.8. The Policy must be periodically reviewed and, whenever necessary, updated to reflect regulatory changes and risk assessments. The version history of the Policy must be duly recorded and retained for the period established by the regulations in force, including an indication of the implementation period or the effective date of each updated version.

A.1 Know Your Customer Process

1.9. The Participant must maintain a Know Your Customer process establishing the rules, procedures and internal controls adopted to verify the identity of its clients, both at the time of initial registration and throughout the entire business relationship. The Know Your Customer process must also specify the conditions and

criteria clients are required to meet for the establishment and maintenance of the business relationship.

1.10. The Know Your Customer process must also include a description of:

(i) the detailed criteria for client risk classification, as well as the procedures for reviewing and updating such classification;

(ii) the criteria and frequency applicable to updates of client registration information, according to the client's risk classification;

(iii) the procedures for properly classifying the risk of clients structured as trusts and Politically Exposed Persons ("PEPs") with whom the Participant maintains a business relationship, including a proper description of the due diligence measures implemented for their appropriate monitoring;

(iv) the procedures for properly classifying the risk of Brazilian or foreign Non-Governmental Organizations ("NGOs") and nonprofit organizations with whom the Participant maintains a business relationship, including the proper identification of persons exercising influence within such organizations and a description of the due diligence measures implemented for their appropriate monitoring;

(v) measures adopted to comply with asset unavailability requirements imposed by sanctioning resolutions issued by the UNSC in relation to the Participant's clients; and

(vi) the due diligence measures adopted by the Participant to identify the beneficial owner, including in relation to Non-Resident Investors

("NRIs") or through custodians, as well as the treatment of situations in which the required registration information cannot be obtained, or the beneficial owner cannot be identified.

1.11. The Participant must assess whether to establish or maintain a business relationship with clients where the minimum due diligence requirements established by the regulations in force, its Policy, its IRA, or its other internal rules, procedures and controls have not been met. If the beneficial owner cannot be adequately identified or verified after the applicable due diligence measures have been carried out, the case must be submitted for formal assessment by the statutory officer responsible for compliance with the regulations in force governing AML/CFT matters ("Responsible Officer") or by the governance body established in the Participant's Policy.

1.12. In addition, the Policy must establish the risk classification, control measures and continuous and enhanced monitoring procedures applicable when the business relationship is maintained, including the criteria governing the Participant's acceptance and continued assumption of the relevant risk, notwithstanding the inability to adequately identify or verify the beneficial owner.

A.2 Know Your Employee, Know Your Relevant Service Provider and Know Your Investment Advisor Processes

1.13. The Policy must incorporate Know Your Employee processes, taking into consideration the ML/TF risks associated with the functions performed, the position

held by the employee and his or her professional background. The purpose of such processes is to verify whether the employee has any connection with financial crimes, money laundering or similar misconduct, in addition to considering other relevant information, depending on the complexity and business model of the Participant.

1.14. Likewise, the Policy must include a Know Your Relevant Service Provider[3] process in order to verify whether such service providers maintain AML/CFT policies and practices consistent with those adopted by the Participant itself, considering the activity performed, the ML/TF risk represented by such activity and the purpose of the relationship established with the contracted third party.

1.15. When applicable, the Participant must maintain a Know Your Investment Advisor process, highlighting the responsibility of the Investment Advisor's responsible officer in monitoring its activities and ensuring compliance with the Participant's applicable policies, rules, procedures and internal controls, pursuant to the regulations in force. In this regard, the Participant must ensure that appropriate due diligence procedures are conducted when onboarding a business partner, as well as full compliance with the applicable regulatory framework.

B. Senior Management and Responsible Officer

[3] Relevant services, pursuant to the regulations in force, are those related to critical business processes, which comprise: (i) order receipt and execution, with a view to ensuring continued client service; (ii) settlement with organized market operators; (iii) settlement of client transactions; (iv) reconciliation and updating of client positions; (v) alternative data sources and bureaus; and (vi) any other processes classified as critical by the Participant as part of its business impact analysis.

1.16. The Participant's Senior Management is responsible for demonstrating commitment, engagement, approval and the provision of adequate resources for the implementation of rules, processes and controls related to AML/CFT and the Internal Risk Assessment ("IRA"), as well as for the assessment, follow-up and monitoring of all AML/CFT-related matters, ensuring timely awareness of identified compliance risks.

1.17. In addition, Senior Management is responsible for appointing the Responsible Officer in charge of ensuring compliance with AML/CFT obligations. The appointment or replacement of such officer must be communicated to the CVM and, when applicable, to organized market administrators, financial market infrastructure entities and self-regulatory organizations with which the Participant maintains a relationship, within the deadline established by the applicable regulations.

1.18. The appointed Responsible Officer must ensure the implementation and maintenance of an AML/CFT Policy that is compatible with the Participant's nature, size, complexity, organizational structure, risk profile and business model, so as to ensure effective management of ML/TF risks. The Responsible Officer is also responsible for preparing the annual Internal Risk Assessment Report and evaluating, in the situations established by the regulations in force, whether it is appropriate to establish or maintain relationships with investors. In the performance of his or her duties, the Responsible Officer must act with integrity, good faith and professional ethics.

