Détecter et prévenir la fraude grâce aux outils d'analyse de données

acl

Sommaire

Beaucoup d'organisations ont réagi aux récentes activités du marché par une compression de personnel, un blocage des dépenses et une approche réactive face aux retombées durables de la crise économique.

Économie instable rime souvent avec activités frauduleuses. Nos clients évoquent la fraude interne qui va de la mauvaise utilisation des cartes d'achat de la part des employés à une fraude de grande ampleur sur les contrats à valeur ajoutée et les violations de contrôles qui pourraient avoir de graves répercussions sur les entreprises. Le temps est venu d'intensifier les mesures de prévention et de détection de la fraude.

Cet e-book porte sur l'utilisation des outils d'analyse de données dans la mise en place d'un programme de fraude réussi. Il inclut ses principaux aspects et des techniques de détection de la fraude illustrées d'un certain nombre d'exemples applicables dans votre organisation.

Pourquoi utiliser l'analyse de données pour la fraude ?

Un grand nombre de systèmes de contrôle interne présentent de graves insuffisances d'où le grand intérêt d'avoir recours aux outils d'analyse de données dans la lutte contre la fraude. Pour tester et surveiller efficacement les contrôles internes, les organisations doivent étudier chaque transaction ayant lieu, puis les tester vis-à-vis des paramètres définis, des applications et des systèmes, et ce, depuis différentes applications et sources de données. La plupart des systèmes de contrôle interne ne peuvent tout simplement pas assurer cela. Par ailleurs, quand des systèmes internes sont mis en place, certains contrôles ne sont même jamais activés.

Vous le savez peut-être vous-même en utilisant certains systèmes au sein de votre propre organisation : au début, lorsque ces systèmes viennent d'être instaurés, vous pouvez par exemple saisir une série de 9 pour un code postal ou régional si vous n'êtes pas sûr. En apparence, ce n'est pas grand-chose, mais cela met en valeur une zone susceptible de comporter des faiblesses pouvant servir à frauder.

Nous avons observé des cas où c'étaient les numéros de sécurité sociale qui avaient été mal saisis et qui ont permis à un fraudeur de profiter de cette faille pour essayer de frauder sur l'identité ou la paie.

Les systèmes de contrôle interne, même bons, ne suffisent pas

Les systèmes de contrôle interne comportent généralement des faiblesses pouvant être exploitées à mauvais escient. Il faut étudier l'intégralité des transactions pour comparer les données de différents systèmes et applications afin de rechercher des correspondances qui ne devraient pas être là ou pour rechercher des écritures en doublons qui indiquent une activité frauduleuse ou une mauvaise utilisation peut-être. Cet examen doit être effectué régulièrement, à l'aide de l'automatisation dans des zones à risque élevé, pour que vous puissiez saisir la fraude dès son apparition et avant qu'elle aille plus loin. Bien sûr, découvrir une activité frauduleuse - quelle qu'elle soit - perpétrée depuis plusieurs années est manifestement une grande victoire, mais découvrir le problème avant qu'il se concrétise répondra mieux aux besoins de l'organisation à long terme.

Un des éléments essentiels des outils d'analyse de données est leur capacité à tenir jour des traces complètes relatant toutes les activités effectuées. Vous pouvez exécuter une application ou un script, saisir des données et détecter des anomalies. Cette fonctionnalité répond parfaitement à vos besoins, mais il vous faudra des preuves de vos actions pour révéler cette activité frauduleuse. Ces preuves doivent être suffisamment précises et détaillées pour résister aux autres enquêtes menées ultérieurement, voire aux poursuites légales peut-être. Dans de nombreux cas, la trace d'audit générée par les outils d'analyse de données d'ACL est utilisée dans les tribunaux pour prouver lors du procès que certaines activités ont été effectuées dans une intention de frauder.

il vous faut des **preuves**

Les outils d'analyse de données spécialisés ont une grande longueur d'avance sur l'échantillonnage manuel

Par le passé, détecter une activité frauduleuse relevait souvent du grand hasard. Maintenant, grâce aux outils d'analyse de données ACL, il est possible de détecter les problèmes d'origine, d'identifier des tendances et de fournir des résultats détaillés. Avec le volume des transactions passant par les organisations aujourd'hui, la vitesse de l'activité augmente à vitesse grand V car il s'avère extrêmement difficile d'examiner dans le détail chaque transaction. Ce manque de surveillance sur les transactions individuelles ouvre la voie aux activités frauduleuses sur les systèmes, à la fraude et, de fait, à des impacts non négligeables sur les résultats financiers.

