

ACSI CONGO | FINTRAX

Rapport d'acceptation et d'audit de sécurité

Date de génération : 2026-10-27T15:18:48.338Z

Source : Plan de vérification de sécurité FinTraX (classeur fourni)

Périmètre : sécurité technique, infrastructure, interconnexions, continuité, applications; fonctionnalités métier exclues selon le classeur.

Synthèse et limites

Contrôles annoncés dans la synthèse : 110 | Contrôles effectivement détaillés : 94

Conformes : 0 | Partiels : 0 | Non conformes : 0 | Non vérifiés : 94 | N/A : 0

P1 sans validation humaine : 73 | Constats graves ouverts : 0

Score sur contrôles revus (pondération P1=3, P2=1) : Non calculable. Ce score ne mesure pas les contrôles non vérifiés.

DÉCISION : AVIS NON DÉLIVRABLE / RÉSERVES À LEVER. Une décision d'acceptation nécessite une signature externe.

Détail des contrôles

FTX-001 • Analyse et traitement de risques [P1]

Les risques de sécurité et dérogations sont-ils enregistrés et acceptés par l'ARTF ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-002 • Matrice des flux [P1]

La matrice de flux finale contient-elle toutes les communications autorisées et leurs paramètres exacts ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-003 • Sauvegardes 3-2-1 [P1]

La stratégie de sauvegarde respecte-t-elle l'objectif 3-2-1 lorsque réalisable ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-004 • Protection des backups [P1]

Les sauvegardes sont-elles protégées contre consultation, modification, suppression et rançongiciel ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-005 • Scénarios de reprise [P1]

Les scénarios de perte d'hôte, VM, DB, SAN, pare-feu et site sont-ils couverts ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-006 • Alimentation [P2]

L'alimentation, les UPS et les batteries sont-ils supervisés et testés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-007 • Incendie et environnement [P1]

La salle serveur dispose-t-elle de protections incendie, climatisation et surveillance environnementale ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-008 • Accès physique [P1]

L'accès au CTI, à la salle serveur et aux supports est-il limité et enregistré ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-009 • Non-exposition Internet [P1]

Aucun service de production FinTraX n'est-il directement exposé à Internet ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-010 • Double pare-feu [P1]

Les deux niveaux de filtrage CTI puis production sont-ils réellement indépendants et actifs ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-011 • Deny by default [P1]

Le filtrage inter-zones applique-t-il un refus par défaut ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-012 • VLAN et zones [P1]

Les zones Production, DB, Administration, Corpo/NOC, stockage et transit sont-elles isolées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-013 • Accès base de données [P1]

Les bases Core et DIT sont-elles accessibles uniquement depuis les composants autorisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-014 • Reverse proxy [P1]

Les backends applicatifs sont-ils inaccessibles directement hors du reverse proxy ou des flux explicitement autorisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-015 • Administration [P1]

Les interfaces d'administration sont-elles isolées du trafic utilisateur et des assujettis ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-016 • Flux OneBox-CTI [P1]

Le flux OneBox vers CTI est-il limité à la liaison privée cible ou au mécanisme transitoire approuvé ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-017 • Twingate [P1]

L'usage transitoire de Twingate est-il borné, contrôlé et suivi jusqu'à son retrait ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-018 • WireGuard [P2]

Les interconnexions WireGuard éventuelles respectent-elles la matrice de flux et une gestion sûre des clés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-019 • DNS interne [P2]

Les zones DNS internes et leurs transferts sont-ils limités aux serveurs autorisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-020 • Protocoles sûrs [P1]

Les protocoles d'administration et d'échange non chiffrés sont-ils désactivés ou justifiés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-021 • Équipements réseau [P1]

Les équipements réseau et de sécurité sont-ils durcis et leurs plans de management isolés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-022 • Journalisation réseau [P1]

Les pare-feu et équipements réseau envoient-ils leurs journaux vers un stockage central protégé ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-023 • Comptes nominatifs [P1]

Les comptes humains d'administration et d'exploitation sont-ils nominatifs ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-024 • MFA [P1]

L'authentification multifacteur est-elle activée pour les accès privilégiés et distants ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-025 • RBAC [P1]

Les rôles et droits applicatifs/techniques suivent-ils le moindre privilège ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-026 • Comptes techniques [P1]

Les comptes de service sont-ils dédiés, limités et sans connexion interactive inutile ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-027 • Cycle de vie [P2]

Les créations, changements et suppressions d'accès sont-ils approuvés et exécutés rapidement ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-028 • Comptes d'urgence [P2]

Les comptes de secours sont-ils protégés et leur utilisation détectée ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-029 • Sessions [P2]

Les sessions administratives et applicatives sont-elles protégées contre l'abus ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-030 • Revue périodique [P2]

