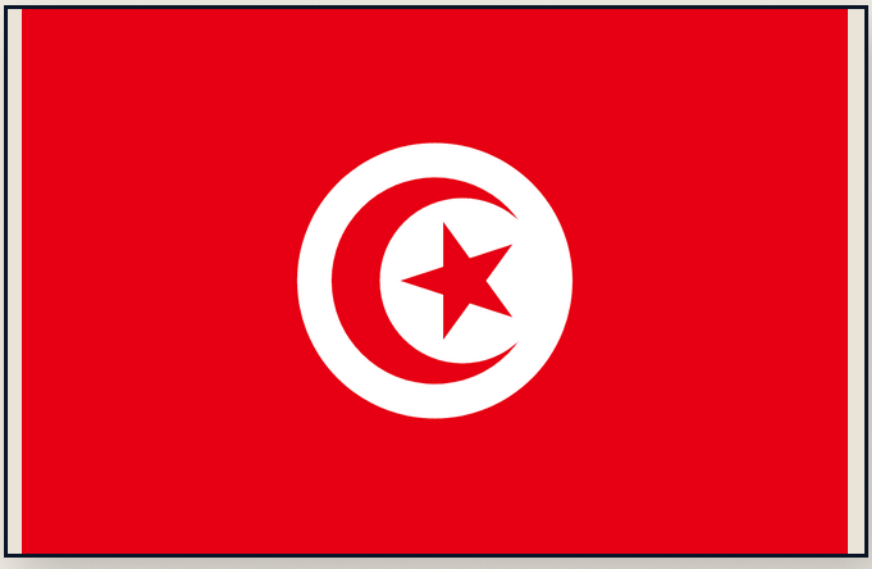
VOVE ID

VOVE COUNTRY CONTROL FILE

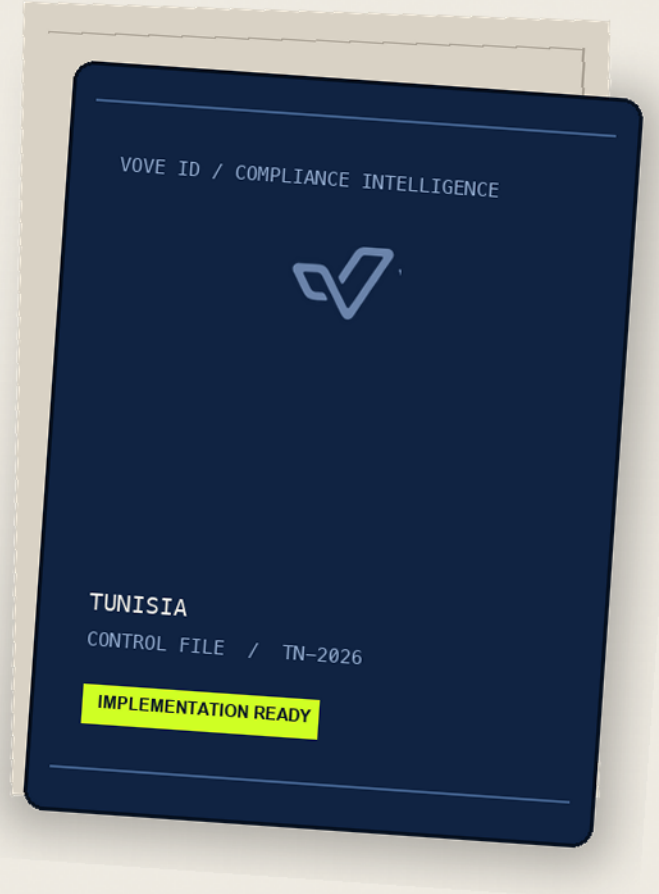
KYC / KYB / AML

2026 EDITION

TUNISIA



TUNISIA / TN



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Tunisia KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for fintechs, banks, financial institutions, payment institutions and other reporting persons operating in Tunisia. It translates the amended Organic Law No. 2015-26, current BCT sector rules, the National Register of Enterprises framework, targeted-financial-sanctions procedures and INPDP privacy formalities into operational controls and audit evidence.