Si vous avez besoin d'être convaincu sur la place essentielle de l'analyse de données dans tout bon programme de lutte contre la fraude, rapprochez-vous de l'ACFE, de l'IIA et de l'AICPA. Toutes ces associations préconisent l'utilisation des technologies d'analyse de données pour aider à détecter la fraude.

mieux vaut **prévenir** que **guérir**

Prévenir la fraude, c'est essentiellement communiquer sur le programme anti-fraude au sein de son organisation. En effet, si chacun est au courant de l'existence de systèmes susceptibles de détecter une fraude ou violation de contrôles, et si chacun sait que chaque transaction transitant par vos systèmes est surveillée, vous voilà en possession d'une excellente mesure préventive. Elle consiste à informer le personnel qu'il ne sert à rien de prendre la peine de frauder puisque les fraudeurs se feront repérer rapidement.

Échantillonnage

De nombreuses méthodes de tests de contrôles comme l'échantillonnage présentent d'importantes lacunes. Bien que l'échantillonnage soit exigé et rendu obligatoire pour certains processus, cela n'est pas forcément suffisant pour faire des tests de contrôle exhaustifs.

Avec l'approche par échantillonnage, vous ne pourrez peut-être pas quantifier entièrement l'impact suite à des omissions de contrôles et vous ne pourrez peut-être pas faire non plus d'estimations dans certaines populations. Vous pourriez passer à côté de certaines anomalies et parfois, c'est la somme de petites anomalies au fil du temps qui aboutit à de grandes situations de fraude. L'échantillonnage est une méthode efficace dans le cas de problèmes qui sont relativement constants dans des populations de données. Or, ce n'est pas toujours le cas dans les situations de fraude. Par nature, les transactions frauduleuses ne se font pas par hasard. Les transactions peuvent être comprises dans les limites de certains tests standard et ne pas être repérées.

Pour tester et surveiller efficacement les contrôles internes, les organisations doivent analyser toutes les transactions pertinentes.

L'échantillonnage peut être utile, mais il ne suffit pas pour détecter efficacement la fraude. Quelle méthode doit-on donc utiliser ? Il existe tout un panel d'outils permettant de détecter la fraude, allant des analyses ad hoc aux analyses répétitives et continues.

Analyse ad hoc

Il s'agit ici de chercher des réponses à donner à des hypothèses spécifiques. Les analyses ad hoc vous permettent d'aller plus loin dans les détails. Vous pouvez enquêter sur des transactions pour vérifier la présence d'indicateurs ou de risques de fraude. Imaginons que vous ayez une hypothèse. L'adresse d'un employé correspond peut-être à l'adresse d'un fournisseur. Vous pouvez aller chercher ces informations : comparer un fichier maître fournisseur à un fichier maître employé, puis rechercher les enregistrements correspondants. Si vous trouvez quelque chose, tant mieux ! Il s'agit d'une découverte importante susceptible de révéler quelqu'un s'étant établi comme fournisseur fantôme et fraudant de la sorte. Vous pouvez en fait rechercher des risques de fraude. Si ce type d'anomalie semble relativement courant ou s'il y a une certaine exposition au risque avec laquelle vous n'êtes pas à l'aise, vous voudrez peut-être aller plus loin, régulièrement.

enquêtez sur les transactions pour vérifier la présence d'indicateurs ou de risques de fraude

Analyse répétitive ou continue

Dans le contexte de la détection de la fraude, l'analyse répétitive ou continue implique de **mettre en place des scripts à exécuter sur de grands volumes de données pour identifier les anomalies à mesure qu'elles apparaissent sur une période donnée**. Cette méthode peut vraiment améliorer l'efficacité, la cohérence et la qualité globales de vos processus de détection de la fraude. Créez des scripts, testez-les et exécutez-les sur les données pour être averti régulièrement en cas d'anomalie.

