TOTEM

POLITIQUE DE LUTTE CONTRE LA FRAUDE

TOTEM France
Edition septembre 2024

Politique de lutte contre la fraude

Introduction

La fraude représente un défi majeur pour notre entreprise, puisqu'elle engage potentiellement des pertes financières significatives, une atteinte à notre réputation et une dégradation de la confiance de nos parties prenantes et en premier lieu nos clients et les bailleurs qui nous font confiance. Dans un environnement économique en constante évolution, il est impératif de mettre en place des mécanismes robustes pour prévenir, identifier et traiter les comportements frauduleux.

Cette politique de lutte contre la fraude a pour objectif de :

- Prévenir la Fraude : établir des contrôles internes solides et des procédures claires pour minimiser les risques de fraude. Cela inclut la formation des employés sur les comportements éthiques et les signaux d'alerte.
- Détecter la Fraude : mettre en œuvre des systèmes de surveillance et d'audit réguliers pour identifier rapidement toute activité suspecte. Des outils technologiques peuvent également être utilisés pour renforcer cette détection.
- Réagir à la Fraude : définir des protocoles clairs pour la gestion des incidents de fraude, y compris des procédures d'enquête et des mesures disciplinaires appropriées.
- Promouvoir une Culture d'Éthique : encourager un environnement de travail où l'intégrité est valorisée et où les employés se sentent en sécurité pour signaler des comportements inappropriés sans crainte de représailles.

En adoptant cette politique, nous affirmons notre engagement envers la transparence, la responsabilité et la conformité légale. Nous croyons fermement qu'une approche proactive et collective est essentielle pour protéger notre organisation et ses valeurs fondamentales.

Thierry PAPIN
Président de TOTEM France

Signé par **Thierry PAPIN** le
14/10/2024 11:24

Table des matières

I. Qu'est-ce que la Fraude ? Définitions et rappels

La distinction entre fraudes internes et externes est importante car les mécanismes de prévention, de détection et de réaction peuvent varier en fonction de la source de la fraude.

TOTEM met en place des politiques et des contrôles appropriés pour se protéger contre les deux types de fraudes.

1. Fraudes internes

La fraude interne est commise par des personnes internes à l'entreprise au détriment de l'entreprise ou en pensant agir "à son avantage". Qu'elle soit intentionnellement faite au détriment de l'entreprise ou à « son avantage », elle est nuisible à l'entreprise.

1. Fraude comptable : Les employés ou les gestionnaires manipulent frauduleusement les données financières de l'entreprise. Cela implique la manipulation délibérée des informations financières de l'entreprise pour dissimuler des pertes, augmenter les bénéfices ou tromper les investisseurs. Les exemples incluent la surévaluation des actifs, la sous-évaluation des passifs, la comptabilisation de revenus fictifs, etc.
2. Fraude fiscale : Les employés ou la direction falsifient les déclarations fiscales de l'entreprise. Cela peut inclure la sous-déclaration des revenus, la surdéclaration des dépenses, l'utilisation abusive de crédits fiscaux, etc.
3. Fraude à la paie : Les employés ou les gestionnaires manipulent les informations de paie pour créer des employés fictifs ou détourner des fonds de la masse salariale.
4. Fraude à l'approvisionnement : Les employés ou les fournisseurs sont impliqués dans des activités frauduleuses liées aux achats. Les employés seuls ou en complicité avec les fournisseurs peuvent surévaluer des biens ou des services fournis à l'entreprise, facturer pour des biens ou services non fournis, ou être impliqués dans d'autres activités frauduleuses liées aux achats.
5. Fraude par détournement d'actifs : Les employés détournent des biens ou des fonds de l'entreprise à des fins personnelles que ce soit de l'argent liquide, des équipements ou d'autres biens de valeur.
6. Fraude par détournement de données : Les employés manipulent ou volent des données sensibles de l'entreprise. Cela implique la violation par des acteurs internes de la sécurité des données de l'entreprise pour accéder à des informations sensibles, telles que des informations client ou financières, en vue de les exploiter ou de les vendre.

2. Fraudes externes

La fraude externe est commise par des personnes extérieures à l'entreprise et au détriment de l'entreprise.