Primary AML law	**Organic Law No. 2015-26, as amended**
Financial intelligence unit	**CTAF**
Banking and payments authority	**BCT**
Privacy authority	**INPDP**
Core AML record period	**At least 10 years**
FATF status	**Not under increased monitoring**

Scope and legal framework

Organic Law No. 2015-26 of 7 August 2015 on combating terrorism and preventing money laundering, as amended by Organic Law No. 2019-9 of 23 January 2019; Law No. 2016-48 on banks and financial institutions; Commission d'agrement Decision No. 2017-04, as amended by Decision No. 2019-20; BCT Circulars No. 2017-08, No. 2018-61 (published in the misleadingly named official file Cir_2018_16_fr.pdf), No. 2020-11, No. 2025-06, No. 2025-17 and No. 2026-02; Law No. 2018-52 on the National Register of Enterprises and Government Decree No. 2019-54; Government Decree No. 2019-419 as amended by Government Decree No. 2019-457; and Organic Law No. 2004-63 with Decrees No. 2007-3003 and No. 2007-3004.

FATF context

Tunisia is not on the FATF list of jurisdictions under increased monitoring as of the FATF statement dated 19 June 2026. FATF removed Tunisia from its monitoring process in October 2019. This status does not replace Tunisia's domestic risk-based requirements or enhanced controls for higher-risk customers, products, channels, transactions and geographies.

IMPORTANT

This checklist is general information, not legal advice. It reflects official materials available on 15 July 2026. Applicability depends on the entity, licence, product and sector. Confirm current requirements, reporting procedures, thresholds and approvals with CTAF, BCT, the relevant sector supervisor, INPDP, the National Register of Enterprises, the National Counter-Terrorism Commission and qualified Tunisian counsel before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

1. CONFIRM SCOPE, AUTHORITIES AND PERMISSIONS

Confirm scope, authorities and permissions

Determine first whether each activity falls within the general reporting-person perimeter and then add the rules of the competent sector supervisor.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document whether each entity and activity is within Article 107's reporting-person perimeter.	Map products and legal entities to banks and financial institutions, microfinance institutions, the National Post Office, securities intermediaries and portfolio managers, exchange offices, insurance businesses, or the specified designated non-financial businesses and professions. Do not assume that every commercial business is an Article 107 reporting person.	Signed perimeter memorandum; entity-product matrix; accountable supervisor mapping.	Organic Law No. 2015-26, as amended, art. 107
Recognise CTAF as the national FIU and reporting authority.	Maintain a controlled route for reports, information requests and freeze instructions. CTAF is established at BCT under Article 118 and receives and analyses suspicious reports under Article 120.	CTAF reporting procedure; nominated contacts; secure access register.	Organic Law No. 2015-26, as amended, arts. 118 and 120
Obtain BCT approval before conducting regulated banking, financial or payment-institution activity.	Classify the proposed service under the licensing provisions of Law No. 2016-48 and the Commission d'agrement approval procedure in Decision No. 2017-04, as amended by Decision No. 2019-20. A technology, agent or outsourcing label does not remove the licensed institution's responsibility or create an exemption.	Licence or approval; legal perimeter opinion; service-to-permission mapping; approval-procedure file.	Law No. 2016-48, licensing provisions; Commission d'agrement Decision No. 2017-04, as amended by Decision No. 2019-20
Apply payment rules only to entities and services within their stated scope.	For payment institutions, map accounts, cash services, transfers, remote payments and prepaid electronic-money distribution to BCT Circular No. 2018-61. The official BCT PDF filename says Cir_2018_16_fr.pdf, but the instrument's cover and operative text identify it as Circular No. 2018-61. Separately map domestic mobile-payment roles under Circular No. 2020-11.	Payment-service inventory; role map; licence conditions; mobile-payment scheme assessment.	BCT Circular No. 2018-61, arts. 1-4; BCT Circular No. 2020-11, arts. 1-3
Apply the current exchange-office AML/CFT/CPF framework only to bureaux de change within its scope.	Exchange offices must map BCT Circular No. 2026-02 into their sector programme, including customer due diligence, beneficial-owner and PEP controls, AML/CFT/CPF governance, immediate suspicious reporting through goAML and applicable supervisory sanctions. Do not present this exchange-office circular as a universal rule for all Article 107 reporting persons.	Exchange-office licence; Circular No. 2026-02 control map; CDD and PEP procedures; goAML access; sanctions register.	BCT Circular No. 2026-02
Assign owners for AML, payments, registry, sanctions and privacy obligations.	Maintain a responsibility matrix covering CTAF reporting, BCT filings, RNE checks, targeted freezes, INPDP formalities, outsourcing and regulatory change. Treat Article 115 as a direction to supervisory authorities to establish risk-based programmes and practical measures; ground each institution's policy, appointments, audit and training duties in the sector instrument applicable to that institution.	RACI; appointment records; committee terms; regulatory calendar; sector-obligation map.	Organic Law No. 2015-26, arts. 115 and 120; applicable BCT or other sector instrument

