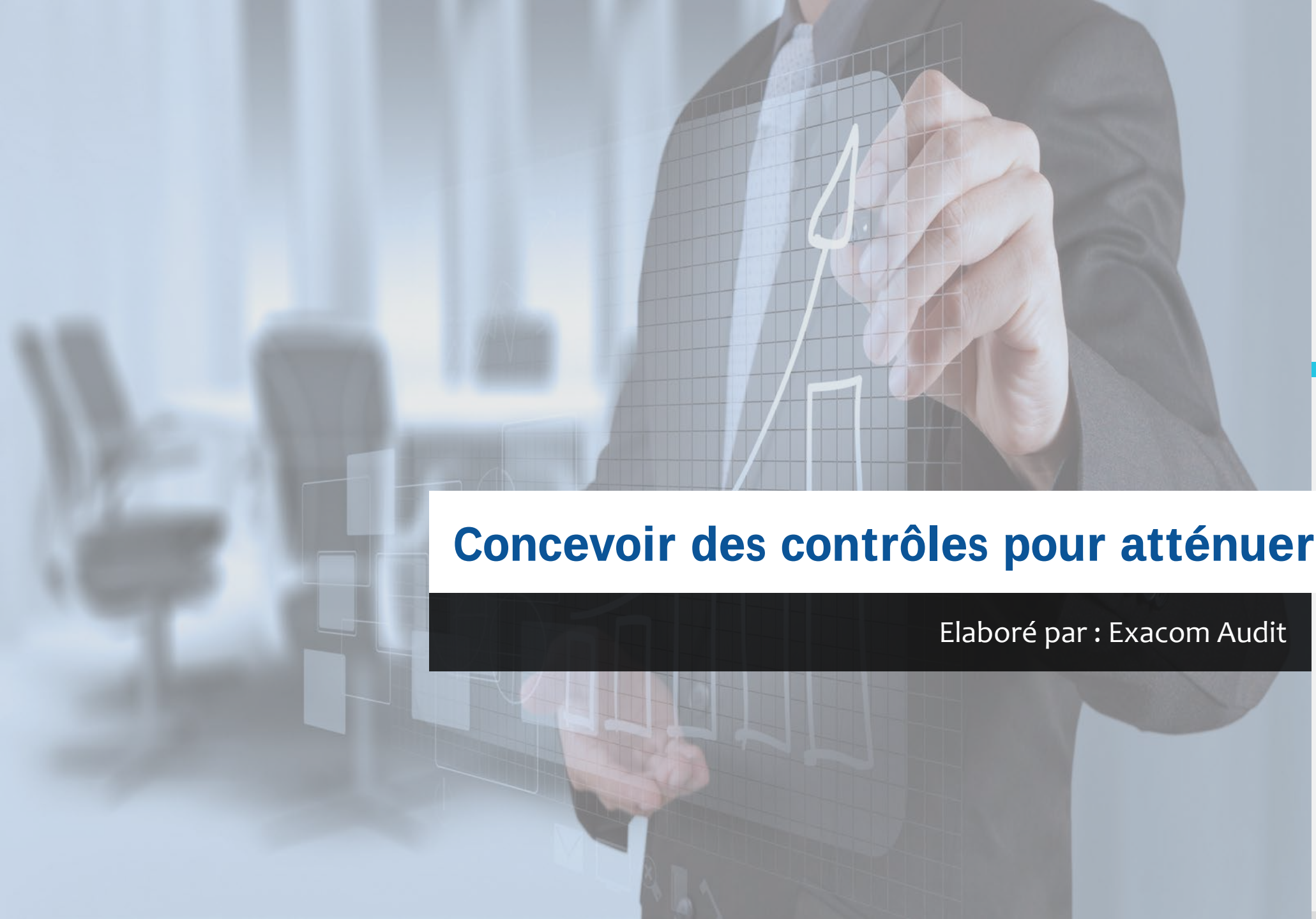

Concevoir des contrôles pour atténuer les menaces

Elaboré par : Exacom Audit

Introduction

Dans le cadre de la démarche d'optimisation des processus, il est essentiel de considérer les contrôles internes comme un investissement.

Ils impliquent des coûts, mais ils présentent également des avantages indéniables. Dans le cadre de notre analyse financière, il est essentiel de prendre en compte les différents coûts associés à la gestion des serrures et des systèmes de sécurité.

Ces coûts peuvent se manifester sous forme d'imposition de délais de traitement, qui peuvent affecter l'efficacité opérationnelle, ou de coûts monétaires liés à l'installation et à la maintenance des serrures et des systèmes de sécurité.

