CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

CHAMBRE FRANÇAISE
DE COMMERCE ET D'INDUSTRIE
DU MAROC

L'instauration de mesures anti-fraude dans les entreprises : Prévenir & Agir »

MOUNIM ZAGHLOUL

CIA, CISA, CGEIT,CRMA,COBIT, TSPM, ITIL, ISO 20000 LI, ISO27001 LA

Casablanca, le 18 Octobre 2016

Sommaire

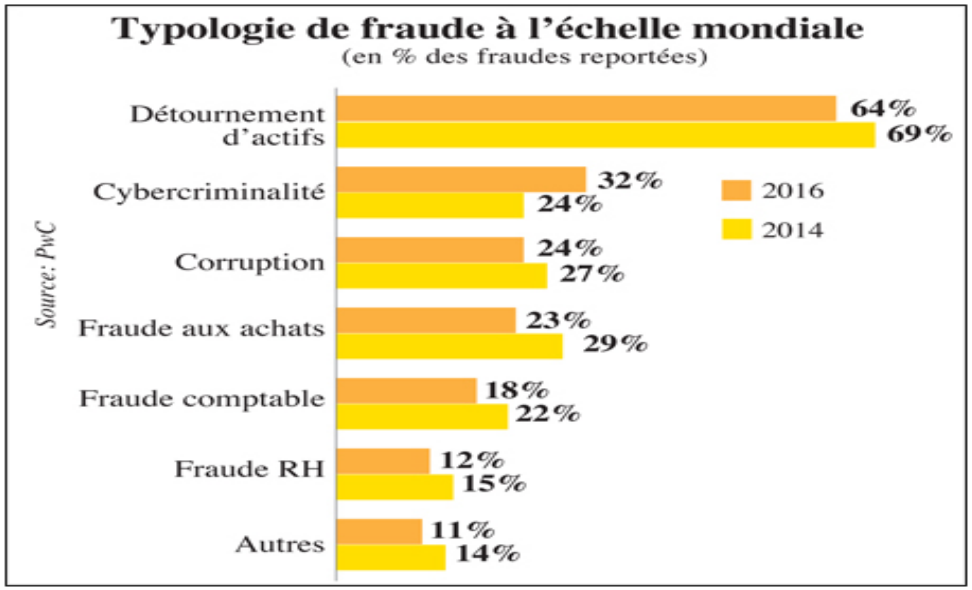
CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

- Contexte International de la Fraude
- Les Types de Fraude en Entreprise
- Les Dispositifs de contrôle interne et le risque de Fraude
- Les Nouvelles Architectures de Contrôle
- Les Dispositifs de Contrôle Continu « CCM »
- La Fraude Externe & Cybercriminalité
- Les modes opératoires (fraude au Président, Fournisseur, Banque …)