2. BUILD A RISK-BASED AML/CFT/CPF PROGRAMME

Build a risk-based AML/CFT/CPF programme

The programme must join governance, risk assessment, controls, training and assurance while preserving sector-specific requirements.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain written AML/CFT policies, monitoring and internal controls under the applicable sector instrument.	Cover customer due diligence, beneficial ownership, PEPs, sanctions, transaction monitoring, reporting, records, new products, non-face-to-face relationships, groups and outsourcing. Article 115 directs supervisory authorities to establish risk-based programmes and practical measures; it is not, by itself, the institution-level source for every policy control.	Approved policy suite; control library; procedure owners; review log; sector-rule mapping.	Organic Law No. 2015-26, arts. 108-115; BCT Circular No. 2017-08 as amended by No. 2025-17, or other applicable sector instrument
Designate responsible staff, assure controls and provide continuing training under the applicable sector instrument.	Create a suspicious-activity monitoring and escalation system, appoint reporting personnel, test control effectiveness and provide role-specific continuing training to the extent required by the BCT or other sector rules governing the institution. Do not attribute these institution-level duties solely to Article 115.	Appointment letters; training records; monitoring plan; control-test results; applicable-sector analysis.	BCT Circular No. 2017-08 as amended by No. 2025-17; BCT Circular No. 2026-02 for exchange offices; other applicable sector instruments; Organic Law No. 2015-26, art. 115
For BCT institutions within scope, assess money-laundering, terrorist-financing and proliferation-financing risk under the current circular.	Assess customers, products, services, delivery technologies and geographies, using national assessments and reliable external information. Document risk treatment and make the report available to BCT.	Institutional risk assessment; methodology; mitigation plan; BCT submission record.	BCT Circular No. 2017-08, art. 4, as replaced by BCT Circular No. 2025-17, art. 2
Apply the three-year assessment update rule only to institutions covered by BCT Circular No. 2025-17.	Update the documented BCT risk assessment at least every three years and sooner after a significant event, relevant regulatory change, new authority information or updated national risk assessment. Do not present this sector interval as a universal Article 107 rule.	Dated assessment cycle; event-trigger log; change analysis; governance approval.	BCT Circular No. 2025-17, art. 2 replacing Circular No. 2017-08, art. 4
Assess new technology and remote-delivery risks before use.	Evaluate impersonation, fraud, cyber, data, channel and AML risks before launching new products, practices, technology or delivery methods and implement proportionate mitigating controls.	Pre-launch risk assessment; threat model; control acceptance; launch decision.	Organic Law No. 2015-26, art. 112

