CONFÉRENCE

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

ACFE®
Association of Certified Fraud Examiners
Chapitre français

PARIS, LE 14 AVRIL 2016

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
PARIS

CONFÉRENCE ORGANISÉE PAR
LA COMPAGNIE RÉGIONALE DES COMMISSAIRES
AUX COMPTES DE PARIS ET LE CHAPITRE FRANÇAIS
DE L'ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

SOMMAIRE

OUVERTURE

PAR :

Jean-Luc Flabeau,
président de la compagnie régionale des commissaires aux comptes de Paris.

Frédéric Burband,
vice-président délégué de la compagnie régionale des commissaires aux comptes de Paris.

Francis Hounnongandji,
certified fraud examiner, chartered financial analyst, président ACFE France.

COMMENT UTILISER LES OUTILS D'ANALYSE DE DONNÉES POUR DÉTECTER LES FRAUDES ?

LOGICIELS, FONCTIONNALITÉS ET DÉMARCHE APPLIQUÉS
À LA DÉTECTION DES RISQUES DE FRAUDES.

AVEC LES INTERVENTIONS DE :

Michel Retourné,
diplômé d'expertise-comptable, associé
en charge de l'activité Systèmes d'information & fraude, PKF Ampersand.

Jocelyn Grignon,
associé, audit & sécurité des systèmes d'information, Grant Thornton.

© Photo : Guy Bellinier

LA DÉMARCHE DE DATAMINING EN PRATIQUE

LE CONTRÔLE DES POINTS CLÉS DANS LES PME,
L'AUDIT CONTINU DANS LES GRANDES ENTREPRISES,
DATAMINING ET CONTRÔLE FISCAL.

AVEC LES INTERVENTIONS DE :

Jean-Romain Cure,
certified fraud examiner, ex-global compliance auditor - Nortel, internal audit manager - Puma Energy.

Mauro Molinari,
certified fraud examiner, data mining engineer.

Jocelyn Grignon,
associé, audit & sécurité des systèmes d'information, Grant Thornton.

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

DE GAUCHE À DROITE SUR LA PHOTO : **Michel Retourné,** associé PKF Ampersand en charge des activités Systèmes d'information et prévention et détection des risques de fraude, **Mauro Molinari,** ingénieur des systèmes d'information et fondateur du cabinet de conseil Limmat (certifié CFE et CISA), **Francis Hounnongandji,** président de l'ACFE France, **Jocelyn Grignon,** associé chez Grant Thornton et directeur de l'offre en audit et sécurité des systèmes d'information, **Jean-Luc Flabeau**, président de la Compagnie régionale des commissaires aux comptes de Paris, **Frédéric Burband,** vice-président délégué de la CRCC de Paris, **Jean-Romain Cure,** global audit manager et membre de l'ACFE France. © Photo : Guy Bréhinier

«Face à l'augmentation exponentielle des cas de fraude interne et externe, le regard du commissaire aux comptes en matière de prévention et de détection des risques de fraude est la preuve de l'utilité de sa mission.»

Propos de **Jean-Luc Flabeau,** président de la Compagnie régionale des commissaires aux comptes de Paris, le 14 avril 2016.

OUVERTURE

Jean-Luc Flabeau,
Président de la Compagnie régionale des commissaires aux comptes de Paris.

Cette conférence est organisée en partenariat avec le *Chapitre français de l'Association of Certified Fraud Examiners* (ACFE), la plus grande organisation mondiale de lutte contre la fraude. Face à l'augmentation exponentielle des cas de fraude interne et externe, le regard du commissaire aux comptes en matière de prévention et de détection des risques de fraude est la preuve de l'utilité de sa mission dans les entreprises, notamment dans les PME, moins armées pour lutter contre ce fléau que les grandes entreprises.

Cette conférence constitue le deuxième volet de notre cycle de travail consacré au commissaire aux comptes et aux risques de fraude, ouvert avec la conférence du 6 juillet 2015 « Fraudes aux entreprises : Attaques et Ripostes ». Organisée en partenariat avec l'Ordre des experts-comptables région Paris Ile-de-France, elle a rencontré un vif succès parmi les confrères. Le troisième volet de notre cycle sera constitué d'une journée de formation consacrée à la démarche d'audit en matière de fraude et de blanchiment le 7 juillet 2016.

Frédéric Burband,
vice-président délégué de la CRCC de Paris.

Détecter les risques de fraude fait partie de la mission du commissaire aux comptes, telle qu'elle est prévue par la NEP 240 (Prise en considération de la possibilité de fraudes lors de l'audit des comptes) et la NEP 315 (Analyse circonstanciée du contrôle interne dans le cadre de la prise de connaissance de l'entité et de son environnement).