Une revue périodique des habilitations est-elle réalisée et signée ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-031 • API et interfaces [P1]

Toutes les API/interfaces sont-elles inventoriées, authentifiées et autorisées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-032 • Validation entrées [P1]

Les données reçues par API, SFTP et OneBox sont-elles validées côté serveur ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-033 • Contrôle d'accès objet [P1]

Les utilisateurs ne peuvent-ils accéder qu'aux ressources autorisées (IDOR/BOLA) ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-034 • Injection [P1]

Les interfaces résistent-elles aux injections courantes et à la manipulation des requêtes ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-035 • Erreurs [P2]

Les erreurs applicatives ne divulguent-elles pas de secrets, chemins, requêtes SQL ou détails internes ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-036 • Limitation de débit [P2]

Les API et points d'entrée sont-ils protégés contre l'abus et l'épuisement de ressources ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-037 • CORS et en-têtes [P2]

Les configurations web appliquent-elles des en-têtes et politiques navigateur adaptés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-038 • Upload et fichiers [P1]

Les fichiers reçus sont-ils contrôlés avant traitement et stockage ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-039 • Dépendances runtime [P1]

Les dépendances chargées en production sont-elles cohérentes avec les versions approuvées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-040 • Configuration sûre [P1]

Les paramètres applicatifs dangereux sont-ils désactivés en production ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-041 • Séparation des fonctions [P1]

Les fonctions d'exploitation et d'administration technique sont-elles séparées dans l'application ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-042 • Traçabilité transaction technique [P1]

Les opérations sensibles sont-elles attribuables à une identité et à une corrélation de bout en bout ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-043 • Résilience [P1]

Les erreurs de dépendance ne provoquent-elles pas des contournements de sécurité ou des pertes silencieuses ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-044 • OneBox durcissement [P1]

La OneBox est-elle durcie, administrée de façon sûre et limitée au rôle de collecte ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-045 • Mode dégradé OneBox [P1]

Le mode dégradé et la synchronisation différée protègent-ils les données en attente ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-046 • Kafka [P1]

Kafka est-il isolé et protégé par authentification, ACL et chiffrement adaptés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-047 • Kafka messages [P1]

Les messages Kafka sont-ils contrôlés contre accès abusif, rejeu et exposition excessive ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-048 • Reverse proxy [P1]

Le reverse proxy est-il durci et configuré pour les seuls services autorisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-049 • Dépôts de code [P1]

Les dépôts Git de production sont-ils protégés contre les modifications non autorisées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-050 • Images et dépôts [P1]

Les images système et conteneurs proviennent-ils de sources autorisées et maintenues ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-051 • HMAC [P1]

L'utilisation de HMAC-SHA256 et du secret DIT_HMAC_SECRET est-elle conforme au modèle documenté ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-052 • Rotation HMAC [P1]

La rotation du secret HMAC est-elle planifiée avec stratégie de ré-hachage et de compatibilité ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-053 • Gestion des clés [P1]

Les clés et secrets sont-ils stockés hors du code et des fichiers accessibles largement ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-054 • Certificats [P2]

Les certificats sont-ils inventoriés, valides, renouvelables et leurs clés privées protégées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-055 • HMAC et pseudonymisation [P1]

Les valeurs HMAC, fingerprints et valeurs masquées ne permettent-elles pas d'exposer des données par les logs ou exports ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-056 • Intégrité et preuves [P1]

Les preuves, claims et événements critiques sont-ils protégés contre altération et suppression non détectées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-057 • Rétention et purge [P2]

La rétention et la suppression des données sont-elles définies et techniquement appliquées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-058 • Séparation des magasins [P1]

Les magasins Core, DIT, pDIT et KYC local/central respectent-ils la séparation de responsabilités ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-059 • Accès DBA [P1]

Les accès privilégiés aux bases sont-ils limités, nominatifs et auditables ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-060 • Inventaire Proxmox [P1]

Les huit hôtes Proxmox et les clusters sont-ils inventoriés, maintenus et alignés avec l'architecture ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-061 • Durcissement hyperviseur [P1]

Les hôtes Proxmox sont-ils durcis et les interfaces de gestion isolées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-062 • Séparation VM [P1]

Les VM de production et de support ne peuvent-elles pas communiquer au-delà des flux nécessaires ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-063 • Systèmes invités [P1]

Les OS invités sont-ils durcis, patchés et supervisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-064 • Snapshots [P2]

Les snapshots et images de VM sont-ils contrôlés et ne remplacent-ils pas les sauvegardes ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-065 • Accès console [P2]

L'accès console aux VM est-il restreint et journalisé ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-066 • Services techniques [P1]

Les services techniques (Git, images build, documentation, password management) sont-ils isolés et sécurisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-067 • NTP et temps [P2]