1. Fraude à l'approvisionnement : Les fournisseurs seuls ou en complicité avec des salariés ou représentants de l'entreprise peuvent surévaluer des biens ou des services fournis à l'entreprise, facturer pour des biens ou services non fournis, ou être impliqués dans d'autres activités frauduleuses liées aux achats.
2. Fraude par virement bancaire : Les fraudeurs cherchent à tromper les employés de l'entreprise pour qu'ils effectuent des virements bancaires frauduleux vers des comptes contrôlés par les escrocs. Dans ce type de fraude on retrouve
    - La fraude dite "fraude au Président" : le fraudeur envoie un message supposé venir du Président ou d'un directeur, demandant un service, un virement, ….
    - La fraude aux coordonnées bancaires : demande frauduleuse de changement de coordonnées bancaires d'un fournisseur.

4. Fraude à la carte de crédit : Des individus externes utilisent des cartes de crédit volées ou frauduleuses pour effectuer des transactions non autorisées. Les entreprises qui traitent des paiements par carte de crédit peuvent être victimes de fraude lorsque des transactions non autorisées sont effectuées à l'aide de cartes de crédit volées ou frauduleuses
5. Fraude en ligne : Des cybercriminels externes utilisent des tactiques telles que le phishing, la fraude par des faux sites Web ou les attaques de ransomware pour extorquer de l'argent à l'entreprise.
6. Fraude en matière de propriété intellectuelle : Des tiers enfreignent la propriété intellectuelle de l'entreprise, comme les brevets, les marques commerciales ou les droits d'auteur.
7. Fraude par détournement de données : Des personnes externes manipulent ou volent des données sensibles de l'entreprise. Cela implique la violation par des acteurs externes de la sécurité des données de l'entreprise pour accéder à des informations sensibles, telles que des informations client ou financières, en vue de les exploiter ou de les vendre

II. Les risques de Fraude chez TOTEM

Cartographie des risques Fraude chez TOTEM France.

1. Les risques rattachés à la fraude

1.1. Fraude interne

1. R1 - Fraude comptable (manipulation de données financières pour dissimuler des pertes, augmenter les bénéfices, etc.)
2. R2 - Fraudes fiscales et financières (carrousel TVA, falsification des déclarations fiscales, fraude à l'assurance, …)
3. R3 - Fraudes dans les processus : notes de frais, voyages, approvisionnements, paie, recrutement, détournement d'actifs, carburant, …
4. R4 - Détournement de données (par les employés pour les exploiter ou les vendre)

1.2. Fraude externe

1. R5 - Fraude Fournisseurs : déploiement de site, surfacturation par les fournisseurs, …
2. R6 - Fraude à l'identité (président, virement bancaire, carte de crédit, ingénierie sociale, …)
3. R7 - Fraude par détournement de données (cyber-attaque, …)

2. Les causes

Les facteurs identifiés comme pouvant générer la fraude ou aggraver le risque de fraude sont :

- L'opportunité
  - L'entreprise dispose de processus opérationnels ou support inadaptés : cumul de tâches incompatibles, absence de supervision / contrôles, faille de sécurité, …
  - Les processus n'ont pas intégré des tâches de supervision ou de contrôle.
  - Les processus ne sont pas optimisés et sont complexes, ce qui conduit à ce que les opérationnels ne le suivent pas.
  - Les processus ne sont pas suivis.

- Inefficacité du programme de prévention : pour défaut de design, manque ou absence de gouvernance, un scope de déploiement insuffisant, absence de maturité des dispositifs de couverture.
- Non engagement du management : en ne passant pas des messages clairs, en ne montrant pas l'exemple, ou en affichant une distance par rapport aux actions de réduction du risque qui pourraient être vues comme inutiles.
- Non-respect du programme antifraude : le programme mis en place n'est pas suivi ou est suivi mais de façon incomplète.
- Défaillance des processus de KYC (Know Your Customer) : absence de Due Diligences sur les fournisseurs, bailleurs institutionnels et sous-traitants et non détection des risques en amont à la contractualisation.
- Défaillance des dispositifs de contrôle interne : non détection de la fraude pour cause de contrôles mal conçus ou non déroulés.
- Prise de contrôle par un hacker / cyberattaque : pour insuffisance de protection et aussi de sensibilisation des utilisateurs.
- Atteinte à l'intégrité et à la confidentialité des données et informations : pour insuffisance de protection et aussi de sensibilisation des utilisateurs.
- Comportement individuel : pression et rationalisation, arrogance, management override sont des comportements qui peuvent conduire à créer un ressenti envers l'entreprise, sentiment qui peut conduire à accroître le risque de fraude chez les personnes mécontentes.
- Conflit d'intérêt / collusion : conflits d'intérêts non déclarés et / ou mal gérés.
- Délit d'initié.
- Contournement des règles de délégation : qui peuvent conduire à des validations indues par des personnes n'ayant pas la légitimité.
- Non séparation des tâches : ce qui conduit à l'absence d'un contrôle par un tiers et à ce qu'une seule personne puisse prendre des décisions potentiellement nocives pour l'entreprise et les valider.
- Crise macroéconomique / inflation : augmente le risque de fraude dans l'espoir de compenser la baisse des revenus.