La Fraude en Entreprise

Evolution du taux de Fraude

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

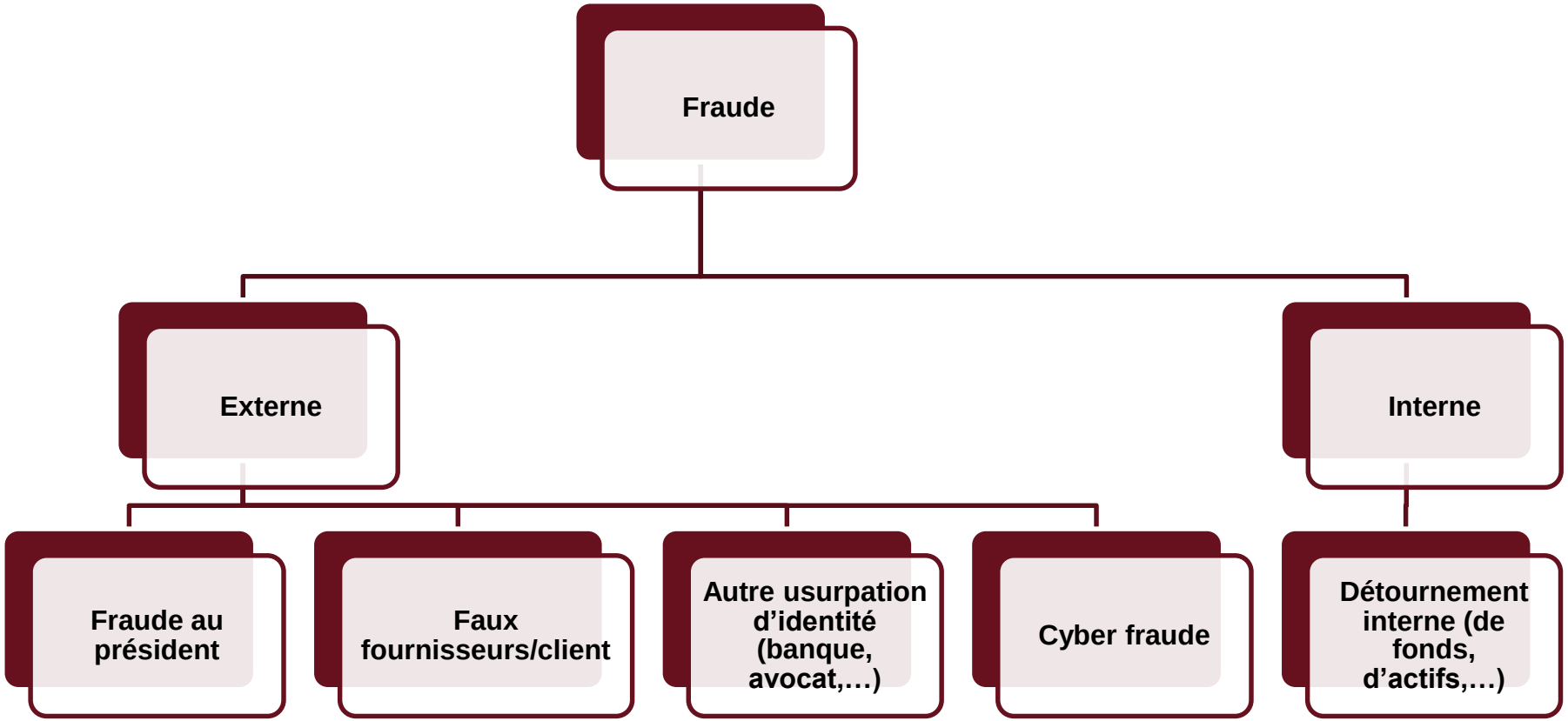


Zone géographique	Taux de fraude constaté en 2014	Taux de fraude constaté en 2016
Afrique	50%	57%
Europe de l'Ouest	35%	40%
Amérique du Nord	41%	37%
Europe de l'Est	39%	33%
Asie-Pacifique	32%	30%
Amérique Latine	35%	28%
Moyen-Orient	21%	25%
Monde	**37%**	**36%**

Évolution du taux de fraude reporté au niveau mondial

Type de Fraudes

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES



DEFINITIONS DE LA FRAUDE

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

- L'Institute of Internal Auditors (IIA) définit la fraude de la manière suivante :

« Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence.

Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou commercial.»

- l'*American Institute of Certified Public Accountants* (AICPA) et l'*Association of Certified Fraud Examiners*, en donne une autre définition :

« La fraude est un acte volontaire ou une omission volontaire ayant pour objet de tromper un ou des tiers. Il en résulte une perte pour les victimes et/ou un gain pour le fraudeur. »

Les fraudes se caractérisent par une tromperie ou une falsification intentionnelle.

Que disent les Normes d'Audit ?

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Norme de la série 2060 : Rapports à la Direction Générale et au Conseil

Le responsable de l'audit interne doit rendre compte périodiquement à la direction générale et au Conseil des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit. Il doit plus particulièrement rendre compte :

- **De l'exposition aux risques significatifs (y compris des risques de fraude)** et des contrôles correspondants …

Norme de la série 2120 : Management des risques

2120.A2 – L'audit interne doit évaluer **la possibilité de fraude et la manière dont ce risque est géré** par l'organisation.

Norme de la série 2210 : Objectifs de la mission

2210.A2 – En détaillant les objectifs de la mission, les auditeurs internes doivent tenir compte de la probabilité qu'il existe des erreurs significatives, **des cas de fraudes** ou de non-conformité ainsi que d'autres risques importants.

ISA 240 – ISA 315 – ISA 330

En application de la Norme ISA 315, l'auditeur doit identifier et évaluer **les risques d'anomalies significatives provenant de fraudes tant au niveau des états financiers** qu'au niveau des assertions retenues pour les flux d'opérations, les soldes de comptes et les informations fournies dans les états financier

Le Triangle de Cressey

- Problèmes familiaux, santé……
- Dépendance à un vice (jeu et/ou drogue)
- Atteinte d'un mode de vie particulier
- Atteinte des objectifs commerciaux, financiers…

- Faiblesse ou inexistence de supervision
- Absence de séparation des fonctions
- Faiblesse du dispositif de Contrôle interne

- Je ne fait qu'emprunté…
- Je suis sous payé et mal considéré malgré mon apport et mes compétences
- Je le mérite
- Je prends comme tout le monde…

Le Dispositif de Contrôle Interne COSO 2013

Définition du Contrôle Interne « COSO »

CONSILIVM

Le Contrôle Interne est :

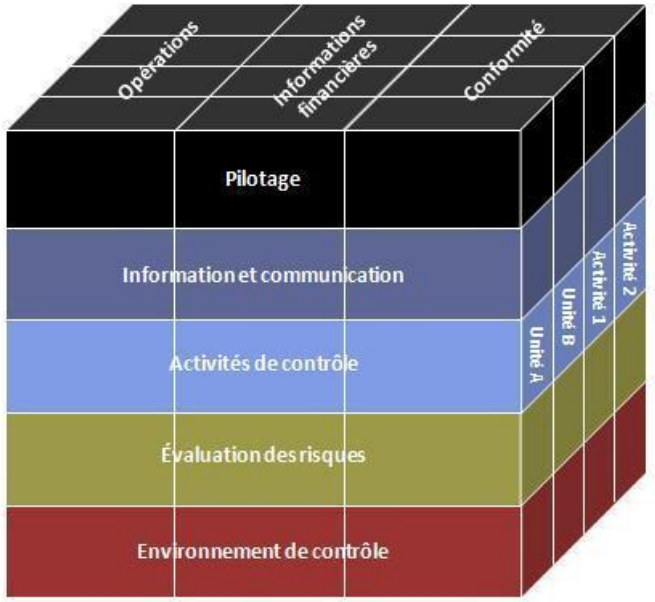
- Un **Processus**
- Mis en œuvre par le **Conseil d'administration**, les **dirigeants** et **le personnel** d'une organisation
- Destiné à fournir une **assurance raisonnable** quant à la **réalisation d'objectifs** liés aux **opérations**, au **reporting** et à la **conformité**.