Le recours à des logiciels d'analyse de données augmente la valeur ajoutée des diligences du commissaire aux comptes et la pertinence de ses travaux. Encore faut-il savoir quels types de données viser, identifier les sources d'informations, structurer la démarche et déterminer les fonctionnalités à mettre en œuvre. D'où l'importance de se former aux nouveaux outils et méthodes de travail associées.

« Le recours à des logiciels d'analyse de données augmente la valeur ajoutée des diligences du commissaire aux comptes.»

Propos de **Frédéric Burband,** vice-président délégué de la CRCC de Paris, le 14 avril 2016.

Francis Hounnongandji,
certified fraud examiner, chartered financial analyst,
président ACFE France.

Les fraudes constituent des activités cachées par nature que seules des analyses plus pointues que celles auxquelles recourent habituellement les audits comptables et financiers standards, sont susceptibles d'en amener la détection. En effet, la détection et la prévention des fraudes requièrent des compétences que le commissaire aux comptes ne maîtrise pas forcément ou ne manipule pas couramment mais qui faciliteraient grandement la mise en oeuvre de ses diligences spécifiques en la matière.

Dans un contexte caractérisé tout à la fois par l'augmentation des risques de fraudes, le formidable développement de l'informatique et des modes d'accès à distance aux données associés à leur constante évolution réglementaire, la recherche des données atypiques et les analyses statistiques requièrent des capacités d'analyse que seuls permettent les outils de datamining. En effet, le recours à des outils informatiques, en complément d'autres techniques d'investigation, offre la possibilité de traiter rapidement l'intégralité des données circonscrites, ce qui serait impossible ou trop long à réaliser manuellement. En conséquence et au vu de l'importance prise actuellement par l'analyse des données et la réglementation fiscale associée aux données informatiques, il devient impératif que le commissaire aux comptes appréhende les atouts et les limites de ces outils, afin d'avoir pleinement conscience des types de fraudes à rechercher et des moyens d'en détecter les éléments d'alerte apparents.

«...il devient impératif que le commissaire aux comptes se familiarise avec ces nouveaux outils et qu'il en appréhende les atouts et les limites.»

Propos de **Francis Hounnongandji,** certified fraud examiner, chartered financial analyst, président ACFE France, le 14 avril 2016.

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

Michel Retourné, diplômé d'expertise-comptable, associé en charge de l'activité Systèmes d'information & fraude, PKF Ampersand. © Photo : Guy Bréhinier

COMMENT UTILISER LES OUTILS D'ANALYSE DE DONNÉES POUR DÉTECTER LES FRAUDES ?

AVEC LES INTERVENTIONS DE :

Jocelyn Grignon,
associé, audit & sécurité des systèmes d'information,
Grant Thornton.

Michel Retourné,
diplômé d'expertise-comptable, associé
en charge de l'activité Systèmes d'information & fraude, PKF Ampersand.

« Les outils d'analyse de données permettent d'aller au cœur des systèmes, là où les fraudeurs ne vont pas...»

Propos de **Michel Retourné,** diplômé d'expertise-comptable, associé en charge de l'activité Systèmes d'information & fraude, PKF Ampersand. le 14 avril 2016