Vous pouvez exécuter le script tous les soirs pour qu'il parcoure toutes ces transactions afin d'être informé en temps utile sur les rapports de tendances, de modèles et d'exceptions pouvant être fournis à la direction. Par exemple, ce script pourrait exécuter des tests spécifiques sur toutes les transactions de cartes d'achat à mesure qu'elles se produisent afin de vérifier qu'elles sont bien conformes aux contrôles. Comme vous le savez, les transactions de cartes d'achat se font sans autorisation préalable dans les grandes organisations, ces cartes sont donc très nombreuses.

Il convient d'appliquer tout un panel d'analyses ; toutefois, l'idée n'est pas de passer d'une analyse à l'autre, mais plutôt de les employer en continu. Si vous êtes passé de l'exploration et de l'investigation à une analyse plus continue dans un domaine, vous aurez plus de temps pour étudier d'autres domaines où les choses pourraient mal se passer.

notification périodique lorsqu'une anomalie apparaît dans les données

Techniques utilisées par les outils d'analyse

Retenez bien : vous recherchez des phénomènes qui ne paraissent pas normaux.

- Calculez des paramètres statistiques et recherchez les valeurs hors normes ou celles dépassant les moyennes ou les écarts types.
- Recherchez les valeurs élevées et les valeurs faibles et recherchez-y des anomalies. Bien souvent, ce sont ces types d'anomalies qui révèlent la fraude.
- Jetez un œil au classement des données : regroupez les données, toutes les transactions, dans des groupes spécifiques en fonction de leur emplacement par exemple. Peut-être qu'un certain nombre de transactions a lieu en dehors des paramètres statistiques. D'où viennent-elles ? Sont-elles réparties de manière égale sur toute la population ou se limitent-elles à une zone géographique donnée ? Si c'est le cas, c'est grave et vous devrez peut-être approfondir la chose.

Loi de Benford

Analyser les données à l'aide de la loi de Benford est vraiment très pratique. Cette loi stipule que les listes de numéros tirés de sources de données réelles sont distribuées de manière spécifique non uniforme. Le chiffre 1 apparaît dans 30 % des cas. Ensuite, c'est le chiffre 2, qui apparaît moins souvent, puis le chiffre 3, 4, jusqu'à 9 qui apparaît moins d'une fois sur 20. Vous pouvez tester certains points et certains chiffres pour identifier ceux qui apparaissent plus souvent qu'ils le devraient et qui sont donc suspects.

Partout où les nombres sont répartis naturellement, vous allez voir cette courbe inverse d'apparition des chiffres dans les nombres. Peut-être que vous ne savez pas précisément ce que vous recherchez mais grâce à l'analyse numérique, vous pouvez observer des pics ou les creux artificiels à l'intérieur de ces nombres. Ces chiffres peuvent être des indicateurs de fraude que vous pourrez explorer et examiner plus minutieusement.

Joignez ou faites correspondre des champs de données entre différents systèmes pour identifier des correspondances possibles entre les fichiers maîtres employé et les fichiers maîtres fournisseur. Ce type de correspondance est évidemment suspect.

Étudiez la **correspondance des données**. Recherchez parmi les données de paie la présence de versements de deux personnes différentes vers le même compte bancaire. C'est un problème qui a été identifié dans une situation de fraude afin de falsifier une activité d'emploi ; une personne s'était en fait organisée pour recevoir trois chèques différents. Regardez les noms, les adresses, les numéros de téléphone, les numéros de série ou les numéros de référence. Ce sont des techniques très puissantes pour détecter la fraude.

Une autre méthode efficace fait appel à la **fonction SOUNDS LIKE (« semblable à »)** pour vous aider à identifier les variations de noms d'employés d'entreprise valides. Il arrive que les fraudeurs essaient de dissimuler un peu leur identité en portant un nom similaire, mais pas tout à fait identique. Ils sont conscients qu'un grand nombre de contrôles internes recherchent une correspondance parfaite. Une fonction SOUNDS LIKE peut établir une sorte de correspondance à la « logique approximative » pour rechercher ces exemples.

Le **test de recherche de doublons** est l'un des tests de fraude les plus répandus. Nous sommes nombreux à l'utiliser car il peut non seulement indiquer une fraude, mais aussi un manque d'efficacité ou des erreurs parmi des transactions professionnelles. Recherchez des variations simples ou complexes de doublons. Recevez-vous des factures en doublon de la part de quelqu'un ? Si oui, est-ce délibéré ou non ? D'une façon ou d'une autre, payer deux fois une facture est préjudiciable.