3. IDENTIFY AND VERIFY INDIVIDUAL CUSTOMERS

Identify and verify individual customers

CDD must establish the customer, any representative, the beneficial owner and the purpose of the relationship using reliable evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Do not open or maintain clearly anonymous or fictitious-name accounts.	Configure onboarding and account controls to require a verified legal identity and detect placeholder, fabricated or materially inconsistent identity data.	Account-opening rules; blocked test cases; exception log.	Organic Law No. 2015-26, art. 108(1)
Identify and verify regular and occasional customers from official documents and reliable independent sources.	Collect the identity data needed to identify the person and verify it against valid official documents and other reliable independent information appropriate to the risk and channel.	Customer file; document and database checks; verification provenance.	Organic Law No. 2015-26, art. 108(1)
Identify the person for whose benefit a transaction is conducted and verify representatives and authority.	Identify the beneficiary of the operation, verify any person managing rights for that beneficiary, and verify the identity and authority of anyone acting for the customer.	Beneficiary record; representative ID; mandate or power; verification result.	Organic Law No. 2015-26, art. 108(2)
Establish the purpose and intended nature of the business relationship.	Record expected products, activity, source and destination patterns, counterparties and business rationale sufficient to set a customer-risk and monitoring profile.	Customer profile; expected-activity baseline; risk score and rationale.	Organic Law No. 2015-26, art. 108(4)
Apply CDD at the statutory triggers without inventing a universal monetary threshold.	Trigger CDD when establishing a relationship, for occasional transactions at or above the amount set by the Finance Minister or involving electronic transfers, whenever ML/TF is suspected, and whenever existing identity data appears unreliable or insufficient. Maintain the currently applicable threshold in a controlled register.	Trigger matrix; current-threshold register; workflow rules; test results.	Organic Law No. 2015-26, art. 108
Refuse or end activity when required identity data cannot be trusted or completed.	Do not open or continue an account or relationship and do not execute the transaction where identity data cannot be verified, are insufficient or are manifestly fictitious; consider filing a suspicious report.	Decline or exit record; investigation decision; STR consideration log.	Organic Law No. 2015-26, art. 108, final paragraph

4. VERIFY BUSINESSES AND BENEFICIAL OWNERS

Verify businesses and beneficial owners

KYB must establish legal existence, management, ownership, control and the natural persons who ultimately own or control the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person or arrangement and its operating identity.	Obtain reliable evidence of legal form, registered office, capital distribution, managers and persons responsible for the entity, together with constitutional, registry and authority records appropriate to the customer.	Current RNE extract; constitutive documents; management list; address and authority checks.	Organic Law No. 2015-26, art. 108(2)
Identify the beneficial owner and take reasonable measures to verify that identity.	Trace ownership and control through every layer to natural persons, use reliable information and record why the analysis supports the identified beneficial owner.	Ownership chart; control analysis; source records; verified BO files.	Organic Law No. 2015-26, arts. 3 and 108(3)
Apply the CTAF beneficial-owner cascade and threshold accurately.	Under CTAF Decision No. 2018-10, identify natural persons holding directly or indirectly at least 20% of capital or voting rights; if identity remains doubtful or no one is identified, identify control by other means; if still unresolved, identify the natural person holding the senior management position. Apply the decision's separate party-based analysis for trusts and similar arrangements.	Percentage calculation; other-control analysis; senior-manager fallback rationale; trust-party file.	CTAF Decision No. 2017-03, as amended by Decision No. 2018-10, arts. 6-8
Reconcile the applicable sector definition rather than silently merging thresholds.	BCT Circular No. 2017-08 defines a beneficial owner for covered BCT institutions using more than 20% of capital or voting rights together with ultimate ownership or effective-control concepts. Record which legal and sector text governs the case and apply the stricter control where necessary.	Threshold mapping; sector legal analysis; approved KYB rule configuration.	BCT Circular No. 2017-08, art. 2, as amended; CTAF Decision No. 2018-10
Apply the National Register of Enterprises beneficial-owner cascade.	For the NRE framework, identify natural persons who directly or indirectly hold at least 20% of capital or voting rights. If no person is identified through ownership, identify control by other means; if the analysis still identifies no natural person, record the senior-manager fallback under Government Decree No. 2019-54.	NRE threshold calculation; layered ownership chart; other-control analysis; senior-manager fallback rationale.	Law No. 2018-52; Government Decree No. 2019-54
Use the National Register of Enterprises without treating it as conclusive CDD.	Verify registration, filings and beneficial-owner declarations under Law No. 2018-52, Government Decree No. 2019-54 and current RNE procedures; reconcile discrepancies with customer evidence and investigate rather than relying solely on a registry extract.	RNE extract; BO declaration or non-filing certificate; discrepancy case; independent corroboration.	Law No. 2018-52; Government Decree No. 2019-54; RNE beneficial-owner services; Order of the Head of Government dated 13 January 2026

