🏦 FinSight Bank

PROCÉDURE KYC ET LUTTE CONTRE LE BLANCHIMENT (LCB-FT)

Date : Janvier 2025
Document interne – À usage de démonstration

---

1. Objet et cadre réglementaire

La présente procédure définit le dispositif de connaissance du client (*Know Your Customer – KYC*) et de lutte contre le blanchiment de capitaux et le financement du terrorisme (*LCB-FT*) mis en œuvre par **FinSight Bank**. Elle a pour finalité d'assurer la conformité intégrale des opérations de la Banque aux prescriptions légales nationales et internationales en matière de prévention des infractions financières, de protection du système bancaire et de préservation de la réputation de l'institution.

Ce dispositif s'inscrit dans le cadre de la **loi tunisienne n° 2016-48 relative aux établissements de crédit et organismes financiers**, de la **loi n° 2015-26 du 7 août 2015 relative à la lutte contre le terrorisme et le blanchiment d'argent**, ainsi que de la **circulaire BCT n° 2018-06 du 6 juin 2018** fixant les exigences minimales du système LCB-FT applicable aux banques et institutions assimilées. Il tient également compte des **Recommandations 10 à 21 du Groupe d'Action Financière (GAFI)** relatives à la diligence raisonnable, à la surveillance continue des relations d'affaires et au signalement des opérations suspectes.

Le champ d'application couvre l'ensemble des produits, services, réseaux et canaux de distribution de FinSight Bank, y compris les services digitaux et les filiales à participation majoritaire. Toute personne physique ou morale entretenant une relation d'affaires avec la Banque est soumise au dispositif KYC et LCB-FT, qu'il s'agisse d'un client, d'un mandataire, d'un bénéficiaire effectif ou d'un partenaire.

FinSight Bank reconnaît que la mise en place d'un cadre LCB-FT robuste constitue une composante essentielle de sa gouvernance et de sa solidité financière. À ce titre, la présente procédure formalise les principes de vigilance, de détection et de déclaration qui doivent être respectés par l'ensemble des collaborateurs.

---

2. Gouvernance et responsabilités

La gouvernance du dispositif LCB-FT repose sur une architecture clairement définie de responsabilités et de lignes de défense complémentaires. Le **Conseil d'Administration** établit les orientations stratégiques et veille à l'allocation des moyens nécessaires à la mise en conformité. Il valide les politiques internes, évalue les rapports périodiques et approuve les plans d'action correctifs.

La **Direction Générale** assure la mise en œuvre opérationnelle de ces orientations et garantit que les procédures de vigilance sont intégrées à l'ensemble des processus bancaires. Elle délègue au **Responsable Conformité/LCB-FT Officer** la mission de supervision quotidienne du dispositif, notamment la veille réglementaire, l'analyse des alertes et la coordination avec la **Commission Tunisienne des Analyses Financières (CTAF)**. Ce responsable agit en toute indépendance fonctionnelle et dispose d'un accès direct au Conseil d'Administration en cas d'alerte majeure.

Les **correspondants LCB-FT régionaux** sont chargés d'appliquer la politique au sein des directions territoriales. Ils veillent à la cohérence des pratiques, à la remontée d'informations et au respect des délais de revue. L'**Audit Interne** constitue la troisième ligne de défense : il évalue périodiquement la qualité du dispositif, la pertinence des outils et la conformité des opérations. Ses conclusions sont communiquées au Comité d'Audit et au Comité des Risques.

L'ensemble du personnel de FinSight Bank, sans distinction de fonction, est tenu de contribuer activement à la prévention du blanchiment et du financement du terrorisme. Chaque collaborateur doit exercer une vigilance constante sur les transactions qu'il initie ou traite, et signaler toute anomalie ou comportement atypique selon la procédure interne de déclaration. Le non-respect de ces obligations expose à des sanctions disciplinaires et, le cas échéant, pénales.