Des **omissions** dans des données séquentielles peuvent être un indicateur intéressant de quelqu'un essayant d'utiliser le système à mauvais escient. Si un certain nombre de bons de commande émis par votre entreprise sont tous séquentiels mais que, tout à coup, il manque un numéro ici et là, est-ce parce que quelqu'un tente d'envoyer un bon de commande non comptabilisé et de le soumettre au système pour un éventuel remboursement ? Il s'agit là d'un véritable indicateur. Ce genre de fraude est assez facile à détecter une fois que vous disposez des bons outils technologiques.

Zones d'application dans la détection de la fraude

Les fraudeurs profiteront des faiblesses là où ils en trouveront. L'analyse de données s'avère vraiment fiable pour détecter et prévenir la fraude dans divers domaines. Nous avons déjà parlé de certains de ces domaines dans les comptes fournisseurs et les créances clients. Pensez simplement aux risques de fraude dans la gestion de cartes de crédit ! Les collaborateurs achètent - sur leurs cartes de crédit professionnelles - des choses qu'ils ne devraient pas. Des clients ont trouvé des achats inappropriés allant des vaches - oui, vous avez bien lu, des vaches ! - à des dizaines de milliers de dollars de lecture de cartes de tarot.

Jetez un œil au Grand livre, en particulier aux écritures passées après une période de clôture. Vérifiez les comptes ayant été souvent inversés ainsi que les écritures passées le week-end. Étudiez les écritures du Grand livre sur un trimestre et posez-vous ces questions :

- Ces écritures ont-elles été passées conformément à nos contrôles internes ou des collaborateurs tentent-ils de publier des écritures dans le Grand livre après la période de clôture ?
- Certains comptes du Grand livre sont-ils souvent inversés ?
- Y a-t-il des comptes inactifs qui sont utilisés tout à coup ?

Il peut valoir la peine d'examiner minutieusement ces petits indicateurs. L'utilisation de l'analyse répétitive est bel et bien recommandée dans les cas suivants :

- Vous étudiez de gros volumes de transactions, peu importe la taille des transactions réelles
- Période continue
- La zone est identifiée comme étant à risque élevé

Le contrôle des stocks et de la gestion des matières renvoie à l'idée de pouvoir comparer les données de deux systèmes différents. Imaginez que mon système de stock m'informe que 30 000 paires de chaussettes grises ont quitté mon entrepôt à New York pour se rendre à Boston. Je regarde les enregistrements du magasin à Boston. Le magasin de Boston indique avoir vendu 20 000 paires de chaussettes grises et indique avoir épuisé le stock. Ensuite, vous pouvez comparer les deux et voir que quelque 10 000 paires de chaussettes grises manquent à l'appel. Cette incohérence serait quelque chose à étudier minutieusement.

Un peu plus tôt, nous avons parlé d'omissions parmi des numéros de bons de commande. Lorsque vous générez des numéros de bons de commande, vous vous attendez à ce qu'ils suivent un ordre : bons de commande 1, 2, 3, 4... etc. Que se passe-t-il si votre système enregistre uniquement les bons de commande 1, 2, puis 4, 5, 6 ? Qu'est-il arrivé au bon de commande n° 3 ? A-t-il été soumis hors compta ?

En raison d'un conflit d'intérêts ou d'une mauvaise séparation des tâches, une fraude peut se produire car quelqu'un est impliqué à plusieurs endroits tout au long du processus d'approbation. Si vous jetez un œil aux enregistrements du livre de paie ou du registre des présences, et que vous recherchez quelqu'un qui n'a jamais pris de vacances, vous voudrez peut-être approfondir la question. Il est bien connu que de nombreux fraudeurs ne peuvent pas prendre de vacances de peur de se faire attraper ! Bien sûr, il existe l'autre type de fraudeur qui soumettra des demandes de remboursement de frais de déplacements et loisirs pendant ses vacances.