5. APPLY PEP, ENHANCED AND REMOTE DUE DILIGENCE

Apply PEP, enhanced and remote due diligence

Higher-risk relationships require stronger approval, source and monitoring controls; sector-specific digital onboarding rules must remain distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify domestic, foreign and international-organisation PEPs, including relevant relatives and connected persons.	Use risk-based systems capable of determining whether the customer or beneficial owner currently or formerly holds the covered public, political or international-organisation function and assess the connected-person relationship.	PEP screening record; relationship analysis; match disposition.	Organic Law No. 2015-26, art. 110
Obtain senior approval and establish source of funds for PEP relationships.	Obtain approval from the legal entity's manager before starting or continuing the relationship, apply tight continuous monitoring and take reasonable measures to identify source of funds.	Source-of-funds review; corroborating records; senior approval; monitoring plan.	Organic Law No. 2015-26, art. 110
Apply enhanced attention to higher-risk countries and relationships.	Identify customers and relationships connected to countries that do not or insufficiently apply international AML/CFT standards and apply documented measures proportionate to the identified risk.	Country-risk methodology; enhanced review; approval and monitoring settings.	Organic Law No. 2015-26, art. 112
Control non-face-to-face relationship risk.	Maintain systems specifically designed to manage relationships conducted without physical presence, including document integrity, impersonation, device, fraud and escalation controls.	Remote-onboarding standard; vendor assessment; control tests; exception cases.	Organic Law No. 2015-26, art. 112
For banks, meet the current electronic-enrollment standard.	Where a bank enrolls customers electronically, implement board-approved procedures, risk mapping, proportionate authentication, reliable document verification, real-presence or liveness controls, biometric matching where used, screening, performance monitoring and incident management. Achieve identity assurance at least equivalent to physical presence.	Board approval; end-to-end process map; liveness and matching tests; performance register; incident log.	BCT Circular No. 2025-06, arts. 1-7

6. MONITOR ACTIVITY AND REPORT SUSPICION

Monitor activity and report suspicion

Monitoring must remain aligned with current customer information and route suspicion immediately and confidentially to CTAF.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep customer identity information current and conduct ongoing vigilance.	Refresh data on risk-based and event-driven triggers, then examine transactions for consistency with known activity, risk profile and, where necessary, source of funds.	Refresh rules; event triggers; completed reviews; overdue dashboard.	Organic Law No. 2015-26, art. 109
Examine complex, unusually large or apparently purposeless activity and record the result.	Investigate the context and purpose of complex operations, unusually high amounts and unusual transactions lacking an apparent economic or lawful purpose; record findings in writing and make them available to supervisors and auditors.	Written special-examination report; supporting data; reviewer sign-off.	Organic Law No. 2015-26, art. 126
Report covered suspicion and attempted activity immediately in writing to CTAF.	File when an operation or transaction, including an attempt, is suspected of direct or indirect connection to proceeds of an unlawful act classified as an offence or crime, or to financing persons, organisations or activities connected with terrorist offences. File after execution as well if new information creates the suspicion.	STR decision; filing receipt; chronology; restricted case file.	Organic Law No. 2015-26, art. 125
For institutions within BCT Circular No. 2025-17, submit immediate reports through goAML.	Use the CTAF goAML platform and its current technical procedures. Do not use the unsupported ten-day timing stated in some secondary materials; the governing law and current BCT rule require immediate reporting.	goAML access; filing procedure; receipt; timing audit.	BCT Circular No. 2025-17, art. 6; Organic Law No. 2015-26, art. 125
Prevent tipping off and implement CTAF temporary-freeze instructions.	Do not tell the affected party about the report or resulting measures. On written CTAF instruction, temporarily freeze the assets linked to the report and place them in a suspense account until the legally prescribed outcome.	Confidentiality controls; access logs; freeze workflow; regulator correspondence.	Organic Law No. 2015-26, arts. 127-132