Composantes du CONTRÔLE INTERNE

CONSILIVM

Ainsi défini, le dispositif de contrôle interne est composé de cinq éléments interdépendants :

- ✓ Environnement de contrôle;
- ✓ Evaluation des risques;
- ✓ Activités de contrôle;
- ✓ Information et communication;
- ✓ Pilotage.



Il est adaptable à la structure de toute entité et peut s'appliquer pour l'ensemble de l'entité ou une filiale, une division, une unité opérationnelle ou un processus métier en particulier.

Un cadre de Référence enrichi

CONSILIVM

- Une description plus précise des modalités de mise en œuvre des 5 composantes du contrôle interne :
  - 17 principes déclinés en caractéristiques
  - 85 critères pour une évaluation de l'efficacité du contrôle interne

- Une prise en compte dans toutes les composantes de l'importance et de la complexité des technologies de l'information

- Un développement des sujets liés à la gouvernance

- L'élargissement de l'objectif « Reporting financier » en « Reporting » afin d'en élargir la portée (interne, non financier)

- **Le renforcement des considérations relatives à la lutte contre la fraude**

- L'élargissement du périmètre du contrôle interne aux acteurs externes intervenant dans la chaîne de valeur : externalisation, sous-traitance, partenariats

17 Principes précisant les 5 Composantes

CONSILIVM

L'organisation

Environnement de contrôle	1. Démontre son engagement pour les valeurs d'intégrité et d'éthique 2. Exerce une supervision pour le développement et la performance du contrôle interne 3. Définit l'organisation, les délégations de pouvoirs et de responsabilité 4. Démontre son engagement en faveur de la gestion des compétences 5. Favorise la responsabilité de chacun
Evaluation des risques	6. Définit clairement les objectifs 7. Identifie et analyse les risques 8. Evalue le risque de fraude 9. Identifie les changements susceptibles d'affecter le système de contrôle interne
Activités de contrôle	10. Choisit et met en œuvre les activités de contrôle 11. Choisit et met en œuvre les activités de contrôle sur les technologies de l'information 12. Définit les activités de contrôle au travers de politiques et procédures
Information Communication	13. Produit et utilise une information pertinente et de qualité 14. Communique en interne sur les objectifs et responsabilités en matière de contrôle interne 15. Communique à l'externe sur les éléments affectant le contrôle interne
Pilotage	16. Conduit des évaluations continues et/ ou périodiques 17. Evalue et communique sur les déficiences du contrôle interne

COSO 2013 Principe 8

COSO 2013 : Focus sur la fraude

Le COSO 2013 a défini 17 principes parmi lesquels un principe dédié à la fraude.

Principe 8: L'organisation intègre le risque de fraude dans son évaluation des risques

Points d'attention (points of focus) :

-Intégrer les différents types de fraudes ;
-Evaluer les incitations/pressions ;
-Evaluer les opportunités ;
-Evaluer les attitudes et comportements.

COSO 2013 Principe 1

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Premier verrou contre la fraude : l'environnement de contrôle

Principe 1: L'organisation manifeste son engagement en faveur de l'intégrité et des valeurs éthiques.

- Instaurer une culture éthique ;
- Faire preuve d'exemplarité ;
- Mettre en place une politique anti-fraude ;
- Adopter un code de conduite ;
- Mettre en place un dispositif d'alerte.

Activités de contrôles et Sensibilisation du Personnel

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

La lutte contre la fraude s'appuie également sur les autres composantes du COSO .

- Mettre en place des contrôles en fonction des schémas de fraudes identifiés ;
- Veiller à mettre à jour ces contrôles ;
- Tester régulièrement ces contrôles.

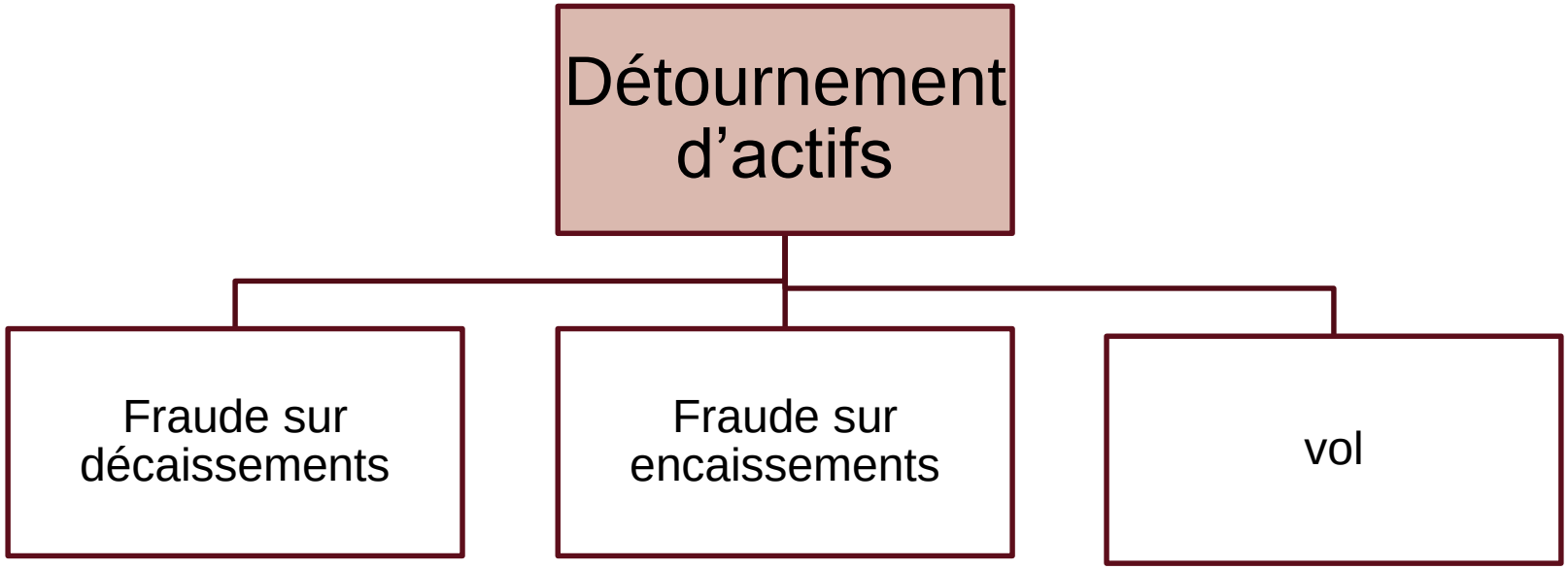
- Information/formation du personnel ;
- Sensibilisation du personnel aux problématiques de fraudes.