L'action sur les causes, contribue à abaisser la probabilité d'occurrence d'une fraude.

3. Les conséquences de la fraude

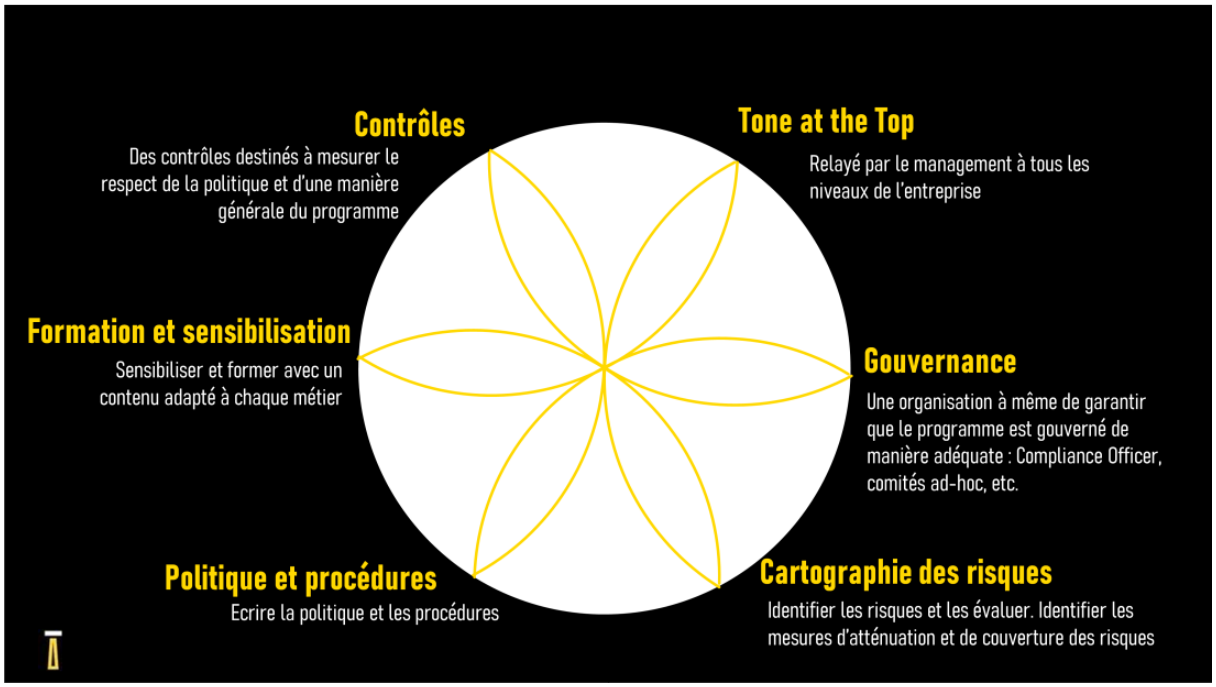
- Dégradation de services / interruption d'activité : lorsque la fraude conduit à une baisse de qualité.
- Préjudice financier (réduction des marges) : dépenses indues, détournements, revenus en baisse, …
- Condamnations civiles ou pénales (amendes, peines d'emprisonnement, …)
- Non certification / Réserves sur les comptes.
- Perte de confiance des parties prenantes (actionnaires, investisseurs, clients, fournisseurs, collaborateurs, …)
- Crise de liquidités.
- Crise de gouvernance.
- Atteinte à l'image et la réputation.

