

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

Supplier Management Procedure (KYP/KYS)

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	2
2. Scope	2
3. Terms and Definitions	3
4. Procedure	4
4.1 Overview of the flow	4
4.2 Request and risk classification	4
4.3 Prior due diligence	5
4.4 Cloud service providers	5
4.5 Contracting	6
4.6 Monitoring	7
4.7 Supplier-related incidents	7
4.8 Measures resulting from the assessment	8
4.9 Termination and exit strategy	8
4.10 Conflict of interest	8
4.11 Waivers	8
5. Review	9
6. Reference Standards	9
7. Effectiveness	10
8. Version Control and History	10

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

1. Purpose

This Procedure sets out the step-by-step operational process for managing suppliers, business partners and third parties, including cloud service providers, detailing the stages, responsible parties and control points applicable to the selection, assessment, contracting, monitoring and termination of the relationship.

This Procedure implements the guidelines on knowing partners and outsourced service providers established in the AML Policy, to which it remains subordinate, and fulfills the duty to implement procedures to know partners and outsourced service providers, including identification and qualification, set out in article 56 of BCB Circular No. 3,978/2020, as well as the measures for knowing business partners and outsourced service providers required by article 47 of BCB Resolution No. 520/2025. In the event of any inconsistency, the Policy prevails.

2. Scope

This Procedure applies to all employees, third parties and other professionals involved in the selection, assessment, contracting, management, monitoring and termination of relationships with the Organization's suppliers, including those responsible for technology services, cloud computing and other services that may affect the Organization's information security, privacy, business continuity, compliance or processes.

The following are outside the scope of this Procedure: knowing candidates and individual employees, and the due diligence of clients and of counterparties that are virtual asset service providers, which are addressed in the corresponding procedures.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

3. Terms and Definitions

Term	Definition
KYP (Know Your Partner)	Process of identifying, verifying and assessing business partners, with the aim of identifying and managing the risks associated with the relationship with the Organization.
KYS (Know Your Supplier)	Process of identifying, verifying and assessing suppliers, with the aim of identifying and managing the risks associated with contracting and with the relationship with the Organization.
Supplier	Individual or legal entity that supplies products or provides services to the Organization.
Business Partner	Individual or legal entity that maintains a commercial or strategic relationship with the Organization for the development of activities, business or objectives of common interest.
Due Diligence	Process of verifying and analyzing information and evidence relating to the supplier or business partner, carried out to identify and assess the risks associated with the relationship.
Risk Classification	Categorization assigned to the supplier or business partner based on the risks identified and on the criteria established by the Organization.
Enhanced Due Diligence	Application of additional checks by reason of the level of risk, the characteristics of the relationship or situations identified during the assessment.
Exit Strategy	Set of planned measures to ensure the continuity of services and the protection of information upon the discontinuation of a critical supplier or cloud service provider.
KYP Form	Standardized form for collecting information on the supplier or business partner, its partners, officers and ultimate beneficial owners, completed in the mandatory assessment cases set out in Section 4.3.
Background Check	Verification of the background of the supplier or business partner, its partners, officers and ultimate beneficial owners, covering corporate and litigation searches, restrictive and sanctions lists, PEP databases and public reputation sources.
Waiver	Exceptional, reasoned and temporary exemption from a requirement set out in this Procedure.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

4. Procedure

4.1 Overview of the flow

The supplier life cycle comprises six blocks: (i) request and classification; (ii) prior due diligence; (iii) contracting; (iv) granting of access and designation of the responsible person; (v) monitoring and handling of incidents and non-conformities; and (vi) termination. The depth of each block is proportional to the risk classification assigned.

4.2 Request and risk classification

Step	Activity
1	Record the contracting request in the supplier analysis request form, with the justification of need and the business requirements applicable to the service.
2	Classify the supplier as Critical, High, Medium or Low, considering: size; nature and criticality of the services; transaction volume; sensitivity of the information accessed, stored or processed; level of access granted; impact on business continuity; legal, regulatory and contractual requirements; existence of subcontracting; and the AML nature of the supplier, where applicable to the regulated activities.
3	Waive the supplier assessment when contracting a specific, one-off product or service with no recurring payment, no access to the Organization's information, systems or environments and no impact on business continuity, such as the supply of stationery and office materials, clothing, and venue booking or event services, upon recording the justification for the classification. The waiver does not dispense with contractual formalization, and the classification is reviewed if the supply becomes recurring or the scope changes. The waiver does not apply to mandatory assessment cases.
4	Apply enhanced risk treatment to relationships with companies of the same economic group classified as supply of services, requiring at a minimum: a formalized intragroup contract; independent due diligence on the counterparty (KYP/KYVASP, where applicable); segregation of duties and flows; and independent reconciliation.
5	Review the classification whenever there is a relevant change in the scope of services, in the supplier's criticality or in the risks associated with the relationship.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