En outre, il est important de considérer les coûts inhérents à la conception, à la mise en place et à la mise en œuvre des contrôles. Parmi les avantages compétitifs des contrôles internes, nous pouvons citer la protection des actifs de l'organisation et la production d'une information fiable et exacte. Si le coût de la mise en place d'un contrôle particulier est trop élevé par rapport aux avantages escomptés, il convient de déterminer si ce contrôle doit effectivement être mis en place ou s'il doit plutôt être allégé ou éliminé. Comme les avantages devraient, en théorie, l'emporter sur les coûts, il est recommandé d'analyser les contrôles en fonction des avantages potentiels qui peuvent en découler. Il est donc essentiel d'évaluer l'importance relative (l'avantage) d'un contrôle interne spécifique. Dans ce cadre, nous adopterons une approche méthodique basée sur l'évaluation rigoureuse des risques potentiels

Sommaire

1. Identifier les risques de fraude
2. Définir les objectifs des contrôles
3. Types de contrôles à mettre en place
4. Liste des contrôles à mettre en place dans un cadre informatique
5. l'approche axée sur l'évaluation des risques

Identifier les risques de fraude

Avant de concevoir des contrôles, il est indispensable de cartographier les menaces. Les risques de fraude peuvent être classés comme suit :

Fraudes internes

Détournement d'actifs, falsification de documents, manipulation des états financiers.

Fraudes externes

Escroquerie, usurpation d'identité, piratage informatique.

Fraudes opérationnelles

Erreurs ou omissions dans les processus qui peuvent être exploitées à des fins frauduleuses.

Outils pratiques :

- Cartographie des risques par processus.
- Historique des incidents et contrôles existants.
- Évaluation des vulnérabilités internes et externes.

Définir les objectifs des contrôles

Chaque contrôle doit avoir un objectif clair lié à un risque spécifique :

- Prévention : éviter que la fraude ne se produise (ex. séparation des tâches, approbations multiples).
- Détection : identifier la fraude dès qu'elle survient (ex. audits, surveillance informatique, analyse des anomalies).
- Correction / Réponse : limiter l'impact et corriger rapidement (ex. enquête interne, procédures disciplinaires, reporting)

Types de contrôles à mettre en place

Contrôles préventifs

Séparation des fonctions : aucun employé ne doit contrôler une opération de bout en bout (ex. saisie vs validation des paiements).
Politiques d'autorisation : seuils d'approbation pour les transactions financières importantes.
Formation et sensibilisation : Programmes réguliers sur l'éthique et la prévention de la fraude.
Sécurité informatique : gestion des accès, mots de passe complexes, authentification à double facteur

Contrôles détectifs

Audit interne périodique : vérification systématique des transactions et processus.
Analyse des anomalies : utilisation de tableaux de bord et de KPI pour identifier les écarts inhabituels.
Surveillance continue :
Logiciels de monitoring et alertes automatiques pour les transactions

Contrôles correctifs

Procédures de traitement des incidents : enquête, sanctions, restitution des pertes.
Mises à jour des processus : adaptation des contrôles suite à des fraudes détectées.
Communication et reporting : informer la direction et les parties prenantes des incidents et mesures correctives.

Types de contrôles à mettre en place

Pour qu'un contrôle soit efficace, il doit être :

Complet

Couvrir tous les risques identifiés.

Cohérent

S'intégrer aux procédures et systèmes existants.

Flexible

Evoluer selon les nouvelles menaces et changements organisationnels.

Documenté

Procédures écrites, manuels de contrôle, instructions claires pour le personnel

Liste des contrôles à mettre en place dans un cadre informatique

- Etablissement d'un plan de sécurité
- Séparation des fonctions incompatibles au sein du système
- Contrôles visant l'élaboration de projets
- Contrôles d'accès physique
- Contrôles d'accès logique
- Contrôles visant la transmission des données
- Normes de documentation
- Réduction des temps d'arrêt du système
- Plans de reprise après sinistre
- Protection des ordinateurs personnels et des réseaux client-serveur
- Protection des ordinateurs portatifs
- Contrôles visant Internet
- Amélioration des méthodes de détection des fraudes

L’approche axée sur l’évaluation des risques :

Menaces — Identifier et énumérer tous les événements indésirables qui pourraient endommager vos systèmes, vos données ou votre organisation.

Exposition — Estimer le montant de la perte potentielle qui serait subie si chaque menace énumérée se réalisait.

Risque — Estimer la probabilité de réalisation de chaque menace.

Contrôles — Identifier et examiner tous les contrôles qui aideraient à empêcher la menace de se réaliser.

Coûts — Estimer les coûts liés à la mise en place des contrôles.

Comparaison — Comparer les coûts, les avantages et les probabilités de réalisation afin de déterminer si les contrôles devraient être mis en place

eXacom
Expertise & Auditing Company

eXacom audit

+216 70 698 845

contact@exacomaudit.com

www.exacomaudit.com