Quelque Schémas de Fraude

Détournement d’actifs

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Il consiste à détourner illégalement, de manière directe ou indirecte, un bien du patrimoine de l’entreprise au profit d’un tiers, sans contrepartie pour l'entreprise victime du détournement.



Détournement d'actifs

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

- **Fraude sur décaissements** : consiste à enregistrer en comptabilité un mouvement de sortie de fonds, tout en engageant une manœuvre frauduleuse venant maquiller l'opération pour que le décaissement paraisse légitime:
  - Enregistrement d'opérations fictives (fausses factures, notes de frais gonflées, etc.).

- **Fraude sur encaissements** : permet au fraudeur de dérober les fruits des ventes avant l'enregistrement des opérations dans les systèmes d'information :
  - Non enregistrement d'une vente (vente et encaissement en espèces) ;
  - Détournement d'un règlement ;
  - Falsification de la facturation (sous ou sur facturation).

- **Vol** : touche essentiellement les espèces (en cas d'accès aux caisses), l'appropriation de matériels coûteux (lorsqu'un employé quitte l'entreprise sans restituer le matériel confié), le vol dans les stocks de marchandises, le vol de fichier clients ou tout simplement de petits vols répétés de fournitures.

Risques liés à Certains Logiciel

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

« Pourriciels » : Logiciels comptables qui permettent, du fait de leur **souplesse** d'utilisation, d'obtenir en sortie documentaire ce que l'on désire et non la réalité des opérations. *Noel Pons (spécialiste de la prévention de la fraude)*

- *La Possibilité de modifier des informations sans laisser de trace*
- *L'opportunité de rendre « automatique » certaines procédures à caractère frauduleux*

- *Domaines sensibles a ce type de fraude:*
  - *Facturation et Tarification*
  - *Stocks (optimisation du BFR)*
  - *Charges*
  - *Paie*
  - *Ecritures comptables & clôtures des exercices.*

Facturation

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

- Possibilité de modifier et/ou de supprimer une facture à tout moment est présente;
- Possibilité de boucher les trous laissés par les factures supprimées;
- Modifier les prix de vente des produits facturés;
- Ne pas facturer certains bons de livraisons;
- Ne pas enregistrer des groupes de factures en comptabilité.
- Possibilité de supprimer une facture et de la recréer sous le même numéro réaffecté automatiquement par le système.

PASSATION DES ECRITURES:

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

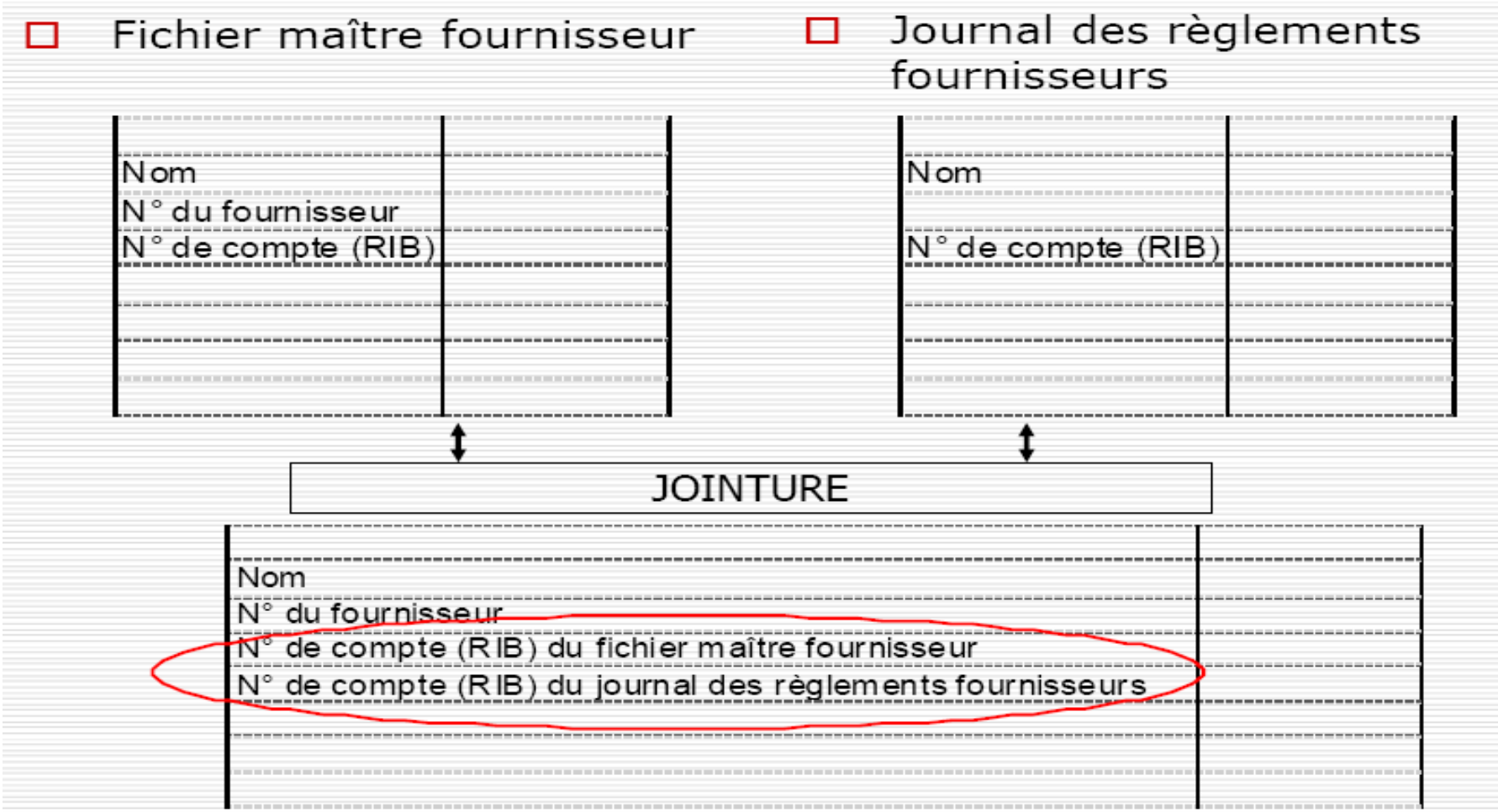
- Possibilité de « délettrer » les écritures antérieurement lettrées;
- Possibilité de purger plusieurs écritures en fonction de critères précis;
- Possibilité d'autoriser une caisse créditrice;
- Existence d'un système de restauration qui écrase les opérations antérieures;
- Possibilité de tenir plusieurs comptabilités pour la même entreprise et pour le même exercice.