---

3. Identification et vérification des clients (KYC)

La connaissance du client constitue le premier rempart contre les activités illicites. Elle repose sur le principe selon lequel aucune relation d'affaires ne peut être engagée sans identification complète et vérification préalable de l'identité du client et de son bénéficiaire effectif.

Lors de l'entrée en relation, le chargé de clientèle collecte les documents officiels d'identité, le justificatif de domicile, les informations sur la profession, la source des revenus et la finalité de la relation bancaire. Pour les personnes morales, sont exigés les statuts, le registre du commerce, la liste des bénéficiaires effectifs et la structure de détention du capital. Les clients doivent être interrogés sur l'origine des fonds, la nature des opérations envisagées et les contreparties habituelles.

Les informations recueillies sont saisies dans le système *FinSight Onboard* qui procède à des vérifications automatiques sur les listes de sanctions nationales et internationales (CTAF, ONU, UE, OFAC). Les correspondances positives déclenchent une procédure de validation renforcée avant toute ouverture de compte.

Le niveau de vigilance appliqué dépend du degré de risque associé au client. FinSight Bank applique trois degrés de diligence : **vigilance simplifiée** pour les clients à risque faible (salariés, revenus stables, origine locale claire), **vigilance standard** pour la majorité des

clients, et **vigilance renforcée** pour les profils sensibles tels que les **personnes politiquement exposées (PEP)**, les non-résidents ou les clients opérant dans des secteurs à forte exposition.

Les données KYC doivent être actualisées périodiquement ou dès qu'un changement significatif est constaté : modification d'adresse, d'activité, d'actionnariat ou de comportement transactionnel. Toute relation d'affaires ouverte sans identification complète doit être bloquée jusqu'à régularisation.

---

4. Classification et évaluation des risques

FinSight Bank a mis en place un système interne de classification des risques permettant de segmenter sa clientèle selon des critères objectifs et mesurables. L'évaluation s'effectue lors de l'entrée en relation et fait l'objet d'une révision régulière.

Le modèle LCB-FT interne prend en compte plusieurs dimensions : le profil du client, la nature de son activité, le volume et la fréquence des transactions, l'origine géographique des fonds, le canal de distribution utilisé et le degré de complexité des opérations. Chaque critère reçoit un coefficient pondéré selon sa contribution au risque global.

Les clients sont classés en trois catégories : **Risque Faible**, **Risque Moyen** et **Risque Élevé**. Un client à risque faible présente une activité transparente et stable, avec des flux domestiques limités. Un client à risque moyen exerce une activité plus diversifiée ou internationale nécessitant une surveillance accrue. Les clients à risque élevé incluent les PEP, les entités sans présence physique significative, les sociétés offshore ou toute structure à chaîne de détention complexe.

Les résultats de la classification alimentent le moteur d'alerte *FinSight AML-Scoring*® qui ajuste la fréquence de la revue périodique :

- risque faible : 12 mois ;
- risque moyen : 6 mois ;
- risque élevé : 3 mois.

Un rapport consolidé des notations est transmis chaque trimestre à la Direction Conformité et au Comité des Risques, permettant une vision globale de l'exposition du portefeuille clients.

Tableau 1 – Catégorisation et revue des clients (2025)

Catégorie de client	Exemples de profils	Fréquence de revue	Niveau de vigilance
Risque faible	Salariés locaux, PME domestiques	12 mois	Vigilance standard
Risque moyen	Importateurs, sociétés mixtes	6 mois	Vigilance renforcée
Risque élevé	PEP, offshore, non-résidents	3 mois	Surveillance continue

---

5. Surveillance des transactions

La surveillance des transactions constitue la seconde ligne de défense du dispositif LCB-FT. Elle permet de détecter les opérations atypiques, incohérentes ou disproportionnées au regard du profil KYC du client.