4.3 Prior due diligence

Step	Activity
6	Carry out due diligence before contracting, proportionally to the classification, covering, where applicable: governance structure and internal controls; information security and data protection controls; legal, regulatory and contractual compliance; service continuity capacity; management of the supply chain and subcontracting; reputation and integrity of the supplier, its partners or officers; and technical, operational and financial capacity. For suppliers and partners involving technical integration or relevant transactional recurrence, the assessment of technology and security controls is conducted jointly with Information Security.
7	For suppliers classified as Critical or High whose activity relates to virtual assets, foreign exchange, custody of funds, correspondent banking or client flows: screen partners, officers and ultimate beneficial owners against sanctions lists and PEP databases, using the same methodology applied to clients and counterparties.
8	Formally record the risks identified, the treatment measures and the decision regarding the contracting or continuation of the relationship.
9	Formalize the analysis of residual risks and the corresponding acceptance decision by the competent areas when it is not possible to fully meet the requirements defined for the assessment.

The background check covers the supplier or partner, its partners, officers and ultimate beneficial owners, and its result, together with the KYP Form, forms part of the due diligence file.

4.4 Cloud service providers

Cloud service providers are subject to the same due diligence requirements applicable to other suppliers, observing the additional requirements arising from the nature of the services provided.

Step	Activity
10	Additionally assess: the shared responsibility model adopted; data residency, location or sovereignty requirements; the existence of certifications, independent reports or other evidence of the effectiveness of controls; and adherence to the applicable legal, regulatory and contractual requirements.
11	Adopt alternative assessment mechanisms when limitations of the service model prevent full due diligence, with a formal risk assessment and recording and approval of the acceptance decision by the competent areas.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

4.5 Contracting

Step	Activity
12	Formalize the engagement through a contract or other legally valid document, including adhesion contracts, terms of use or terms of acceptance, before the start of the provision of services.
13	Ensure that the contract covers, where applicable: confidentiality, integrity and availability of information; protection of personal data; intellectual property; minimum information security requirements; responsibilities regarding subcontractors; incident reporting; right to audit or to obtain evidence; continuity of services; conditions for termination, return or secure disposal; integrity, ethics and compliance requirements; and the scope of services and responsibilities of the parties.
14	Include, for cloud providers: definition of responsibilities for security controls under the shared responsibility model; continuity, availability and resilience requirements; data location, residency or sovereignty requirements; and conditions for migration, return, portability and secure deletion upon termination of the services.
15	Assess the risks, formally record the acceptance decision and define compensating measures when the contractual terms are standardized by the provider and do not allow negotiation of specific clauses.
16	Establish formal confidentiality mechanisms commensurate with the risks when classified or sensitive information is shared.
17	Designate the Supplier Relationship Owner and record the designation.
18	Grant access to the supplier in accordance with the established security requirements.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

4.6 Monitoring

Step	Activity
19	Periodically reassess the supplier's risk classification.
20	Assess performance and compliance with contractual requirements.
21	Review information security, privacy, service continuity and compliance conditions.
22	Carry out audits, obtain evidence or perform other verification activities commensurate with the level of risk.
23	Monitor incidents relating to the supplier or its supply chain.
24	Assess relevant changes in the corporate structure, the services provided, the use of subcontracting or other factors that may affect the relationship.
25	For cloud providers: monitor changes in services or in the service model, changes in data location, residency or sovereignty, incidents and unavailability, and relevant changes in implemented security controls, using automated mechanisms whenever technically feasible.
26	Record monitoring activities and keep them in a traceable manner.