CLÔTURES DES EXERCICES

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

- Pas de clôture obligatoire et l'exercice par défaut peut porter sur 24 ou 36 mois
- Possibilité de rouvrir un exercice déjà clôturé
- L'inscription d'un report à nouveau n'est pas obligatoire
- La possibilité de définir le résultat comptable et de modifier en conséquence les écritures afin d'arriver au résultat souhaité.

Un règlement « fournisseur » est versé sur un autre compte



- ✓ Rechercher les numéros de compte bancaire différents
- ✓ Extraire les règlements crédités sur des comptes bancaires différents de ceux figurant sur le fichier maître fournisseur

Les anomalies dans les coordonnées du client ou du fournisseur

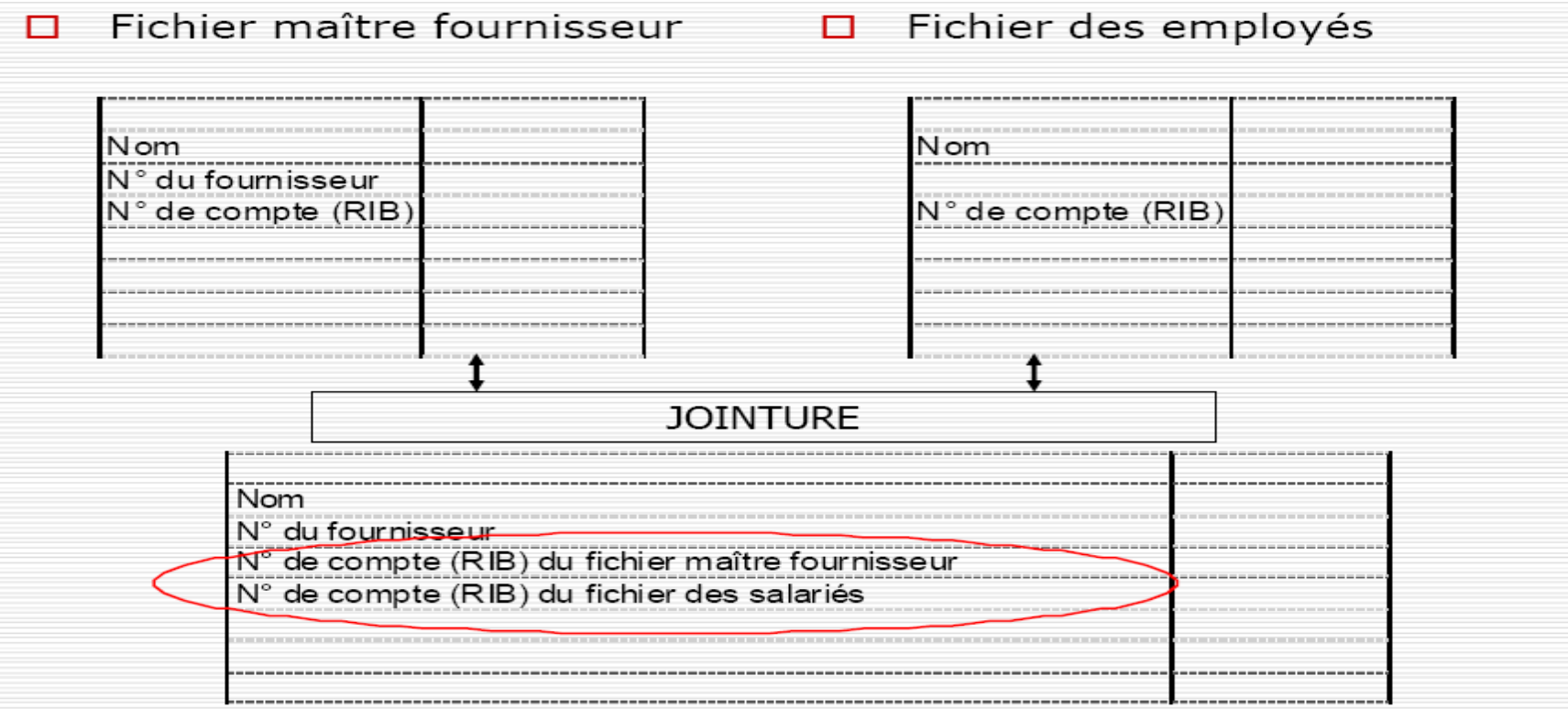
CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Fichier client / fournisseur