III. La démarche de gestion du risque de la fraude

La promotion d'une culture d'éthique au sein de TOTEM est essentielle pour garantir l'intégrité, la transparence et la responsabilité dans toutes nos actions. Une culture d'éthique forte non seulement protège notre réputation, mais favorise également un environnement de travail positif et productif. Voici les éléments clés pour instaurer et maintenir cette culture.

La prévention de la fraude comprend un ensemble de mesures et de stratégies visant à réduire le risque de fraude au sein de TOTEM. Il est crucial de prendre des mesures proactives pour prévenir la fraude dans la mesure où elle peut entraîner des conséquences importantes financières et de réputation.

La prévention de la fraude chez TOTEM s'appuie sur 6 piliers.



1. Engagement de la Direction :

Engagement de l'instance dirigeante par une volonté affichée et relayée par le management à tous les niveaux de l'entreprise.

La direction doit démontrer un engagement clair envers l'éthique en intégrant des valeurs éthiques dans la vision et la mission de l'organisation. Cela inclut :

- Modèle de Comportement : les membres du comité de directions et les managers doivent agir en tant que modèles en respectant les normes éthiques et en prenant des décisions basées sur des principes éthiques.
- Communication Transparente : partager régulièrement des messages sur l'importance de l'éthique et des comportements attendus.

2. Gouvernance & moyens

- Mise en place une organisation à même de garantir que le programme est gouverné de manière adéquate.

- Désignation d'une personne chargée de superviser les efforts de prévention de la fraude, d'évaluer en permanence les risques, de mettre à jour les stratégies de prévention et d'enquêter sur les suspicions de fraude et en lui donnant les moyens d'atteindre les objectifs.

3. Évaluation des risques de fraude

Évaluation approfondie des vulnérabilités de notre organisation à la fraude. Identifier les domaines où la fraude est la plus susceptible de se produire, tels que les transactions financières, les achats, les salaires ou le traitement des données.

- Identifier les risques de fraude et les évaluer sous les angles de la probabilité et de l'impact.
- Identifier les mesures de couverture de risque ou d'atténuation à mettre en place.

L'évaluation est à mettre à jour annuellement.

4. Politiques claires et accessibles

Établir des politiques éthiques claires et accessibles à tous les employés est crucial :

- Code de Conduite : élaborer un code de conduite qui définit les attentes en matière de comportement éthique et les conséquences en cas de non-respect.
- Procédures de Signalement : mettre en place des procédures simples et sécurisées pour signaler des comportements contraires à l'éthique, garantissant l'anonymat et la protection contre les représailles.
- Déclaration des conflits d'intérêt : selon le cas exiger une déclaration relative à la présence ou l'absence de conflit d'intérêt pour certaines fonctions ou pour certaines personnes au cas par cas sur des projets bien spécifiques

5. Formation et sensibilisation

Sensibilisation des employés aux risques de fraude et à l'importance d'un comportement éthique. Ils doivent connaître les mécanismes de fraude les plus courants et savoir comment signaler les activités suspectes au sein de l'entreprise. La sensibilisation se fait à deux niveaux. Sensibilisation basique pour tous complétée de formations ciblées qui adresse les risques posés à chaque typologie de collaborateurs. L'identification des formations à proposer à chaque population s'appuie sur l'évaluation des risques. Pour que tous les employés comprennent et adoptent les valeurs éthiques, des programmes de formation réguliers doivent être mis en place :

- Accueil des nouveaux arrivants : intégrer la sensibilisation à la fraude dans les formations obligatoires faites aux nouveaux arrivants. Y insister sur l'importance de traiter et gérer les dilemmes éthiques, les lois et règlements applicables, ainsi que sur les comportements appropriés.
- Communiquer régulièrement et selon l'actualité : pour maintenir un niveau de sensibilisation en adéquation avec les risques.
- Ressources Éducatives : fournir des ressources, telles que des guides et des études de cas, pour aider les employés à naviguer dans des situations éthiques complexes.

6. Contrôles

Mettre en place les contrôles destiner à mesurer l'efficacité du programme et les axes d'amélioration possibles.