FinSight Bank a développé un outil interne de *Transaction Monitoring* intégré à sa plateforme AML-Suite. Cet outil analyse quotidiennement l'ensemble des opérations enregistrées, qu'elles soient réalisées en agence, via les canaux digitaux ou à travers les systèmes interbancaires. Les règles de détection reposent sur des seuils paramétrables, des scénarios de comportement et des indicateurs d'alerte définis par la Direction Conformité.

Les typologies d'alerte couvrent notamment :

- les virements internationaux récurrents de faible montant sans justification économique claire ;
- les dépôts et retraits successifs en espèces suivis de transferts rapides vers l'étranger ;
- les mouvements croisés entre comptes liés sans logique commerciale ;
- l'utilisation de comptes de transit par des sociétés récemment constituées ;
- les opérations impliquant des juridictions à risque élevé ou sous sanctions internationales.

Chaque alerte générée est analysée par un analyste conformité dans un délai maximum de 48 heures. Les dossiers jugés suspects font l'objet d'un examen approfondi et, le cas échéant, d'une **Déclaration d'Opération Suspecte (DOS)** adressée à la CTAF dans les 24 heures suivant la confirmation du caractère douteux.

Le système AML-Suite conserve la trace de toutes les alertes, des décisions prises et des justifications associées afin d'assurer la traçabilité et la possibilité d'audit. Les indicateurs

de performance (nombre d'alertes, taux de DOS, délai de traitement) sont communiqués mensuellement à la Direction Générale et au Comité de Conformité.

Tableau 2 – Typologies suspectes observées (2025)

Catégorie de risque	Exemple d'opération	Action attendue	Délai de traitement
Particulier	Virements récurrents vers zones offshore sans justification	Analyse + déclaration	≤ 24 h
PME	Flux triangulaires entre comptes liés	Vérification contractuelle	≤ 48 h
PEP	Dépôts espèces répétés suivis de transferts rapides	Escalade Conformité / CTAF	Immédiat

---

FinSight Bank considère que la surveillance continue est une obligation permanente et non un exercice ponctuel. La technologie ne saurait remplacer le jugement humain : la vigilance du personnel demeure la clé du dispositif. Chaque collaborateur doit adopter une attitude prudente, conserver une distance critique face aux comportements inhabituels et signaler sans délai toute situation ambiguë.

---

6. Déclaration des opérations suspectes (DOS)

La déclaration des opérations suspectes représente le point culminant du dispositif de vigilance mis en place par FinSight Bank. Elle traduit l'obligation légale pour tout établissement financier de signaler sans délai à la **Commission Tunisienne des Analyses Financières (CTAF)** toute opération ou tentative d'opération qui paraît suspecte quant à son origine, sa destination, son objet ou sa justification économique.

Le processus interne est strictement encadré afin d'assurer la confidentialité, la rapidité et la traçabilité des déclarations. Lorsqu'une anomalie est détectée, l'analyste conformité examine le dossier à la lumière du profil KYC et des historiques de transactions. Si les explications fournies par le client demeurent insuffisantes ou incohérentes, un **rapport d'alerte** est immédiatement transmis au **Responsable LCB-FT** pour évaluation.

Celui-ci dispose d'un délai maximal de **vingt-quatre heures** pour valider ou écarter le signalement. En cas de confirmation, la **Déclaration d'Opération Suspecte (DOS)** est rédigée dans le format prévu par la CTAF et transmise par canal sécurisé. La décision et les pièces justificatives sont archivées dans le système *FinSight AML-Suite* de manière chiffrée.

Aucun collaborateur n'est autorisé à informer le client de l'existence ou du contenu d'une DOS, conformément au principe de **non-divulgation** prévu par la législation tunisienne et les standards internationaux. Cette confidentialité absolue protège à la fois l'enquête et la Banque.

Le suivi des déclarations s'effectue en coordination étroite avec la CTAF : les réponses ou demandes d'informations complémentaires sont traitées dans un délai de quarante-huit heures. Un registre interne récapitulatif des DOS est tenu par la Direction Conformité et communiqué trimestriellement au Comité d'Audit.