C. Risk-Based Approach (RBA)

1.19. The Participant must establish a Risk-Based Approach ("RBA") process employing a prevention methodology that is proportionate to the identified risks. The process must be designed to optimize the use of human resources, material resources and information, thereby enabling effective management of activities related to the identification, monitoring, analysis, understanding and mitigation of ML/TF risks.

1.20. The description of the Participant's RBA process must be included in the Policy or in other internal regulations specifically dedicated to AML/CFT matters and expressly referenced in the Policy.

C.1 Minimum Requirements

1.21. The Participant's RBA methodology must, at a minimum:

(i) be formalized in a written document;

(ii) contain an effective date;

(iii) describe the governance structure, including defined roles and responsibilities;

(iv) be approved by Senior Management; and

(v) describe:

a. how the Responsible Officer will have access to relevant AML/CFT information and controls;

b. the mechanisms for information exchange among responsible areas of Participants belonging to the same financial conglomerate, ensuring compliance with regulatory requirements;

c. the risk classification criteria for clients, products and services, their distribution channels and the trading and registration environments in which they operate, segmented at a minimum into low, medium and high risk;

d. the criteria and frequency for the reclassification of clients, products and services whenever changes in risk are identified, including as a result of monitoring activities and the annual IRA report;

e. the criteria for continuous and enhanced monitoring of clients and transactions, including enhanced monitoring in cases involving unidentified beneficial owners or incomplete client registration information;

f. the description of the measures adopted: (i) in response to unusual indicators identified through continuous monitoring; and (ii) in relation to situations that can be assessed based on complete information, such as relevant court decisions, convictions for ML/TF offenses involving clients and similar events;

g. the processes used to obtain and evaluate information relevant to client risk analysis, including information obtained from entities within the relationship chain and custodians, when applicable, as well as the criteria used to characterize such information as relevant;

h. the relationship between risk levels and the Participant's monitoring and response measures, demonstrating differentiated treatment according to each risk level; and
i. the integration of relevant risk-assessment information into the review and updating process.

1.22. The adopted RBA methodology must consider the elements analyzed in the Participant's IRA, so that the risks mapped in relation to clients and their respective relationship chains, as well as products offered, services provided, distribution channels and trading and registration environments, are appropriately mitigated through the application of the RBA methodology.

1.23. The Participant's Policy must establish the due diligence measures applicable to the adoption of the simplified registration model, including criteria enabling the assessment of the reliability of the foreign institution with which clients are registered, in order to ensure that appropriate investor identification, registration and beneficial ownership identification procedures are carried out in accordance with the legislation applicable in the institution's jurisdiction of origin.

1.24. For clients subject to simplified registration, the Participant must establish procedures in its Policy to verify that the foreign institutions with which such clients are registered are not located in jurisdictions classified by competent international organizations, particularly the Financial Action Task Force (FATF), as non-cooperative jurisdictions or jurisdictions with strategic deficiencies in AML/CFT matters and are

not subject to sanctions, restrictions or similar measures imposed by the United Nations Security Council (UNSC).

C.2 Risks

1.25. The Participant shall develop and implement its RBA methodology considering, at a minimum, the following criteria when classifying a client's risk: (i) jurisdiction; (ii) entities within the relationship chain; (iii) products and services, their respective distribution channels and trading and registration environments; and (iv) clients.

C.2.1 Jurisdiction Risk

1.26. As previously mentioned, the Participant shall assess ML/TF risk factors associated with the jurisdiction of origin and residence of its clients whenever sufficient information is available to enable such assessment. The Participant shall pay particular attention to jurisdictions presenting, among others, the following characteristics:

(i) subject to sanctions or similar measures issued by international organizations, such as the United Nations ("UN");

(ii) jurisdictions that do not apply, or insufficiently apply, the recommendations issued by the Financial Action Task Force ("FATF"), as identified through FATF restrictive lists;

(iii) jurisdictions that provide favorable tax treatment or are subject to privileged tax regimes, pursuant to rules issued by the Brazilian Federal Revenue Service; and

(iv) border regions.

C.2.2 Relationship Chain Entity Risk

1.27. The Participant shall consider the characteristics of the entities involved in the relationship chain leading to the client and shall observe entities acting on behalf of the client from order origination through execution by the Participant, including, for example, asset managers, custodians and fiduciary administrators.

1.28. The Participant shall make and document reasonable efforts to identify the client represented by entities forming part of the relationship chain, exercising enhanced due diligence whenever such entities:

(i) do not perform ML/TF risk controls or maintain controls below the standards expected under Brazilian AML/CFT regulations;

(ii) are classified as presenting higher ML/TF risk without satisfactory mitigating measures or whose control environment cannot be properly assessed by the Participant based on available information;

(iii) are subject to investigations or have criminal convictions, particularly those related to financial crimes, when applicable;

(iv) are located in higher-risk jurisdictions or jurisdictions with less robust AML/CFT frameworks;

(v) have a history of unremediated violations of securities market regulations or have been cited by reliable information sources for AML/CFT-related deficiencies; and

(vi) refuse to cooperate in sharing information. In such cases, unjustified refusal shall be regarded as presenting a higher level of risk than situations in which the Participant accepts the justification presented.