7. IMPLEMENT TARGETED FINANCIAL SANCTIONS

Implement targeted financial sanctions

UN and national designations require immediate operational controls distinct from ordinary suspicious-transaction investigations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen customers, beneficial owners, controllers and transactions against applicable UN and national designations.	Screen at onboarding, on list changes, on material customer changes and before relevant transactions; include aliases, transliteration and ownership or control analysis.	List inventory; screening configuration; update logs; match files.	Organic Law No. 2015-26, art. 103; Government Decree No. 2019-419 as amended by No. 2019-457
Freeze covered funds and assets without delay and prevent making resources available.	Create an always-available legal and technical path to freeze funds and other assets and prevent direct or indirect availability to designated persons, organisations and entities under the applicable UN or national decision.	Freeze procedure; system tests; incident timeline; decision record.	Organic Law No. 2015-26, art. 103; Government Decree No. 2019-419 as amended
Notify the National Counter-Terrorism Commission and provide useful implementation information.	Follow the notification, information, delisting, unfreezing and false-positive procedures in the 2019 decree framework and current CNLCT instructions.	Notification template; filing record; authority correspondence; release decision.	Organic Law No. 2015-26, art. 103; Government Decrees No. 2019-419 and No. 2019-457
For BCT-covered institutions, manage proliferation-financing risk and BCT sanctions reporting.	Include UN targeted-financial-sanctions evasion in proliferation-financing risk. Submit the required quarterly frozen-assets statement to BCT within 20 working days after quarter-end, covering UN, national and proliferation-financing freezes.	PF risk controls; frozen-assets register; quarterly return; submission receipt.	BCT Circular No. 2025-17, arts. 2 and 8
Keep sanctions and STR decisions separate but coordinated.	Execute a legally required freeze without waiting for an STR decision, then separately assess CTAF reporting and preserve confidentiality across both workflows.	Decision matrix; linked case records; role-based access; audit trail.	Organic Law No. 2015-26, arts. 103, 125 and 127

8. RETAIN RECORDS AND SUPPORT RECONSTRUCTION

Retain records and support reconstruction

Records must permit reconstruction of transactions, customer decisions and persons involved over the statutory period.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep AML records for at least 10 years from transaction completion or account closure.	Retain ledgers, books and other physical or electronic records so the stages of an operation or transaction can be reviewed, the parties identified and the reliability of the transaction assessed.	Retention schedule; lifecycle configuration; sample retrieval.	Organic Law No. 2015-26, art. 113
Apply the correct retention event to each record class.	Use transaction completion for transaction records and account closure for account-linked records; preserve legal holds and longer periods where another applicable law or authority instruction requires them.	Record-class matrix; clock rules; legal-hold procedure.	Organic Law No. 2015-26, art. 113
For payment institutions, keep payment-operation registers for at least 10 years from execution.	Preserve identifiers, amounts, dates, parties, account or wallet references, agent data, screening and decision history sufficient for full payment reconstruction.	Payment register; data-lineage map; reconstruction test.	BCT Circular No. 2018-61, art. 12
Preserve written unusual-transaction analysis and reporting evidence securely.	Separate STR, sanctions and special-examination files from ordinary service access while keeping them retrievable for authorised CTAF, BCT, supervisory and audit requests.	Access matrix; immutable logs; disclosure register; retrieval test.	Organic Law No. 2015-26, arts. 113, 121, 124, 126 and 127
Test record completeness and recoverability.	Periodically reconstruct selected onboarding, ownership, payment, alert and reporting cases from source data through final decision and remediate missing lineage.	Sample test results; defects; remediation evidence; management reporting.	Organic Law No. 2015-26, arts. 113 and 115

9. PROTECT PERSONAL AND BIOMETRIC DATA

Protect personal and biometric data

KYC and monitoring data remain subject to Tunisia's privacy law and INPDP formalities even when processing supports a regulatory obligation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Define a specific, lawful purpose for each personal-data processing operation.	Map identity, biometric, contact, device, transaction, screening and investigation data to stated purposes, recipients, systems, retention and security controls; separate mandatory compliance use from optional analytics or marketing.	Data inventory; processing register; purpose and necessity assessment.	Organic Law No. 2004-63
Submit an INPDP declaration for each processing purpose before processing.	Classify each purpose and complete the declaration required by Article 7 using the procedure and supporting documents specified by INPDP and Decree No. 2007-3004.	INPDP declaration; receipt; purpose-to-filing matrix.	Organic Law No. 2004-63, art. 7; Decree No. 2007-3004; INPDP forms
Obtain additional INPDP authorisation where the processing category requires it.	In addition to the declaration, seek prior authorisation for biometric processing, transfers abroad and the other categories identified by Articles 13 and 14 and current INPDP forms. Do not treat customer consent as a substitute for the authority filing.	Authorisation application and decision; data-flow map; production gate.	Organic Law No. 2004-63, arts. 13-14; Decree No. 2007-3004; INPDP forms
Minimise and secure identity evidence throughout its lifecycle.	Collect only necessary data, restrict access, encrypt appropriately, log use, validate deletion, manage incidents and test processors in proportion to identity, biometric and financial-crime risk.	Data-minimisation review; security architecture; access logs; deletion and incident tests.	Organic Law No. 2004-63; Decree No. 2007-3004
Operationalise data-subject information and rights subject to lawful AML retention and confidentiality limits.	Provide the required information, authenticate requests and document any lawful restriction arising from AML recordkeeping, STR confidentiality, investigations or sanctions controls.	Privacy notice; request workflow; response log; restriction rationale.	Organic Law No. 2004-63; Organic Law No. 2015-26, arts. 113, 124 and 127