- Contrôles internes : mettre en place des contrôles internes solides et une séparation des tâches. Cela signifie qu'aucun employé ne doit avoir un contrôle absolu sur une fonction

financière ou opérationnelle essentielle. Par exemple, différentes personnes doivent être responsables de l'approbation et du rapprochement des transactions financières.

- Audits et rapprochements réguliers : effectuer régulièrement des audits internes et externes afin d'identifier les divergences et les irrégularités. Il s'agit notamment d'audits financiers, d'audits de la sécurité informatique et d'audits des marchés publics. Rapprocher les registres financiers afin d'en garantir l'exactitude.
- Diligence raisonnable (Due Diligence) à l'égard des tiers : réaliser des Due Diligences en préalable à toute nouvelle contractualisation avec un bailleur, fournisseur, sous-traitant pour vérifier leur légitimité et leur intégrité. Des processus et des contrôles clairs en matière de passation de marchés afin d'éviter les facturations frauduleuses ou les surfacturations.
- Sécurité des données : protéger les données sensibles, y compris les informations sur les clients et les bailleurs et les dossiers financiers, grâce à des mesures de cybersécurité solides. Mettre en place des pares-feux, un système de cryptage, des contrôles d'accès et une formation des employés pour éviter les violations de données.
- Surveillance et analyse : utiliser des outils avancés d'analyse et de surveillance des données pour détecter les anomalies et les schémas indiquant une fraude. Cela peut aider à identifier les activités frauduleuses en temps réel ou lors d'examens réguliers.
- Conformité aux réglementations : veiller à ce que TOTEM respecte les lois et réglementations relatives à la prévention de la fraude, telles que les lois contre le blanchiment d'argent (AML) et la corruption.

Ce 6 piliers sont complétés par une démarche d'amélioration continue partant du principe que la prévention de la fraude est un processus continu. Nous encourageons la communication ouverte et évaluons et mettons régulièrement à jour les mesures de prévention de la fraude pour nous adapter à l'évolution des risques et aux nouvelles menaces.

- Encouragement de la communication ouverte

Favoriser un environnement où les employés se sentent à l'aise de discuter d'éthique et de poser des questions :

  - Canaux de Communication : créer des canaux de communication ouverts, tels que des réunions régulières ou des séances d'échanges, pour aborder les préoccupations éthiques.
  - Feedback Constructif : encourager les salariés à donner leur avis sur les pratiques éthiques et à suggérer des améliorations.

- Évaluation continue

La culture d'éthique doit être régulièrement évaluée et améliorée :

  - Sondages et évaluations : réaliser des sondages pour mesurer la perception des employés concernant l'éthique au sein de l'organisation.
  - Révisions des politiques : adapter les politiques et les formations en fonction des retours d'expérience et des évolutions réglementaires.

IV. Détection et traitement de la fraude

1. Détection de la fraude

La détection de la fraude est un élément essentiel de notre politique globale de lutte contre la fraude. En adoptant une approche proactive et en impliquant tous les niveaux de l'organisation, nous pouvons renforcer notre capacité à identifier et à prévenir les actes frauduleux.

1.1. Méthodes de détection

a) Surveillance continue

- Systèmes de Contrôle Internes : mettre en place des contrôles internes rigoureux pour surveiller les transactions financières et opérationnelles.
  - Les transactions financières sont sous-traitées aux Centres de Services Partagées de notre maison mère Orange SA. Ceci garantit l'application des processus rigoureux mis en place par Orange et nous fait bénéficier des contrôles associés.
  - Contrôle des notes de frais permet de détecter d'une part les notes de frais suspectes et d'autres part les invitations faites dans le cadre des relations d'affaires qui n'ont pas respectés le processus de déclaration requis par notre politique anti-corruption.
- Audits Réguliers : effectuer des audits internes et externes périodiques pour identifier les anomalies. Ces audits sont réalisés par des auditeurs du Groupe Orange ou les Commissaires Aux Comptes dans le cadre de la certification des comptes.

b) Analyse des données

- Outils d'Analyse : utiliser des logiciels d'analyse de données pour détecter des modèles inhabituels ou des transactions suspectes. Pour TOTEM, nous avons mis en place des rapports PowerBI.
- Indicateurs de Fraude : développer une liste d'indicateurs de fraude potentiels, tels que des variations significatives dans les chiffres financiers.