C.2.3 Product or Service Risk

1.29. Participants may offer products and services through different distribution channels and within different trading and registration environments. The RBA shall consider the risks associated with each product or service offered, classifying them, at a minimum, as low, medium or high risk. Furthermore, it is essential to evaluate how the method of distribution or the nature of the product or service may create potential vulnerabilities to ML/TF practices.

1.30. The following non-exhaustive risks related to products and services should be considered:

(i) the geographic reach of the product or service, including products whose underlying assets are traded in higher-risk jurisdictions;

(ii) products with unusual complexity or structures lacking an apparent economic rationale; and

(iii) products or services that facilitate the transfer of funds through simulated or artificial transactions in the securities market, for example, due to the

trading or registration environment in which transactions occur, or as a result of characteristics such as the liquidity of the underlying asset.

C.2.4 Client Risk

1.31. The Participant shall evaluate risks associated with the client, taking into account factors such as occupation or business sector, products and services used, address and securities market transactions conducted on the client's behalf. Additionally, continuous monitoring of such information and other relevant data is essential, including changes in the Brazilian National Classification of Economic Activities (CNAE) applicable to legal entity clients.

1.32. The Participant's RBA methodology shall address the risk treatment applicable, among others, to clients presenting the following characteristics:

(i) classification as a PEP, family member of a PEP, close associate of a PEP or legal entity controlled by a PEP;

(ii) classification as a nonprofit organization;

(iii) corporate structures lacking economic rationale, whose complexity cannot be justified by apparent benefits;

(iv) economic activities conducted by non-financial legal entities, particularly those involving the export, commercialization or provision of services related to sensitive goods or directly related services as referred to in Law No. 9,112/1995, including, but not limited to:

a. dual-use goods;

b. goods used in nuclear, chemical and biological sectors;

c. goods and services that wholly or partially contribute to the development, production or use of weapons of mass destruction; and

d. delivery systems, including missiles capable of carrying weapons of mass destruction;

(v) the existence of a representative or attorney-in-fact who unjustifiably refuses to provide client information, alleges a contractual or legal impediment that is inapplicable, or provides information deemed inconsistent by the Participant;

(vi) sanctions imposed on the client by domestic or international authorities related to ML/TF or authorities responsible for supervising securities market activities, with the Participant being permitted to consider the existence of consent decrees or similar settlement arrangements;

(vii) references to the client in reliable news sources concerning ML/TF or financial crimes, or indicating that the client has:

a. committed, attempted to commit, participated in or facilitated terrorist acts; or

b. engaged in activities potentially associated with terrorist financing or proliferation financing, as provided in Law No. 13,260/2016;

(viii) references to the client as a suspect in reports concerning ML/TF or financial crimes issued by competent domestic or international authorities;

(ix) activities conducted by the client in jurisdictions deemed non-cooperative according to FATF reports and those of other competent bodies, such as the Office of Foreign Assets Control ("OFAC"), when applicable;

(x) clients whose place of origin or residence is connected with jurisdictions listed in Section C.2.1 of this Supervision Standard;

(xi) transactions involving securities subject to sanctions imposed pursuant to UNSC resolutions referred to in Law No. 13,810/2019;

(xii) securities owned or controlled, directly or indirectly, by a client who has committed, attempted to commit, participated in or facilitated terrorist acts, as provided in Law No. 13,260/2016; and

(xiii) requests submitted to the Participant for the transfer of funds or securities to accounts located in higher-risk jurisdictions or lacking an economic rationale that would justify the transaction.

1.33. For clients classified under the Participant's Policy as blocked from opening new positions, while remaining active within B3's infrastructure, an appropriate risk classification in accordance with the RBA guidelines remains mandatory.

1.34. Additionally, the Participant shall determine whether the client qualifies as a PEP and implement any additional control measures required in view of the risks associated with that category. The Participant may use external data providers, including bureaus, for PEP classification purposes, provided that consultation and assessment of all individuals included in official public databases, including the lists made available through SISCOAF[4], remain mandatory. For classification and

[4] SISCOAF is a restricted-access virtual environment intended exclusively for individuals and legal entities specified under Law No. 9,613, of March 3, 1998. A public version of the PEP list is made available by the Brazilian Office of the Comptroller General ("CGU") through the Transparency Portal (available at: https://portaldatransparencia.gov.br/download-de-dados/pep). However, it should be noted that the public database does not disclose the taxpayer identification number (CPF) of the individuals listed, which may hinder effective monitoring by the Participant. This limitation may pose

monitoring purposes, the Participant shall also observe the retention period applicable to PEP status as established by the regulations in force, counted from the date on which the circumstance that gave rise to the classification ceases to exist.

1.35. The Access Registration regime does not exempt the Participant from the obligation to assign a risk classification to its clients, which should not be confused with the investor suitability classification required under applicable regulations. The Participant shall classify and continuously reclassify clients, ensuring that any change in the client's circumstances or behavior is appropriately reflected in its risk rating.

1.36. With respect to risk reclassification, the Participant shall retain evidence demonstrating that all criteria established in the documents comprising its RBA framework were considered for every client whose risk classification was revised.

C.3 Financial Capacity and Assets Monitoring

1.37. The Participant shall implement mechanisms to address situations in which it is not possible to obtain client registration information, particularly with respect to clients' qualifications and financial capacity or net worth. For this purpose, the Participant may rely on supplementary information capable of supporting inferences regarding a client's financial capacity, provided that such information is effective and aligned with the methodology adopted under its Know Your Customer process.