10. OPERATE PAYMENT AND MOBILE-PAYMENT CONTROLS

Operate payment and mobile-payment controls

Licensed payment operations add safeguarding, governance, security, agent and scheme controls to the general AML framework.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Provide only the payment services and geographic-currency scope allowed by the licence and BCT rules.	Map payment accounts, cash-in and cash-out, direct debits, payments, transfers, remote payments and prepaid electronic-money distribution to the approval. Circular No. 2018-61 limits covered payment-institution services to Tunisian dinars within Tunisia, subject to specific foreign-transfer authority where applicable.	Licence conditions; product map; currency and geography controls.	BCT Circular No. 2018-61, arts. 2-4
Maintain payment-institution governance, control, traceability and resilience.	Operate proportionate governance, audit and risk oversight, real-time transaction recording, fraud and intrusion prevention, personal-data controls, operational and cyber-risk management, a tested continuity plan and the prescribed security audit.	Governance records; system architecture; continuity test; security-audit report; incident file.	BCT Circular No. 2018-61, arts. 5-10
Apply AML controls and the applicable cu stomer-identification tier to every payment account.	Treat payment institutions as subject to the BCT AML-control circular through Article 11, and configure each account level according to the identification and operating limits in Article 14. Maintain current regulatory values rather than copying thresholds into uncontrolled product code.	Account-tier matrix; AML control mapping; configuration approval; test cases.	BCT Circular No. 2018-61, arts. 11 and 14; BCT Circular No. 2017-08 as amended
Safeguard customer funds in the separate global account and reconcile them.	Keep the global account balance aligned with all customer payment-account balances, prohibit use for the institution's own operating needs, maintain holder-level allocation and perform the required reconciliation.	Depository agreement; global-account ledger; customer allocation; reconciliation and shortfall log.	BCT Circular No. 2018-61, arts. 20-23
Control payment agents under the institution's continuing responsibility.	Select, train and monitor agents, notify BCT as required, contract the permitted services, verify capacity and integrity, and ensure agents apply the same customer-identification standard. Do not use agents to open payment accounts remotely where the circular prohibits it.	Agent policy; due-diligence file; BCT notice; contract; training and monitoring records.	BCT Circular No. 2018-61, arts. 24-30
Map domestic mobile-payment roles and scheme obligations.	Identify the wallet issuer, acquirer, participant, agent and mobile-switch roles and implement Circular No. 2020-11 controls for interoperability, security, customer protection, AML and operational responsibility.	Scheme role map; participant agreements; control matrix; operational tests.	BCT Circular No. 2020-11

11. LAUNCH, OVERSEE AND EVIDENCE COMPLIANCE

Launch, oversee and evidence compliance

A publication-ready policy is not enough; each control needs an owner, system implementation and evidence that can survive supervisory review.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Run a documented pre-launch regulatory gate.	Confirm perimeter, licence, CTAF registration and reporting access, CDD and BO rules, PEP and sanctions controls, monitoring, records, RNE access, INPDP filings, safeguarding, agents, outsourcing and incident readiness before production.	Launch checklist; accountable approvals; unresolved-risk register.	Organic Law No. 2015-26; applicable BCT, RNE, CNLCT and INPDP instruments
Control reliance and outsourcing without transferring legal responsibility.	Assess providers, obtain required customer data immediately, ensure prompt access to identity records, contract security and audit rights and maintain the reporting person's responsibility for verification.	Provider assessment; contract; data-access test; exit plan.	Organic Law No. 2015-26, art. 108(5); applicable BCT outsourcing rules
Maintain regulatory-change monitoring with sector ownership.	Track CTAF decisions, BCT circulars and notes, RNE procedures, CNLCT lists and decrees, INPDP formalities and FATF statements; assess each change against product configuration and customer files.	Legal inventory; change alerts; impact assessments; implementation tickets.	CTAF, BCT, RNE, CNLCT, INPDP and FATF official publications
Test controls independently and remediate findings.	Use risk-based compliance monitoring and independent audit to test onboarding, BO, PEP, sanctions, payment, monitoring, STR, privacy and recordkeeping controls; report material issues to governance bodies.	Monitoring plan; audit reports; issue register; closure evidence.	Organic Law No. 2015-26, art. 115; applicable BCT internal-control circulars
Preserve a defensible implementation record.	For each material rule, retain the source, interpretation, configuration, test, owner, approval and effective date so the organisation can explain not only what the control is, but why it is correctly implemented.	Obligations register; control-to-law map; approvals; release and test history.	Organic Law No. 2015-26, arts. 113 and 115; BCT Circular No. 2025-17