Nom	Dupont	
N° du fournisseur	35125	98541
N° de compte (RIB)		5479310

- ✓ Réaliser un « filtre » pertinent sur le fichier du client ou du fournisseur
- ✓ Extraire **tous les blancs** existants.

Les paiements détournés par les employés



- ✓ Rechercher les numéros de compte bancaire identiques
- ✓ Extraire les « doublons » de ces comptes bancaires

Les « doublons »

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Grand livre d'achat

Nom	Dupont	Durand
N° du fournisseur	35125	98541
N° de compte (RIB)	3258621	5479310
N° de facture	213456	213456
Montant en €	10 395,19	10 395,19

- ✓ Extraire les « doublons »
- ✓ Analyser chacun des cas identifiés

LES NOUVELLES ARCHITECTURES DE CONTROLE

Le MODELE Des 3 L.O.D

&

Le Continuos Control Monitoring

LES 3 LIGNES DE DEFENSE / MAITRISE

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

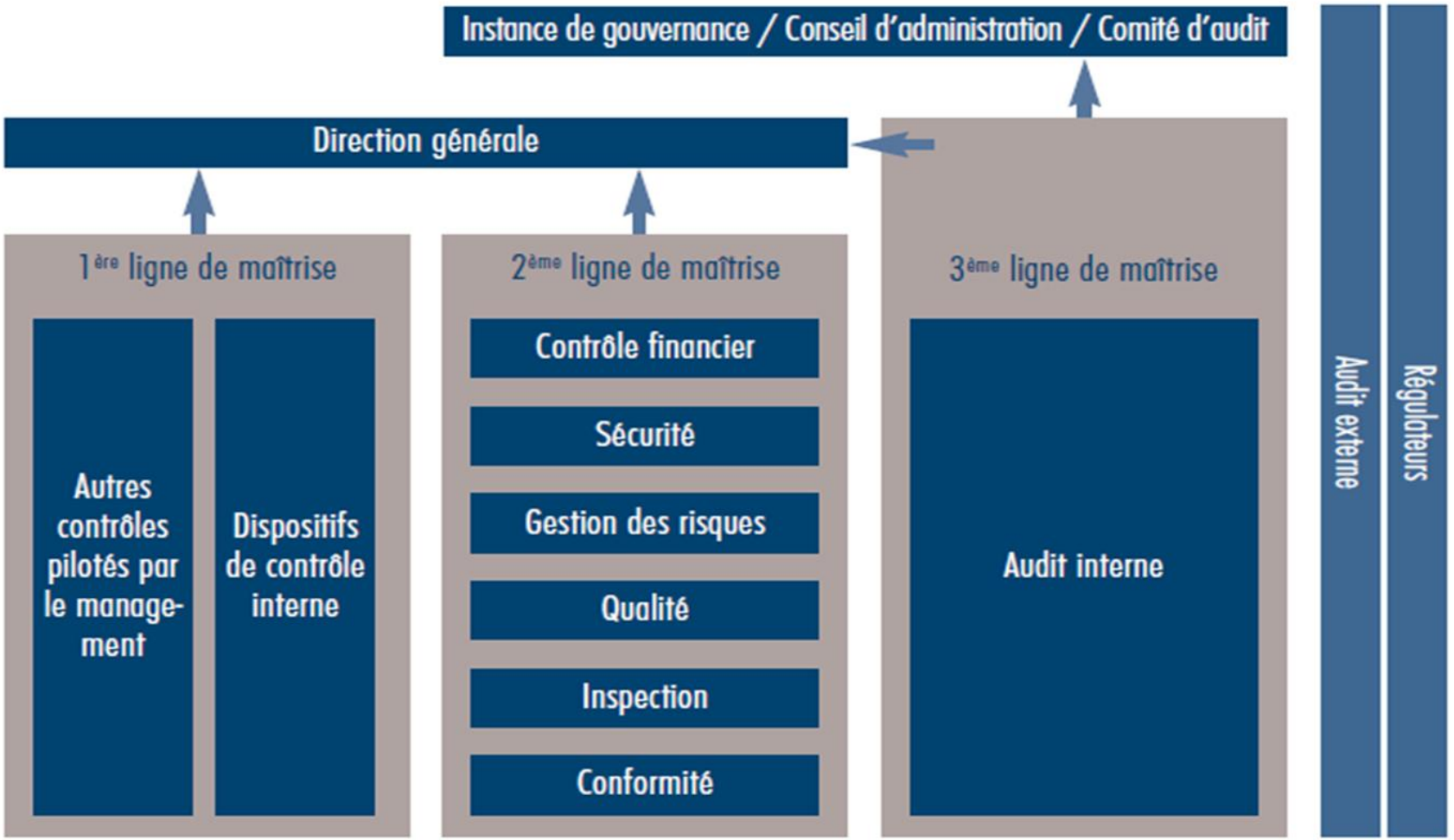
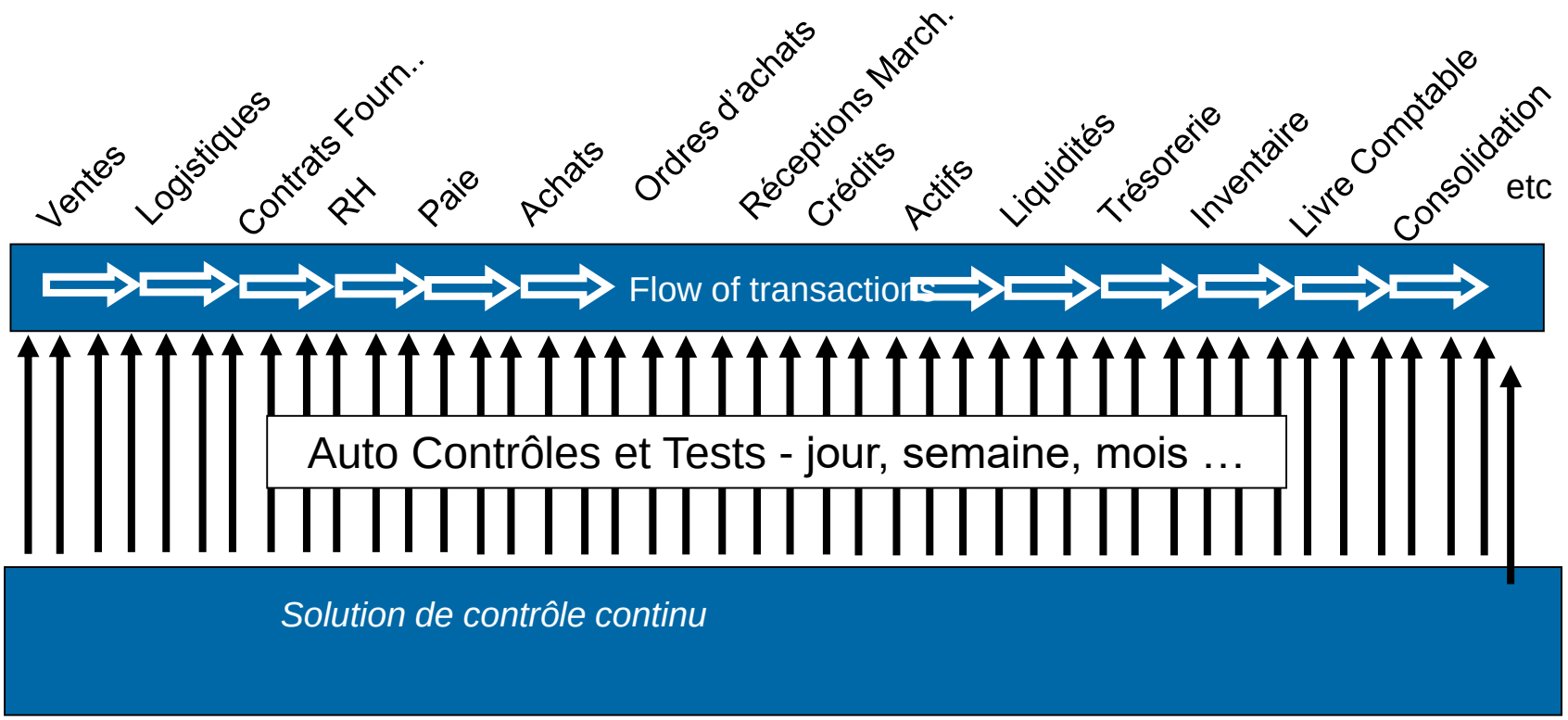


Schéma adapté à partir des lignes directrices ECIIA/FERMA sur la 8e directive de l'UE relative au droit des sociétés, article 41.

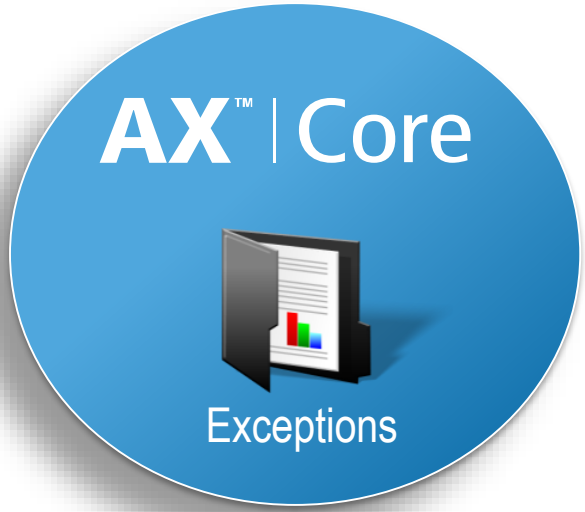
Le Contrôle Continu : Systématiser les Contrôles

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES



AX™ | Exception

- Accès Web
- Diffusion des alertes
- Gestion de ces alertes sous forme d'un workflow
- Reporting sur les résultats des controles



AX™ | Exception

Business Stakeholders

"Audit Interested"

- Processus comptable
- Les achats
- La paie
- Analyse fiscale
- Toutes fonctions de l'entreprise