---

an additional challenge in identifying and managing risks associated with clients who fall within this category.

1.38. The following are non-exhaustive examples of supplementary information that may be used, as applicable, to assess a client's financial capacity:

(i) for natural persons, updated information regarding income and net worth;

(ii) for legal entities, except legal entities whose securities are admitted to trading on organized markets, updated information regarding average monthly revenue over the preceding twelve (12) months and the entity's financial position;

(iii) for investment funds registered with the CVM and other applicable situations, updated information regarding financial capacity and net worth;

(iv) value of the client's managed portfolio;

(v) publicly available financial statements and revenue information;

(vi) information available through databases accessible to the Participant;

(vii) transaction volume based on the client's historical activity during the relationship period; and

(viii) the monitoring threshold assigned to the client pursuant to the Policy or equivalent internal regulation.

C.4 Monitoring and risk classification of Non-Resident Investors

1.39. Considering the specific monitoring requirements applicable to Non-Resident Investors ("NRIs"), the Participant shall specify in its Policy the additional

criteria used to assess their transactions and unusual situations, irrespective of the risk classification assigned to such clients.

1.40. If the Participant does not have access to all information required under Brazilian regulations, including information relating to simplified registration procedures applicable to NRIs, the Participant may take into account the RBA applied by entities within the relationship chain associated with the NRI, including information and controls maintained by custodians and foreign institutions, when applicable, together with the continuous monitoring of the NRI throughout the business relationship.

1.41. If the NRI is an investment fund or similar investment vehicle managed by a foreign portfolio manager and the Participant does not have access to all NRI information, the Participant may consider the RBA adopted by the manager or equivalent entity in its home jurisdiction as a basis for the NRI risk assessment.

1.42. Monitoring performed by the Participant shall focus on securities transactions executed on behalf of the individual NRI rather than on transactions undertaken by the foreign manager.

1.43. The Participant shall be familiar with the risk methodology adopted by the foreign institution to classify the entities within the relationship chain, including custodians, through to the NRI. Any entity providing securities-related services between the issuance of an order by or on behalf of the NRI and its execution by the Participant shall be deemed part of the relationship chain. The Participant shall

consider any known events indicating significant ML/TF red flags involving any entity in such chain.

1.44. Accordingly, the Participant may adopt the risk classification assigned to an NRI by a foreign institution or another entity within the relationship chain, provided that it: understands the RBA methodology used by such institution or entity and confirms that the methodology is consistent with its own RBA methodology. In such cases:

(i) if the RBA methodology of the foreign institution or entity within the relationship chain does not fully satisfy the minimum requirements established under Brazilian regulations, the foreign Participant and the custodian shall supplement the assessment and obtain the missing information;

(ii) the Participant shall evaluate the risks arising from reliance on the RBA methodology of the foreign institution or entity within the relationship chain when such methodology is not consistent with the requirements established under Brazilian regulations; and

(iii) the Participant shall demonstrate that its Know Your Customer procedures were performed in accordance with the adopted risk classification, without prejudice to its obligation to monitor all transactions intermediated on behalf of the NRI in the Brazilian securities market.

1.45. When the Participant determines that an NRI's manager or representative presents a heightened ML/TF risk, the represented NRI's risk assessment shall be

influenced by such higher-risk designation, unless a documented rationale supports a different conclusion. Likewise, a higher-risk classification assigned to one NRI shall not automatically affect other NRIs represented by the same manager unless there is evidence of collaboration in the unusual conduct identified.

D. Internal Risk Assessment (IRA)

1.46. The Participant shall prepare and formalize, in writing, an Internal Risk Assessment ("IRA") for the purpose of understanding its risk appetite and identifying factors that may increase or reduce the likelihood of ML/TF events. For this purpose, the Participant shall consider its size, transaction volume, complexity and business activities in order to better understand and classify the risks associated with its operations.

1.47. The IRA shall encompass, at a minimum, the following risk categories:

(i) client risk profile;

(ii) products and services risk profile;

(iii) distribution channels and trading and registration environments risk profile; and

(iv) risk profile associated with the institution's relationship with other persons subject to AML/CFT regulations.

1.48. Each category shall be classified into at least three risk levels: low risk; medium risk; and high risk. The IRA shall also describe the characteristics supporting each assigned risk profile and classification.

D.1 Internal Risk Assessment Report (IRAR)

1.49. The Participant shall prepare an Internal Risk Assessment Report ("IRAR"), which shall be submitted to the governing bodies designated in the Policy no later than the last business day of April of each year.

1.50. The Participant shall maintain evidence demonstrating submission of the IRAR to Senior Management through, for example: (i) minutes of a dated meeting confirming awareness of the IRAR and signed by all members; or (ii) another supporting document, such as an e-mail, evidencing delivery of the IRAR to all members. The IRAR must remain available for submission to regulators or to BSM upon request.

1.51. Relevant information to be included in the IRAR includes:

(i) the frequency with which clients classified as PEPs or nonprofit organizations are identified and validated;
(ii) risk ratings assigned to all clients;
(iii) the existence of trust structures, when applicable, and a description of the due diligence procedures used to identify trust parties and beneficial owners; and

(iv) the existence of exclusive funds[5], whether in Brazil or abroad, or corporations, when applicable, together with a description of the due diligence procedures used to identify their beneficial owners.