c) Signalement anonyme

- Ligne de Signalement : mettre en place un système de signalement anonyme et accessible aussi bien aux internes qu'aux externes et tout tiers interagissant avec TOTEM, pour permettre de signaler des comportements suspects sans crainte de représailles. Ce
- Sensibilisation : Informer régulièrement les employés sur l'importance du signalement et les procédures à suivre. Informations intégrées dans les formations d'accueil obligatoires pour les nouveaux arrivants.

d) Formation et sensibilisation

- Formations Régulières : Organiser des sessions de formation pour sensibiliser les employés aux signes de fraude et aux méthodes de détection.
  - Sessions systématiques intégrées dans les formations d'accueil obligatoires pour les nouveaux arrivants
  - Sessions ou information ad-hoc selon le besoin et l'actualité
- Mises à Jour : Fournir des mises à jour sur les nouvelles tendances en matière de fraude et les meilleures pratiques pour les détecter.

1.2. Responsabilités

- Équipe de Conformité : Responsable de la mise en œuvre et de la supervision des mesures de détection de la fraude.
- Tous les Employés : Chaque employé a un rôle à jouer dans la détection de la fraude en restant vigilant et en signalant toute activité suspecte.

2. Réaction à la fraude

Lorsqu'un acte de fraude est suspecté ou détecté, il est impératif d'agir rapidement et de manière structurée pour minimiser les impacts négatifs sur l'organisation. Ce processus se décline en plusieurs étapes clés. En adoptant cette approche systématique et proactive, nous nous engageons à traiter les incidents de fraude avec sérieux et à protéger l'intégrité de notre organisation.

2.1. Signalement immédiat

- Notification : tout employé ayant connaissance d'un acte frauduleux doit le signaler immédiatement à l'équipe de conformité via les canaux établis, tels que la ligne de signalement anonyme.
- Documentation : le signalement doit inclure des détails précis sur l'incident, tels que la nature de la fraude, les personnes impliquées et les preuves disponibles.

2.2. Enquête préliminaire

- Évaluation Initiale : l'équipe de conformité procède à une évaluation préliminaire pour déterminer la gravité de la situation et décider si une enquête approfondie est nécessaire.
- Collecte de Preuves : des preuves doivent être collectées de manière systématique, en respectant les procédures légales, éthiques (protection du lanceur d'alerte et confidentialité), afin de garantir l'intégrité de l'enquête.

2.3. Enquête approfondie

- Équipe d'Enquête : constituer une équipe dédiée des membres de la conformité, des ressources humaines et, si nécessaire, des experts externes.
- Analyse des Données : utiliser des outils d'analyse pour examiner les transactions et les comportements suspects, afin d'identifier l'étendue de la fraude.
- Interviews : mener des entretiens avec les personnes concernées pour recueillir des témoignages et clarifier les faits.

2.4. Mesures correctives

- Actions Disciplinaires : en fonction des résultats de l'enquête, des mesures disciplinaires appropriées seront prises contre les employés impliqués, pouvant aller jusqu'au licenciement.
- Ajustements des Contrôles Internes : réviser et renforcer les contrôles internes pour prévenir la récurrence de tels incidents, en intégrant les leçons tirées de l'enquête.
- Mise à jour de la sensibilisation : réviser et mettre à jour les contenus de sensibilisation et les formations afin de tenir compte des enseignants tirés de l'incident.

2.5. Communication transparente

- Information des Parties Prenantes : informer les parties prenantes, y compris les employés, et si concernés les clients et les partenaires, des actions prises pour traiter l'incident, tout en respectant la confidentialité des personnes impliquées.

- Rapport de Synthèse : élaborer un rapport de synthèse sur l'incident, les mesures prises et les actions préventives mises en place, afin de renforcer la confiance dans notre engagement envers l'intégrité.

2.6. Suivi et Évaluation

- Suivi des Mesures : mettre en place un suivi régulier des mesures correctives pour évaluer leur efficacité et ajuster les stratégies si nécessaire.
- Formation Continue : organiser des sessions de formation pour sensibiliser les employés aux nouvelles procédures et renforcer la culture d'éthique au sein de l'organisation.