Tableau 3 – Processus interne de déclaration des opérations suspectes

Étape	Acteur responsable	Délai maximal	Système utilisé
Détection de l'anomalie	Analyste Conformité	48 h	AML-Suite
Validation et décision	Responsable LCB-FT	24 h	AML-Suite
Transmission CTAF	Direction Conformité	Immédiat	Canal sécurisé
Archivage et suivi	Responsable Sécurité SI	Permanent	Serveur chiffré

---

7. Formation et sensibilisation

La conformité n'est pleinement efficace que si elle s'appuie sur une culture institutionnelle partagée. FinSight Bank considère la **formation LCB-FT** comme un levier stratégique de prévention et un élément central de la responsabilité individuelle.

Chaque nouveau collaborateur suit, dès son intégration, un module d'e-learning obligatoire sur les obligations KYC, la détection des opérations suspectes et la procédure de déclaration. Ce programme est complété par des sessions présentielles animées par la Direction Conformité, abordant les typologies locales de blanchiment et les tendances émergentes identifiées par la BCT et la CTAF.

Une **formation continue annuelle** est dispensée à l'ensemble du personnel, avec un contenu adapté aux fonctions : le front-office est formé à la vigilance client et à l'entretien KYC ; le back-office à la surveillance transactionnelle ; la direction aux responsabilités pénales encourues.

Les participants sont évalués à l'aide de tests de validation ; leurs résultats sont conservés dans le *Système de Gestion des Compétences FinSight HR*. Les taux de participation et de réussite font l'objet d'un reporting semestriel présenté au **Comité des Risques**.

La Banque renforce cette dynamique par une **campagne annuelle de sensibilisation** intitulée *"Culture Conformité – Un reflexe quotidien"*, diffusée sur l'intranet et les supports internes. Elle vise à maintenir la vigilance, valoriser les bonnes pratiques et rappeler que la lutte contre le blanchiment est l'affaire de tous.

---

8. Conservation et archivage

La conservation des documents KYC et des éléments de surveillance constitue une obligation réglementaire majeure. FinSight Bank applique les principes énoncés dans la *Circulaire BCT n° 2018-06* et les standards du GAFI : tout document, donnée ou enregistrement relatif à l'identification des clients, à leurs transactions ou aux déclarations suspectes doit être conservé **au minimum 10 ans** après la fin de la relation d'affaires.

Les dossiers sont stockés de manière électronique dans l'outil *FinSight Docs Secure*, hébergé sur des serveurs redondants situés en Tunisie et conformes aux exigences de la **Loi 2022-30 relative à la protection des données personnelles**. Les documents papier essentiels (formulaires d'ouverture, attestations signées, copies de pièces d'identité) sont numérisés puis archivés physiquement dans un centre de conservation agréé.

L'accès aux archives est strictement limité : seul le personnel autorisé de la Conformité, de l'Audit Interne et de la Direction Juridique peut consulter les données, et uniquement à des fins de contrôle ou d'enquête. Chaque consultation est enregistrée dans un journal d'accès horodaté.

Les délais légaux de conservation peuvent être prolongés sur demande expresse de la CTAF, de la BCT ou de l'autorité judiciaire. À l'expiration du délai, les données sont détruites de manière sécurisée selon une procédure de purge validée par le Responsable Sécurité SI.

Tableau 4 – Durées de conservation applicables

Type de document	Support principal	Durée minimale	Responsable de conservation
Dossier KYC initial	Numérique + Papier	10 ans	Direction Conformité
Revue périodique KYC	Numérique	10 ans après mise à jour	Responsable Agence
Déclaration DOS	Numérique chiffré	10 ans après clôture	LCB-FT Officer

Type de document	Support principal	Durée minimale	Responsable de conservation
Journal d'accès aux données	Numérique	5 ans	Sécurité SI

---

9. Coopération interbancaire et reporting BCT

FinSight Bank reconnaît que la lutte contre le blanchiment et le financement du terrorisme dépasse le cadre d'une seule institution. La coopération interbancaire et la transparence envers les autorités de régulation constituent des obligations essentielles.