CYBERCRIMINALITÉ & FRAUDE

Profil des attaquants

Attaquants

LUCRATIVE
Cybergangs
Cybermercenaires
Officines

POLITIQUE
Hacktivistes
Cyberpatriotes
Cyberterroristes

MILITAIRE
Unités spécialisées

LUDIQUE
Adolescent désoeuvré

TECHNIQUE
Hacker

PATHOS
Employé mécontent

Les Techniques d'ingénierie sociale les plus courantes

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

La "Fraude au président ou Directeur Général "

- En usurpant l'identité d'un dirigeant, le fraudeur obtient la collaboration d'une personne de l'entreprise afin d'effectuer un virement à l'étranger, par exemple en prétextant une acquisition de société urgente et très confidentielle
  - Les principaux critères d'alerte de cette fraude:
    - Une demande urgente, exceptionnelle et confidentielle
    - Une forte pression exercée sur le collaborateur
    - Une opération inhabituelle vers des comptes et/ou bénéficiaires inconnus

L'usurpation de la banque

- Le fraudeur se fait passer au téléphone pour un interlocuteur de la banque afin d'obtenir des informations confidentielles (codes d'accès, mots de passe), par exemple en demandant à l'entreprise d'effectuer des « virements tests » ou encore des connexions pour mises à jour
  - Les principaux critères d'alerte de cette fraude:
    - Une demande de virement avec un montant élevé pour un test
    - L'Utilisation de la norme SEPA pour justifier un tel virement
    - Une demande de prise de contrôle à distance de l'ordinateur du collaborateur

Détournement de lignes téléphoniques

- Les fraudeurs se font passer pour des fournisseurs pour demander des modifications de coordonnées bancaires. Ils confirment ces demandes par de faux courriels ou faux numéros de fax, allant même jusqu'à demander aux opérateurs télécom de re-router les lignes des standards vers leur numéro → Les contre-appels sont dès lors inopérants
  - Les principaux critères d'alertes de cette fraude:
    - Un de vos fournisseurs communique de nouvelles coordonnées bancaires par fax ou courriel

La démarche du fraudeur 5 phases d'attaque

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

1. La collecte de renseignement :Identification des employés, localisation des documents, copinage, fouille de poubelle, ingénierie sociale,…*

2. Recherche du maillon faible : analyse des informations recueillies et sélection d'identités, ciblage , recoupement …

3. Acquisition d'adresses mail, numéro de fax, de téléphone,…

4. Elaboration de l'objet de la demande: contrôle fiscal, opération en capital très confidentielles, règlements d'avocat à l'étranger,…

5. Exécution de l'attaque : Munis des informations collectées et utilisant un numéro du pays, le fraudeur se fait passer pour le président/dirigeant, et va persuader le directeur financier ou le trésorier d'effectuer un virement.

Les mesures de vigilance Au niveau de l'entreprise – 1/2

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Adopter de bons comportements et des mesures de prévention	• Respecter les règles de sécurité de l'entreprise • Alerter toute demande inhabituelle
Sécuriser les processus et outils internes à l'entreprise	• Limiter, contrôler et sécuriser l'accès aux applications sensibles • Dissocier saisie et validation des ordres bancaires • Définir et respecter les procédures de validation • Réaliser des contrôles réguliers
Sécuriser les échanges avec la banque	• Limiter ou supprimer les virements papiers ou fax (risque de fraude élevé) • Alerter au plus vite la banque en cas de doute

C'est en sécurisant leurs procédures de virements manuels, en contrôlant leur information, et en sensibilisant leurs salariés que les entreprises peuvent espérer échapper à ces escroqueries d'un nouveau type.

Les mesures de vigilance Au niveau de l'entreprise – 2/2

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

Sensibiliser régulièrement les collaborateurs

- Inciter les collaborateurs à conserver un esprit critique et un exercice du droit d'alerte, à résister à l'agression psychologique
- Informer les collaborateurs sur le mode opératoire des fraudeurs
- Ne pas se contenter des informations affichées
- Encourager la bonne connaissance des interlocuteurs (clients, fournisseurs, partenaires,…)
- Rappeler aux collaborateur de ne révéler, sous aucun prétexte, les identifiants/mot de passe
- Garder un respect absolu des procédures

Maitriser la diffusion d'information

- Limiter les informations publiées sur les sites internet de l'entreprise
- Privilégier les intranets sécurisés pour l'accès aux documents de l'entreprise
- Conserver la confidentialité des signatures manuscrites
- Limiter l'accès aux documents sensibles (modèles de fax,..), broyer les documents confidentiels obsolètes

Rebondir après la fraude

CONSILIVM
VOTRE PARTENAIRE POUR LES MEILLEURES PRATIQUES

- **Au-delà de la perte financière et du risque d'image associé, une fraude doit être l'occasion de rebondir.**
- **En renforçant les dispositifs de maîtrise des risques :**
  - Identification des risques
  - Renforcement du dispositif de contrôle
  - Revue de l'organisation et de la gouvernance
    - ✓ *Changement de culture : Vigilance*
    - ✓ *Rigueur et discipline*
    - ✓ *Responsabilité individuelle*
- **L'existence de la fraude doit générer une prise de conscience des insuffisances du dispositif et la mise en place de programme de lutte contre la Fraude**
  - Code d'éthique
  - Support et attention du management (Tone at the top)
  - Sensibilisation des collaborateurs aux risques
  - Dispositif d'alerte et Investigations
- **…qui permettront à l'entreprise de rebondir et de sortir renforcé de l'épreuve**

MERCI POUR VOTRE ATTENTION