Les systèmes utilisent-ils une source de temps cohérente et surveillée ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-068 • Durcissement DB [P1]

Les moteurs de bases de données sont-ils durcis et limités aux fonctionnalités nécessaires ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-069 • Comptes DB applicatifs [P1]

Chaque application utilise-t-elle un compte DB dédié avec des droits limités ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-070 • Audit DB [P1]

Les opérations sensibles des bases sont-elles journalisées et surveillées ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-071 • SAN et zoning [P1]

Le SAN HPE MSA 2060 et le Fibre Channel sont-ils isolés et limités aux hôtes autorisés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-072 • Multipath [P2]

Le multipath et les chemins redondants sont-ils opérationnels et testés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-073 • Chiffrement SAN [P2]

Les données stockées sur SAN et supports de sauvegarde sont-elles protégées contre l'accès non autorisé ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-074 • Séparation sauvegardes [P1]

Les sauvegardes sont-elles indépendantes du domaine de panne et de compromission de la production ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-075 • Restauration [P1]

Les restaurations ont-elles été testées avec validation du service reconstruit ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-076 • RPO/RTO [P1]

Les RPO/RTO sont-ils définis, approuvés et démontrés par les tests ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-077 • HA et quorum [P1]

La haute disponibilité Proxmox, le quorum et le comportement lors de perte de nœud sont-ils testés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-078 • PRA multisite [P1]

Les limites de la HA locale et la reprise après perte du site sont-elles traitées par un PRA testé ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-089 • Couverture supervision [P1]

La supervision couvre-t-elle tous les composants critiques et leurs dépendances ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-090 • Alertes de sécurité [P1]

Les événements de sécurité déclenchent-ils des alertes exploitables ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-091 • Centralisation des logs [P1]

Les logs applicatifs, systèmes, réseau, bases et OneBox sont-ils centralisés avec accès protégé ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-092 • Contenu des logs [P1]

Les journaux évitent-ils d'enregistrer mots de passe, secrets et identifiants bruts ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-093 • Rétention des logs [P2]

La rétention et la protection des journaux permettent-elles une investigation rétrospective ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-094 • Procédure incident [P1]

La procédure FINTRAX-SEC-INC-001 est-elle disponible, approuvée et exercée ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-095 • Gestion des incidents [P2]

Les incidents et demandes sont-ils suivis de bout en bout dans l'outil prévu ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-096 • Détection de dérive [P1]

Les changements critiques de configuration et les écarts à la baseline sont-ils détectés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-097 • Synchronisation horaire [P2]

Les horodatages permettent-ils de corréler un incident entre OneBox, réseau, Kafka, Core, DIT et bases ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-098 • Playbooks [P2]

Les scénarios de compromission de compte, malware, exfiltration et indisponibilité disposent-ils de consignes ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-099 • Scan de vulnérabilités [P1]

Les hôtes, applications, API, images et dépendances sont-ils couverts par une gestion périodique des vulnérabilités ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-100 • Priorisation CVE [P1]

Les vulnérabilités sont-elles priorisées selon exploitabilité, exposition, criticité et impact ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-101 • Correctifs [P1]

Les correctifs OS, hyperviseur, bases, Kafka, proxy et applications sont-ils planifiés et vérifiés ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-102 • Changements [P1]

Les changements de production sont-ils autorisés, testés, traçables et réversibles ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-103 • Tests sécurité préproduction [P1]

Les changements sont-ils testés en environnement séparé avant mise en production ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

FTX-104 • Pentest [P1]

Un test d'intrusion technique récent et autorisé couvre-t-il les frontières et composants critiques ?

Statut : Non vérifié | Score : N/A / 4 | Validé par : Non validé

Registre des constats

Référentiels

Document source — FINTRAX-ARCH-001 — Dossier d'Architecture Technique HLD/LLD v1.0, 09/09/2026

Document source — §3-§4 — Architecture fonctionnelle et physique CTI

Document source — §5-§6 — Réseau et architecture de sécurité

Document source — §7-§8 — Architecture applicative et OneBox

Document source — §9 — Interconnexion des assujettis

Document source — §10.B — Données DIT

Document source — §12-§13 — Stockage, continuité et supervision

Document source — §14-§19 — LLD, hôtes, services et validation

Contrôle complémentaire — Chaîne d'approvisionnement logicielle

Méthode — Cycle de contrôle

Échelle de priorité — P1

Échelle de priorité — P2

Statuts — Non vérifié / En cours / Conforme / Partiellement conforme / Non conforme / Non applicable

Limite d'utilisation — Avis de sécurité

Réserves de méthode

Analyse IA non probante en elle-même. Les réponses humaines, preuves horodatées, résultats de tests et revues autorisées priment. La vérification de l'intégralité du périmètre demeure nécessaire.