4.7 Supplier-related incidents

Step	Activity
27	Handle information security incidents involving suppliers in an integrated manner with the corporate incident management process.
28	Require the supplier to promptly report incidents that may affect the confidentiality, integrity, availability or privacy of information, under the contractual terms.
29	Assess the impacts arising from the incident and adopt measures proportional to the risks, including review of the controls, of the risk classification or of the continuation of the relationship.
30	For cloud services: observe the shared responsibility model, handling incidents under the provider's responsibility jointly with the provider, in accordance with the contracted service levels, and incidents under the Organization's responsibility in accordance with internal processes, engaging the provider when necessary.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

4.8 Measures resulting from the assessment

Step	Activity
31	Formally assess non-conformities, contractual breaches and situations that represent relevant risks, and define the applicable measures, which may include revision of the risk classification, implementation of treatment measures, or suspension or termination of the contractual relationship.

4.9 Termination and exit strategy

Step	Activity
32	Define and maintain an exit strategy for suppliers classified as Critical or High and for cloud providers whose interruption may affect business continuity, covering: recovery or migration of information in a usable format; secure deletion or return of information; continuity of services during the transition; preservation of evidence; and other necessary technical or contractual requirements.
33	Carry out termination in a controlled manner, covering: return, transfer or secure disposal of information and other assets; revocation of access granted to the supplier, its employees and authorized third parties; controlled termination or discontinuation of services; preservation of operational continuity during the transition; and recording of evidence.

4.10 Conflict of interest

Step	Activity
34	Act with impartiality, integrity and independence in the selection, assessment, contracting, monitoring or management of suppliers. Soliciting, offering, promising, receiving or accepting any advantage, benefit, gift or favor that may influence, or appear to influence, the impartiality of decisions is prohibited.
35	Promptly report to the responsible area any situations that may constitute a conflict of interest, including personal, family, corporate or commercial relationships with suppliers, for assessment and handling.

4.11 Waivers

A total or partial waiver of the requirements of this Procedure is an exceptional measure, always reasoned, temporary and recorded, and does not dispense with the contractual formalization set out in Section 4.5.

Screening against sanctions lists and PEP databases, where applicable under Section 4.3, enhanced treatment applicable to companies of the same economic group and contractual

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

formalization prior to the start of services cannot be waived.

5. Review

This Procedure is reviewed at least annually, or whenever there is a relevant change in the applicable legal, regulatory or contractual requirements, in the portfolio of critical suppliers or in the operational contracting flow, with approval by the Compliance area.

6. Reference Standards

- AML Policy (the policy to which this Procedure is subordinate).
- BCB Circular No. 3,978/2020, article 56: duty to know partners and outsourced service providers within the anti-money laundering and counter-terrorist financing program; and article 67: retention of records for 10 years.
- Law No. 9,613/1998: Anti-Money Laundering Law.
- BCB Resolution No. 520/2025: article 43, V (management of services provided by third parties), article 43, X (contracting of data processing and storage services) and articles 32 to 42 (duties relating to the contracting of third parties, including prior verification of capacity and compatibility of recovery plans with the incident response plan).
- BCB Resolutions No. 519 and 521/2025: applicable when the supplier operates in activities related to virtual assets or foreign exchange in the context of the activity of a Virtual Asset Service Provider (PSAV).
- BCB Resolution No. 85/2021: cybersecurity policy and contracting of data processing and storage and cloud computing services.
- Law No. 13,709/2018: General Personal Data Protection Law (LGPD).
- Law No. 12,846/2013: Anti-Corruption Law.
- ISO/IEC 27001:2022, Annex A: A.5.19 (Information security in supplier relationships), A.5.20 (Addressing information security within supplier agreements), A.5.21 (Managing information security in the ICT supply chain), A.5.22 (Monitoring, review and change management of supplier services) and A.5.23 (Information security for use of cloud services).
- ISO/IEC 27036 (applicable parts): Information security for supplier relationships.
- ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection, Information security management systems, Requirements.

	Supplier Management Procedure (KYP/KYS)	CPL-PRO-003-FIN
Publication Date: 08/31/2026	Compliance	Public

- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection, Information security controls.

7. Effectiveness

This Procedure is permanent in nature. The content of this document may be modified at any time according to current needs. Trace Finance's employees and service providers must, whenever necessary, consult the latest available version.

8. Version Control and History

Version	Date	Change/Addition History	Approved by
1.0	08/31/2026	Initial issue.	AML Director, with acknowledgment of the Compliance Committee