La Banque entretient un **canal de communication permanent** avec la **Banque Centrale de Tunisie**, la **CTAF** et les autres établissements de crédit via la plateforme sécurisée *AML Exchange Portal*. Ce système permet l'échange rapide d'alertes, de bonnes pratiques et d'informations sur les typologies émergentes.

Les rapports périodiques transmis à la BCT comprennent : le **rapport semestriel LCB-FT**, les **statistiques de DOS**, les **listes des formations réalisées** et le **suivi des recommandations d'audit**. Ces documents sont validés par le Comité Conformité et signés électroniquement par la Direction Générale avant transmission.

FinSight Bank participe activement aux **groupes de travail sectoriels** pilotés par la BCT et la CTAF afin de renforcer la cohérence du dispositif national. Elle coopère également avec les autorités judiciaires dans le respect du secret professionnel prévu par l'article 110 du Code Bancaire.

Tout refus injustifié de collaboration ou tout retard dans la communication d'informations sensibles constitue une faute grave susceptible de sanctions disciplinaires et réglementaires.

Tableau 5 – Obligations de reporting et coopération

Autorité destinataire	Fréquence	Contenu du rapport	Mode de transmission
Banque Centrale de Tunisie	Semestrielle	États LCB-FT + DOS + Formations	AML Exchange Portal
CTAF	À chaque DOS	Fiche de déclaration + pièces	Canal sécurisé CTAF

Autorité destinataire	Fréquence	Contenu du rapport	Mode de transmission
Autorités judiciaires	À la demande	Informations ciblées	Courrier confidentiel

---

10. Dispositions finales

La présente procédure entre en vigueur le **1er janvier 2025**. Elle annule et remplace toutes versions antérieures relatives au dispositif KYC et LCB-FT. Son application est obligatoire pour l'ensemble du personnel, quel que soit le niveau hiérarchique ou la fonction exercée.

La **Direction Conformité** est responsable de la diffusion, du suivi et de la mise à jour annuelle du document. Toute évolution réglementaire ou recommandation de la BCT, de la CTAF ou du GAFI doit être intégrée sans délai.

Les manquements constatés dans l'application de la présente procédure font l'objet de mesures correctives immédiates. Les récidives ou comportements délibérés de non-conformité peuvent entraîner des sanctions disciplinaires, voire pénales, conformément à la législation en vigueur.

Un exemplaire officiel de cette procédure est conservé au siège de FinSight Bank et disponible en version électronique sur l'intranet institutionnel. Les filiales et succursales sont tenues de l'adapter à leurs spécificités locales, tout en respectant les principes généraux fixés par la Banque Mère.

La Direction Générale réaffirme son engagement à maintenir un système de contrôle interne robuste, proportionné aux risques encourus et conforme aux attentes du régulateur. La lutte contre le blanchiment et le financement du terrorisme constitue un axe prioritaire de la stratégie de conformité de FinSight Bank et un gage de confiance vis-à-vis de ses clients, partenaires et autorités de supervision.

Synthèse exécutive – Procédure KYC et Lutte Contre le Blanchiment (LCB-FT)

La *Procédure KYC et Lutte Contre le Blanchiment de Capitaux et le Financement du Terrorisme* constitue un pilier essentiel du dispositif global de conformité de **FinSight Bank**. Elle traduit la volonté de la Banque d'opérer dans un cadre rigoureux de gouvernance, de transparence et d'intégrité, conformément aux exigences de la **Banque Centrale de Tunisie**, de la **Commission Tunisienne des Analyses Financières (CTAF)** et aux recommandations du **Groupe d'Action Financière (GAFI)**.

Cette politique s'inscrit dans une approche intégrée de maîtrise des risques, où la conformité n'est plus perçue comme une contrainte réglementaire, mais comme un levier stratégique de confiance et de réputation. La vigilance KYC et le dispositif LCB-FT visent à prévenir toute utilisation abusive des produits bancaires à des fins de blanchiment d'argent, de fraude ou de financement d'activités terroristes, tout en assurant la protection des clients et la stabilité du système financier tunisien.