1.52. The Participant shall expressly document in the IRAR any item required under regulation or this Supervision Standard that is deemed not applicable.

1.53. The IRAR shall: specify the parameters used to identify, analyze, understand and classify risks; demonstrate that the samples tested are statistically significant and representative; reference the methodology and criteria used for sample selection, testing frequency and the tests performed; and identify the document, including its name and version, in which such information is described.

1.54. The IRAR shall separately identify actions adopted to implement specific due diligence measures aimed at preventing: (i) money laundering; (ii) terrorist financing; and (iii) proliferation financing. The IRAR shall also describe the results produced by effectiveness indicators, as per item D.2 below, and, when appropriate, propose enhancements to address the principal risks identified.

1.55. The Participant shall retain all effectiveness testing supporting the IRAR, including testing procedures, databases used and results obtained, and such records

[5] Pursuant to the regulations in force, exclusive funds are those that receive funds, directly or indirectly, from a single professional investor, from quota holders linked by family and corporate relationships, or from quota holders linked by a single and inseparable interest.

shall be available to BSM for the retention period required under applicable regulations.

D.2 Effectiveness Indicators

1.56. Effectiveness indicators are intended to assess the effectiveness of the Participant's rules, procedures and internal controls, as well as its ability to mitigate ML/TF risks in accordance with its business model. The assessment of effectiveness enables the Participant to identify control deficiencies; evaluate the adequacy of risk mitigation strategies; and assess the efficiency of implemented processes.

1.57. The Participant shall implement enhancements identified through effectiveness assessments by means of action plans. Senior Management shall be committed to the results of such assessments and to the follow-up of any resulting action plans, including providing resources and supporting process improvements.

1.58. The analysis of effectiveness indicators shall be carried out on an ongoing basis and documented within the IRAR[6] in order to promote continuous enhancement of the Policy and the Participant's rules, procedures and internal controls.

1.59. The Participant shall establish in its Policy the effectiveness indicators that will be used. In cases where a single RBA methodology applies across entities within the

[6] For further information, please refer to the RAIR Guide available at: https://www.bsmsupervisao.com.br/materiais-de-apoio?section=guia-bsm.

same financial conglomerate, as per item 1.21 above, the Policy shall specify the applicable effectiveness indicators.

1.60. Effectiveness indicators presented in the IRAR shall include: metrics and criteria adopted for effectiveness assessments; timeliness of detection, analysis and reporting activities relating to unusual transactions or situations. It is recommended that the results of the indicators be presented using statistical values, together with a conclusion regarding effectiveness and trends over time, in accordance with the methodology established by the Participant in its Policy.

1.61. With respect to relevant service providers, the Participant shall assess whether such providers maintain AML/CFT policies and practices compatible with those adopted by the Participant itself, considering the activity performed, the associated ML/TF risk and the purpose of the relationship established with the third party, with a view to ensuring high standards within its framework.

E. Monitoring, analysis and reporting of atypical situations

E.1 Analysis of atypical situations

1.62. The Participant shall implement monitoring controls covering all offerings and transactions, capable of identifying and preventing violations related to AML/CFT.

1.63. The table below provides a non-exhaustive list of situations that will be subject to BSM supervision.

SITUATION	BSM SUPERVISION
a) Situations in which client registration information cannot be kept up to date.	(i) Clients who refuse to keep their registration information up to date in accordance with the minimum requirements established by applicable regulations; and (ii) Clients whose registration information is outdated and who cannot be contacted by the Participant for updating purposes.
b) Situations in which the beneficial owner cannot be identified.	In cases where the minimum monitoring procedures include ongoing due diligence related to the Know Your Customer process, and such due diligence cannot be completed, the Participant shall include the following in its monitoring activities: (i) Non-Resident Investors ("NRIs"), particularly those structured as trusts or similar vehicles, exclusive funds, whether domestic or foreign, and corporations; (ii) Domestic and foreign nonprofit organizations; (iii) Restrictive-list screening; (iv) Exclusive investment funds; and (v) Politically Exposed Persons ("PEPs").
c) Situations in which the due diligence required under the Know Your Customer process cannot be completed.	The Participant's monitoring shall include: (i) NRIs, particularly those established as trusts; (ii) Nonprofit organizations; (iii) Restrictive-list screening; (iv) Exclusive investment funds; and (v) PEPs.