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

Organic Law No. 2015-26 as amended by Organic Law No. 2019-9, English consolidation
CTAF · Primary legislation
Open official source

CTAF mandate, Article 107 scope and Article 125 reporting guidance
CTAF · Official FIU portal
Open official source

BCT circulars and notes, including 2025 and 2026 instruments
Central Bank of Tunisia · Official regulatory register
Open official source

BCT Circular No. 2017-08 on AML/CFT internal controls
Central Bank of Tunisia · Primary regulation
Open official source

BCT Circular No. 2025-17 on AML/CFT/CPF internal controls
Central Bank of Tunisia · Primary regulation
Open official source

BCT Circular No. 2025-06 on electronic customer enrollment
Central Bank of Tunisia · Primary regulation
Open official source

BCT Circular No. 2018-61 governing payment institutions (the official filename misleadingly reads Cir_2018_16_fr.pdf)
Central Bank of Tunisia · Primary regulation
Open official source

Commission d'agrement Decision No. 2017-04 on approval procedures, as amended by Decision No. 2019-20
Central Bank of Tunisia · Primary licensing procedure
Open official source

BCT Circular No. 2026-02 governing bureaux de change
Central Bank of Tunisia · Primary sector regulation
Open official source

BCT Circular No. 2020-11 on domestic mobile-payment services
Central Bank of Tunisia · Primary regulation
Open official source

Law No. 2018-52 on the National Register of Enterprises
CTAF / Republic of Tunisia · Primary legislation
Open official source

Government Decree No. 2019-54 establishing the NRE beneficial-owner cascade
Republic of Tunisia · Primary regulation
Open official source

National Register of Enterprises legal framework and beneficial-owner services
National Register of Enterprises · Official registry guidance
Open official source

Order of the Head of Government of 13 January 2026 on access to beneficial-owner information
National Register of Enterprises / Republic of Tunisia · Primary regulation
Open official source

Government Decree No. 2019-419 as amended by No. 2019-457
National Counter-Terrorism Commission · Primary sanctions framework
Open official source

Tunisian personal-data protection texts
INPDP · Official legislation portal
Open official source

Organic Law No. 2004-63 on personal-data protection
INPDP · Primary legislation
Open official source

Decree No. 2007-3003 on the operation of INPDP
INPDP · Primary regulation
Open official source

Decree No. 2007-3004 on declarations and authorisations
INPDP · Primary regulation
Open official source

Personal-data declarations and prior-authorisation forms
INPDP · Official compliance procedure
Open official source

Jurisdictions under increased monitoring, 19 June 2026
FATF · Official FATF statement
Open official source

Tunisia no longer subject to FATF monitoring, 18 October 2019
FATF · Official FATF statement
Open official source

Tunisia country page and assessment history
FATF · Official country profile
Open official source

AML Compliance in Tunisia: A 2026 Guide for Fintechs and Regulated Businesses
VOVE ID · Contextual implementation guide; not legal authority
Open contextual guide

Document control

Version 1.2 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general information, not legal advice. It reflects official materials available on 15 July 2026. Applicability depends on the entity, licence, product and sector. Confirm current requirements, reporting procedures, thresholds and approvals with CTAF, BCT, the relevant sector supervisor, INPDP, the National Register of Enterprises, the National Counter-Terrorism Commission and qualified Tunisian counsel before launch.