L'année 2025 marque pour FinSight Bank une étape décisive dans la consolidation de son cadre de conformité. L'institution a renforcé la digitalisation de ses processus de vigilance à travers l'implémentation de la suite technologique *FinSight AML-Suite*, intégrant le scoring automatique des risques clients, le suivi temps réel des transactions et la déclaration électronique des opérations suspectes. Ce dispositif centralisé garantit la traçabilité complète des contrôles, l'uniformisation des pratiques entre agences et la réduction significative des délais de traitement.

Sur le plan organisationnel, la Banque a consolidé son dispositif de **gouvernance LCB-FT** autour de quatre axes :

1. **Une responsabilité clairement établie** du Responsable Conformité LCB-FT, agissant sous l'autorité directe de la Direction Générale et du Conseil d'Administration ;

2. **Une coordination renforcée** entre les fonctions Conformité, Audit Interne et Sécurité Systèmes d'Information, assurant une couverture complète des lignes de défense ;

3. **Une montée en compétence continue** du personnel via un plan de formation obligatoire et certifiant couvrant toutes les fonctions sensibles ;

4. **Une coopération institutionnelle active** avec la BCT, la CTAF et les organismes partenaires du secteur bancaire.

Sur le plan opérationnel, la mise en œuvre du principe de *"Connaissance approfondie du client"* constitue le socle de toute relation d'affaires. L'identification systématique du client, la vérification de son bénéficiaire effectif et la compréhension de l'origine des fonds précèdent désormais tout engagement commercial. Les procédures d'évaluation du risque client, basées sur un modèle de classification triaxiale (faible, moyen, élevé), assurent un

suivi proportionné du niveau de vigilance, avec des revues périodiques à 12, 6 ou 3 mois selon la criticité.

Les systèmes de *transaction monitoring* ont permis d'améliorer la détection des typologies suspectes : virements récurrents non justifiés vers des zones offshore, transferts circulaires entre sociétés liées, flux non cohérents avec le profil économique du client. Les résultats du programme de surveillance sont consolidés dans un **rapport LCB-FT semestriel** transmis à la Banque Centrale et à la CTAF, contribuant à la transparence du dispositif national de lutte contre le blanchiment.

FinSight Bank considère que la conformité LCB-FT n'est pas un simple cadre procédural, mais une **valeur culturelle** ancrée dans le quotidien de ses collaborateurs. La politique de *tolérance zéro* à l'égard des pratiques non conformes s'accompagne d'un engagement fort pour la formation, la communication interne et la sensibilisation éthique.

Les résultats attendus à horizon 2025-2026 portent sur :

- le maintien d'un taux de conformité KYC supérieur à **98 %** sur l'ensemble du portefeuille clients ;
- la réduction de **30 %** du délai moyen de traitement des alertes ;
- l'atteinte d'un taux de couverture de **100 %** des collaborateurs formés ;
- et la transmission systématique des rapports réglementaires dans les délais impartis par la BCT et la CTAF.

Sur le plan de la gouvernance, le **Conseil d'Administration** réaffirme son rôle central dans la supervision du dispositif et s'engage à garantir les moyens humains, techniques et financiers nécessaires à son efficacité. La **Direction Générale** veille, quant à elle, à la mise à jour permanente des procédures et à l'intégration des nouvelles exigences internationales.

En conclusion, la *Procédure KYC et LCB-FT* illustre la maturité de FinSight Bank en matière de conformité et de gestion des risques. Elle incarne la conviction que **la confiance se construit par la rigueur, la transparence et la responsabilité partagée**. En alignant son dispositif sur les standards les plus exigeants, FinSight Bank renforce sa position d'institution financière exemplaire au service d'un système bancaire tunisien solide, éthique et durable.