SITUATION	BSM SUPERVISION
d) Natural person clients whose transactions involve amounts objectively incompatible with the professional occupation, income and/or financial condition or net worth of any party involved, based on registration information.	The Participant's monitoring shall consider: (i) Cash movements (deposits, withdrawals or deposits only) incompatible with the income and/or financial condition and net worth declared by the client; (ii) Transactions incompatible with the income and/or financial condition and net worth declared by the client, considering either individual transaction amounts or transaction results; and (iii) Custody-position transfers (incoming, outgoing or incoming-only asset transfers) incompatible with the client's declared income and/or financial condition and net worth.
e) Legal entity clients whose economic activity, corporate purpose or reported revenue is inconsistent with the operational profile normally exhibited by clients with a similar profile.	The Participant's monitoring shall consider: (i) Transactions incompatible with the revenue and/or financial condition and net worth declared by the client; (ii) Cash movements incompatible with the revenue and/or financial condition and net worth declared by the client; (iii) Custody-position transfers incompatible with the revenue and/or financial condition and net worth declared by the client; (iv) Changes in CNAE classification; (v) Trading of sensitive goods and provision of directly related services referred to in Law No. 9,112, including technologies, software and dual-use goods; and (vi) Connections with high-risk jurisdictions.
f) Transactions conducted between the same parties or for the benefit of the same parties in which one of the parties repeatedly realizes gains or losses.	The Participant's monitoring shall consider: (i) Transactions accumulated over a period that present recurring counterparties; and (ii) The assessment of gains or losses arising from recurring transactions.

SITUATION	BSM SUPERVISION
g) Transactions demonstrating significant fluctuations in transaction volume and/or frequency relative to the historical profile of any of the parties involved.	The Participant's monitoring shall consider: (i) Significant variations in monthly transaction volume compared with the client's transaction history; and (ii) Significant variations in monthly trading volume or in the number of derivative contracts traded compared with the client's transaction history.
h) Transactions whose characteristics may constitute mechanisms intended to conceal the identity of the actual parties and/or beneficiaries involved.	The Participant's monitoring shall consider the effective identification of the parties and/or beneficiaries involved in the transactions. Such monitoring may be conducted through continuous due diligence performed under the client-identification process.
i) Transactions evidencing a sudden and objectively unjustified change in relation to the operational modalities normally used by the client.	The Participant's monitoring shall consider changes in products traded by the client when compared with products previously traded by the same client, based on the client's transaction history.
j) Transactions whose degree of complexity and risk appears incompatible with the client's profile or the profile of its representative, as well as with the client's size and corporate purpose.	The Participant's monitoring shall consider: (i) The suitability process. Monitoring shall include clients subject to suitability requirements who have no defined investment profile, have an outdated profile, or have carried out transactions incompatible with their profile; and (ii) Transactions incompatible with the client's size and corporate purpose.
k) Transactions intended to generate gains or losses that objectively lack an economic or legal rationale.	The Participant's monitoring shall consider transactions lacking an economic or legal rationale in the capital markets, including, for example: transfers of funds between clients (money pass arrangements), exercise of out-of-the-money options, purchases of securities at off-market prices, transactions designed to obtain tax benefits, among others.

SITUATION	BSM SUPERVISION
l) Transfers of funds or securities without an apparent rationale.	The Participant's monitoring shall consider: (i) Whether transfers of securities between different holders are supported by the documentation required by the Participant or by a declared rationale; (ii) Whether custody-position transfers are incompatible with the income and/or financial condition and net worth declared by the client; (iii) Whether the transfer occurs between registration accounts maintained by the Participant; (iv) Whether the transfer occurs outside an organized market environment; and (v) Whether cash movements are unrelated to transaction settlement or do not result from services provided by the Participant to the client.
m) Deposits or transfers made by third parties for the settlement of client transactions or for the provision of collateral in futures-market transactions.	The Participant's monitoring shall consider: (i) Entries in client registration accounts; and (ii) Bank reconciliations.
n) Payments made to third parties, in any form, in connection with transaction settlements or withdrawals of assets pledged as collateral and registered in the client's name.	The Participant's monitoring shall consider: (i) Entries in client registration accounts; and (ii) Bank reconciliations.
o) Transactions executed at prices outside prevailing market prices.	The Participant's monitoring shall consider significant price movements in securities (largest price increases or decreases during the period) caused by its clients.

SITUATION	BSM SUPERVISION
p) Transactions and situations involving persons suspected of involvement in terrorist acts, or transactions involving natural persons, legal entities or other entities residing, established or incorporated in countries, jurisdictions, dependencies or locations referred to in Section 1.26 of this Supervision Standard.	At a minimum, the Participant shall verify whether clients: (i) Are subject to sanctions imposed by UNSC resolutions; (ii) Are subject to asset-freezing requests issued by a foreign central authority; (iii) Reside in or originate from jurisdictions that do not apply, or insufficiently apply, FATF recommendations; (iv) May be associated with terrorist acts or terrorist financing activities; (v) Reside in or originate from jurisdictions offering favorable tax treatment or privileged tax regimes; and (vi) Reside in or originate from locations classified as border regions.

1.64. In addition to the examples set forth in the table above, Participants shall monitor their clients' access and trading patterns through audit trails containing records of order origin, in accordance with the BSM File Layout and Audit Trail Manual[7], as well as access and/or registration records. Such monitoring shall, at a minimum, consider risk scenarios based on the risk profile and operating model established in the Policy. Based on such monitoring, the Participant shall assess cases in which the origin of the order, including the user's IP address, geolocation and/or other mechanisms capable of identifying its geographic origin, is inconsistent with the client's usual access pattern.

E.2 Alert analysis

[7] Available at: https://www.bsmsupervisao.com.br/materiais-de-apoio?section=manuais-bsm

1.65. The Participant shall implement a regular and continuous monitoring procedure covering all transactions under its responsibility in order to identify unusual situations that may potentially involve ML/TF activities. Such procedure shall include the establishment of objective criteria, defined in the Policy, for the detection of anomalies in client transactions and activities. The procedure shall also include the use of monitoring tools and systems capable of generating alerts whenever activities deviating from normal patterns are detected.