Retour sur investissement grâce aux découvertes de fraude

Un cabinet de services financiers a identifié une simple fraude sur les notes de frais estimée à 30 000 $ et plus de 200 instances d'activité frauduleuse en seulement un mois. Il s'agit d'un grand cabinet avec beaucoup d'employés qui a fait appel à ACL pour mettre en place une détection de la fraude en continu. Beaucoup de notes de frais d'employés soumis de manière électronique étaient validées. Cette société a en réalité surveillé 3 Go de données tous les jours et traite avec plus de 80 000 fournisseurs dans 16 devises différentes. Cela serait pratiquement impossible sans la bonne technologie. Grâce aux outils d'analyse de données ACL, elle a pu tout de suite identifier une seule fraude sur les frais d'une valeur bien supérieure à 30 000 dollars, et a ensuite identifié plus de 200 cas d'utilisation frauduleuse sur les notes de frais en seulement un mois. Pour détecter la fraude, il faut même faire attention aux petites choses qui se produisent régulièrement. Il s'avère donc indispensable de gagner en efficacité et en organisation.

Grâce aux outils d'analyse de données ACL, ce cabinet a tout de suite identifié une seule et même fraude sur les notes de frais estimée à une valeur bien supérieure à **30 000 dollars.**

7 étapes à suivre pour lancer votre programme de lutte contre la fraude

1) Créez un profil avec une liste répertoriant les différentes zones dans lesquelles une fraude risquerait de se produire ainsi que les types de fraudes possibles. Il pourrait s'agir d'une sorte d'approche descendante concernant les emplacements où la fraude est susceptible d'apparaître dans votre entreprise.

2) Quantifiez le risque de fraude et l'exposition globale pour l'organisation. Traitez les grandes priorités en les surveillant en continu.

3) Réalisez des tests ad hoc pour rechercher des indicateurs de fraude dans ces domaines, puis, à partir de cette analyse, définissez une bonne évaluation des risques et déterminez là où vous allez prêter plus d'attention. Recherchez les modèles et les indicateurs qui apparaissent.

4) Communiquez sur l'activité de surveillance dans toute l'organisation afin que les employés et les fournisseurs puissent être au courant du fait que vous prêtez une grande attention aux événements qui se produisent autour de vous.

5) Avertissez immédiatement votre direction lorsque les choses commencent à mal se passer. Il vaut mieux soulever les problèmes tout de suite plutôt que de devoir rechercher des explications plus tard.

6) Corrigez tout de suite les contrôles rompus. Il est important de bien séparer les tâches. Si je peux initier la transaction, l'approuver et être le destinataire des biens de la transaction, il y a un problème quelque part.

7) Étendez le champ d'application et refaites la même chose.

La technologie de l'analyse de données peut quantifier l'impact de la fraude : elle vous permet d'observer en réalité combien elle coûte à votre organisation et vous fournit un programme rentable avec des résultats immédiats.

À propos d'ACL

ACL fournit des solutions technologiques qui transforment la gestion des audits et des risques. En combinant logiciels et contenu spécialisé, ACL permet de mettre en place des contrôles internes puissants qui identifient et atténuent le risque, protègent les profits et accélèrent les performances.

Animés par un désir d'ouvrir les horizons de la gestion des audits et des risques pour pouvoir offrir une plus grande valeur métier stratégique, nous développons et soutenons une technologie qui renforce les résultats, simplifie l'adoption et améliore la facilité d'utilisation. La gamme intégrée de produits ACL - y compris notre gouvernance cloud, notre solution de gestion des risques et de conformité (GRC) et nos produits d'analyse de données phares - associe tous les éléments essentiels de l'audit et du risque. Ils sont utilisés de manière transparente à tous les niveaux de l'organisation, de la direction supérieure aux professionnels de l'audit et du risque en première ligne et des responsables professionnels avec lesquels ils interagissent. La création de rapports et de tableaux de bord améliorée offre la transparence et le contexte professionnel idéal permettant aux organisations de se concentrer sur ce qui compte vraiment.

Par ailleurs, forts de 25 ans d'expérience alliés à notre approche consultative, nous garantissons des mises en œuvre rapides et efficaces permettant à nos clients d'obtenir des résultats opérationnels concrets rapidement et avec un minimum de risque. C'est notre communauté active et engagée de plus de 14 000 clients dans le monde entier — dont 89 % des entreprises de la liste des 500 du magazine Fortune — qui parle le mieux de notre histoire. En voici quelques-uns.

Rendez-vous en ligne sur www.fr.acl.com

Vous êtes intéressé pour en savoir plus sur nos produits et services ?

Appelez le +33 (0) 1 70 70 79 88 pour parler avec un agent

Consultez notre site Internet sur fr.acl.com

Écrivez-nous à l'adresse info@acl.com