1.66. The Participant shall establish, in its Policy, protocols for the analysis of such alerts, ensuring that each situation is properly assessed by qualified professionals. During the alert review process, the Participant shall examine information regarding the identified transactions, including their origin, destination, value and context, in order to confirm or rule out the possibility of ML/TF practices.

1.67. The analysis of alerts generated through the Participant's monitoring activities shall be deemed effective when it includes, at a minimum and without limitation:

(i) information related to the unusual transaction or situation scenario established under applicable regulations, together with information clarifying the identified alert;

(ii) an assessment of the dynamics and purpose of the transactions, as well as the client's operating model in relation to the transactions that originated the alert;

(iii) a documented conclusion regarding the analysis performed; and

(iv) the action or measure to be adopted by the Participant.

1.68. Alerts generated through monitoring activities may be dismissed, provided that such decision: is formally justified; is supported by a written methodology containing clear and objective criteria; and is properly documented in the Policy. Alerts shall not be dismissed solely on the basis of the client's risk classification.

1.69. The analysis of each alert shall be concluded within the timeframes established by applicable regulations. The methodology used to calculate such timeframe, including its triggering event, shall be clearly described in the Policy.

1.70. The Participant shall prioritize the quality of unusual situation monitoring through continuous staff training and the use of appropriate technologies for alert analysis. Monitoring quality shall not be measured solely by the number of generated alerts or reports filed, but rather by the effectiveness of the alerts produced and the quality of the analyses and reports prepared.

1.71. The Participant shall adopt a sampling methodology that ensures a qualitative and representative review of the assessed processes, so that the selected sample population is sufficiently comprehensive to support meaningful conclusions and is aligned with the methodology described in the Policy.

E.3 Reporting obligation

1.72. When assessing potential unusual situations, it is essential that the Participant distinguish situations raising suspicion of ML/TF from situations involving other potential unlawful activities defined under applicable laws and regulations, which shall be reported to the CVM, BSM and other competent authorities, as appropriate.

1.73. Indications of ML/TF activities shall be reported by the Participant to the Brazilian Financial Intelligence Unit ("COAF"). The identification of such indications shall result from the analysis conducted by the Participant in accordance with the criteria, methodology and procedures established in its Policy and under applicable regulations.

1.74. During the monitoring and reporting process relating to ML/TF indicators, the Participant shall assess whether the analyses submitted to COAF should also be reported to BSM. Making such information available contributes to self-regulatory activities by providing relevant inputs for Risk-Based Supervision ("RBS") initiatives.

1.75. Reports shall identify the unusual situations detected, including a detailed description of the facts and grounds supporting the Participant's assessment regarding the existence of ML/TF indicators. Such reports shall be accompanied by complete supporting documentation substantiating the findings and indicators reported, including: a description of the methodology used to identify the unusual situation; documentation obtained during the investigation conducted by the Participant; and whenever possible, the date and time at which the information was collected or captured.

1.76. Reports to COAF shall be submitted within the timeframe established by applicable regulations following completion of the Participant's analysis, whenever the unusual situations identified cannot be satisfactorily justified.

1.77. The Participant shall maintain records of all reports submitted to COAF, including reports regarding the absence of transactions or proposed transactions requiring reporting ("NIL Report").

1.78. Reports to COAF shall be submitted through the SISCOAF system using the segment designated as "CVM – Securities Market". Access management and authorization procedures relating to such information shall observe, at a minimum, the following requirements:

(i) access credentials shall be individual and shall not be shared;

(ii) access shall be protected by password or an equivalent security mechanism;

(iii) access shall be restricted to professionals acting on behalf of the Participant, with access levels compatible with their respective duties and structured so as to avoid conflicts of interest. The Participant shall establish, in advance, the criteria governing access permissions and identify activities that, if cumulatively performed by the same individual, could create conflicts of interest;

(iv) the technical qualifications of each user shall be assessed in relation to the access granted;

(v) immediate access revocation procedures shall be implemented whenever a professional ceases to work for the Participant; and

(vi) access to SISCOAF shall be monitored, controlled and logged and shall be strictly limited to the extent necessary for regulatory compliance purposes.

E.4 Monitoring of restrictive lists

1.79. The Participant shall directly and continuously monitor restrictive lists related to economic sanctions, terrorist activities, proliferation financing and other financial crimes.

1.80. The Participant shall adopt the necessary due diligence measures to ensure the immediate adjustment of its rules, processes and controls whenever such lists are updated, without prejudice to any additional measures that may be required in relation to clients identified therein. With respect to the restrictive list published by the United Nations Security Council ("UNSC"), the Participant shall additionally comply with the provisions of Law No. 13,810/2019, especially regarding the freezing and unavailability of assets belonging to persons designated under such sanctions lists.

1.81. Furthermore, within the scope of its responsibilities, the Participant shall adopt enhanced due diligence measures for transactions or situations involving Non-Resident Investors ("NRIs") who reside in, are incorporated in, have their registered office in, or are otherwise connected to countries, jurisdictions,

dependencies or locations that do not apply, or insufficiently apply, the recommendations issued by the Financial Action Task Force ("FATF"), as identified in FATF publications. The same enhanced measures shall be considered whenever the risk arises, directly or indirectly, from: the ownership structure; the control chain; beneficial owners; representatives; or other circumstances identified by the Participant as presenting heightened risk under its Risk-Based Approach ("RBA") methodology. In such situations, continuous and enhanced monitoring shall apply through the implementation of more rigorous procedures for the selection of unusual transactions or situations, regardless of the risk classification assigned to the investor, pursuant to the regulations in force.

Enhanced due diligence measures shall include, at a minimum:

(i) restrictions or additional conditions for establishing business relationships;

(ii) limitations, postponements or refusals regarding transactions involving assets classified as higher risk;

(iii) requests for additional information or supporting documentation; and

(iv) termination of the business relationship whenever risks are determined to be unacceptable and incapable of being effectively mitigated.

1.82. All procedures relating to restrictive-list monitoring shall be documented in the Policy, including identification of the professionals and business areas responsible for monitoring activities and for ensuring the effective blocking of accounts whenever a client is identified on any restrictive list.

F. Training and capacity building

1.83. The Participant shall maintain a team possessing sufficient technical qualifications and appropriate staffing levels, considering its business model, to conduct ML/TF monitoring and analysis activities.

1.84. The Participant shall maintain documented training and capacity-building processes for employees, Investment Advisors and Relevant Service Providers ("Training"). Such Training shall be effective and delivered using clear and accessible language, taking into account the functions performed and the level of risk associated with the relevant activities, as identified through the Participant's Internal Risk Assessment.

1.85. Training shall be conducted according to the minimum frequency established by the Participant in its Policy and whenever internal rules, procedures or applicable regulations are updated.

G. Documentation and evidence

1.86. Documentation and evidence relating to compliance with the obligations established under this Supervision Standard shall be retained by the Participant for the period and under the conditions required by the applicable regulations.

II. BSM Supervision

2.1. BSM's supervision and oversight activities regarding the obligations established in this Supervision Standard are conducted on an ongoing basis through audits and other supervisory and inspection activities intended to verify a Participant's compliance with the applicable rules.

2.2. During its supervision and inspection activities relating to AML/CFT matters, BSM assesses, among other things:

(i) the rules, procedures and internal controls implemented by Participants to identify and prevent ML/TF-related misconduct;

(ii) the appointment of a Responsible Officer;

(iii) the existence of a Policy approved by Senior Management expressly describing the rules, procedures and internal controls for monitoring activities aimed at identifying indications of ML/TF;

(iv) the existence of a documented, up-to-date and Senior Management-approved RBA methodology, including an effective date and all elements required by applicable regulations, and:

a. adequate risk-classification criteria for clients, products and services, distribution channels, trading environments and registration environments; risk reclassification procedures consistent with the Participant's Policy; monitoring procedures associated with such classifications;

b. rules, processes and controls applicable to trusts, NGOs, nonprofit organizations, PEPs and persons identified through restrictive-list screening;

c. compliance with risk-reclassification criteria and periodic reviews established under the RBA framework; and

d. appropriate identification and monitoring of clients classified as PEPs or nonprofit organizations, including reviews associated with electoral cycles and updates to the official PEP lists published by the Office of the Comptroller General ("CGU").

(v) preparation of a properly documented IRA, and:

a. preparation and timely submission of the Internal Risk Assessment Report ("IRAR") to Senior Management;

b. inclusion of all mandatory contents established by regulations and this Supervision Standard;

c. effectiveness tests and indicators applied by the Participant;

d. sample-selection criteria and supporting statistical analyses; and

e. presentation of effectiveness results using statistical metrics.

(vi) the number of AML/CFT alerts generated during the review period; whether all alerts were analyzed within the regulatory deadlines; and the number of reports submitted to competent regulatory and self-regulatory authorities;

(vii) whether the Participant reassesses the parameters of its AML/CFT monitoring systems, the assumptions used for such reassessment, the frequency with which it is performed, and whether these processes are described in the Policy;

(viii) whether the Participant applies objective criteria, taking into account its clients' operating models and history of atypical activity, to define, calibrate and reassess the parameters used to monitor the offerings, transactions and atypical situations set forth in the regulations in force, as well as the frequency with which such reassessment is performed;

(ix) the procedures established in the Policy for reporting unusual situations to competent authorities;

(x) the structure of the Participant's AML/CFT function, including staffing levels, professional qualifications, analytical processes and alert volumes; and

(xi) the implementation of AML/CFT Training programs for employees, Investment Advisors and Relevant Service Providers, including whether training materials adequately and distinctly address: (i) money laundering; (ii) terrorist financing; and (iii) proliferation financing.

III. *Enforcement*

3.1. Participants that fail to comply with the obligations established under applicable regulations and this Supervision Standard shall be subject to Enforcement measures pursuant to the provisions of the BSM Procedural Rules.

This Supervision Standard shall become effective on November 3, 2026, revoking BSM Supervision Standard No. 18/2025, originally published on October 9, 2025.

Additional information may be obtained by calling +55 (11) 2565-6200 (option 1) or by e-mail at bsm@bsmsupervisao.com.br.

Fátima Guerra

Acting Director of Self-Regulation