LES FONCTIONNALITÉS DES OUTILS D'ANALYSE DE DONNÉES

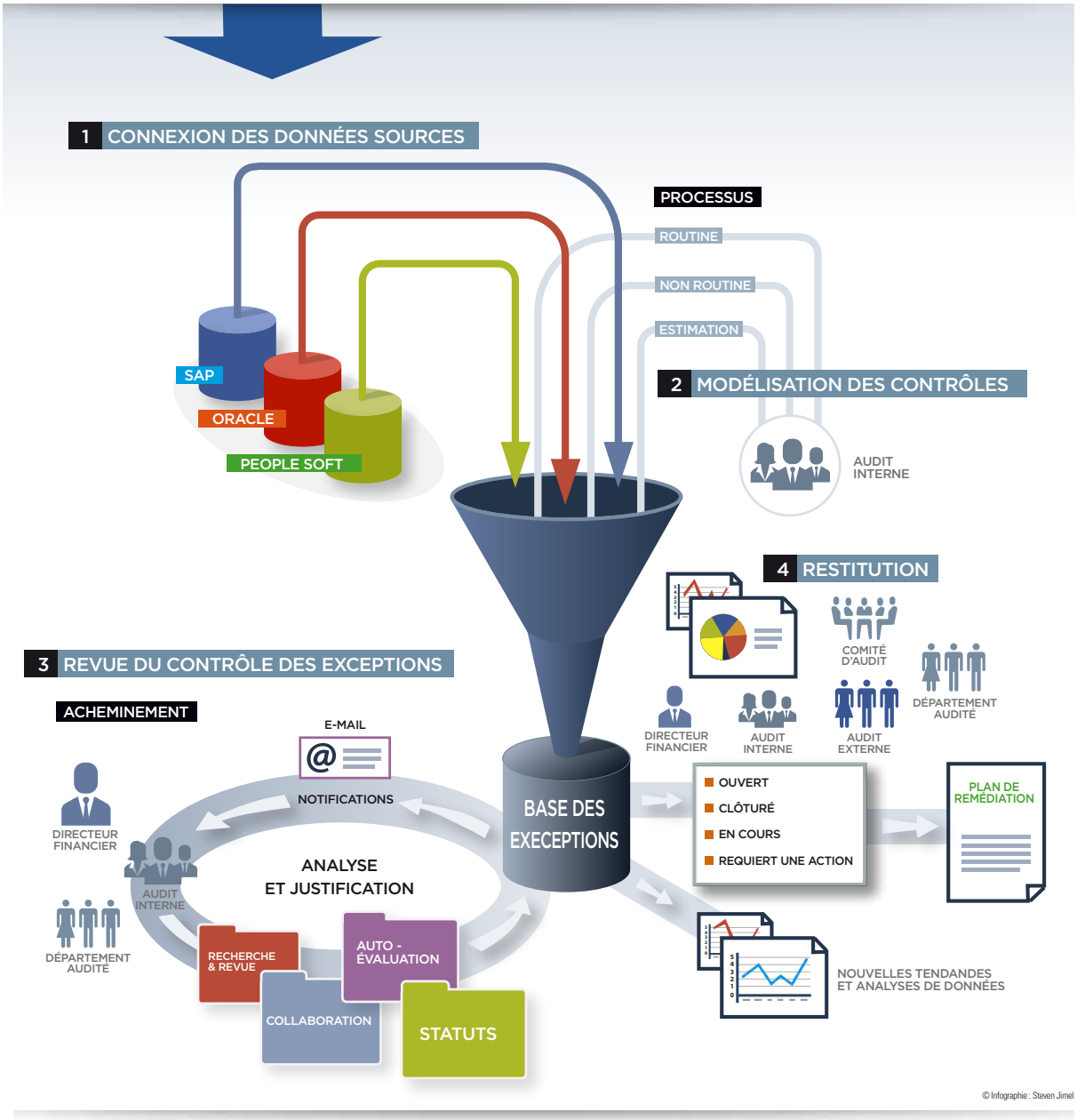
Les fraudeurs cherchent à dissimuler leurs forfaits dans les replis organisationnels de l'entreprise. Or fraudes, erreurs, insuffisances de contrôle interne ou anomalies informatiques laissent des traces durables au sein des systèmes d'information. Les outils d'analyse de données permettent d'aller au cœur de ces systèmes, là où les fraudeurs ne vont pas, et de maximiser les capacités de détection grâce à une analyse exhaustive qui révolutionne la pratique du contrôle.

Tout l'enjeu consiste à transformer des masses de données en quelques lignes de transactions susceptibles d'être révélatrices de fraude, c'est-à-dire d'exceptions.

Cette démarche se déroule en 4 temps : il faut tout d'abord accéder aux données sources en fonction de l'analyse des risques, modéliser les contrôles permettant de vérifier les risques et analyser le caractère potentiellement frauduleux des exceptions remontées, effectuer une revue du contrôle des exceptions et vérifier les résultats avec l'entreprise avant de restituer l'information aux parties prenantes.

Jocelyn Grignon, associé, audit & sécurité des systèmes d'information, Grant Thornton. © Photo : Guy Bréhinier

LES 4 TEMPS FORTS DE L'ANALYSE DE DONNÉES



Ces outils d'analyse de données sont dotés d'un large panel de fonctionnalités. Ils ont la capacité de brasser l'ensemble du patrimoine informationnel de l'entreprise et permettent de s'affranchir des questions de seuils et des approches « statistiques » grâce à la portée exhaustive des analyses. En s'appuyant sur des Key Risk Indicators (tendances) ou sur la recherche d'exceptions, ils permettent de mettre en évidence les zones de risques ou fournissent directement les anomalies à investiguer.

Lorsqu'un contrôle se révèle efficace, ils offrent la possibilité de le reproduire et de le généraliser. Enfin, ils n'affectent pas les données et offrent une traçabilité.

« Dotés d'un large panel de fonctionnalités, ces outils d'analyse n'affectent pas les données et offrent une traçabilité. »

Propos de **Jocelyn Grignon,** associé, audit & sécurité des systèmes d'information, Grant Thornton, le 14 avril 2016

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

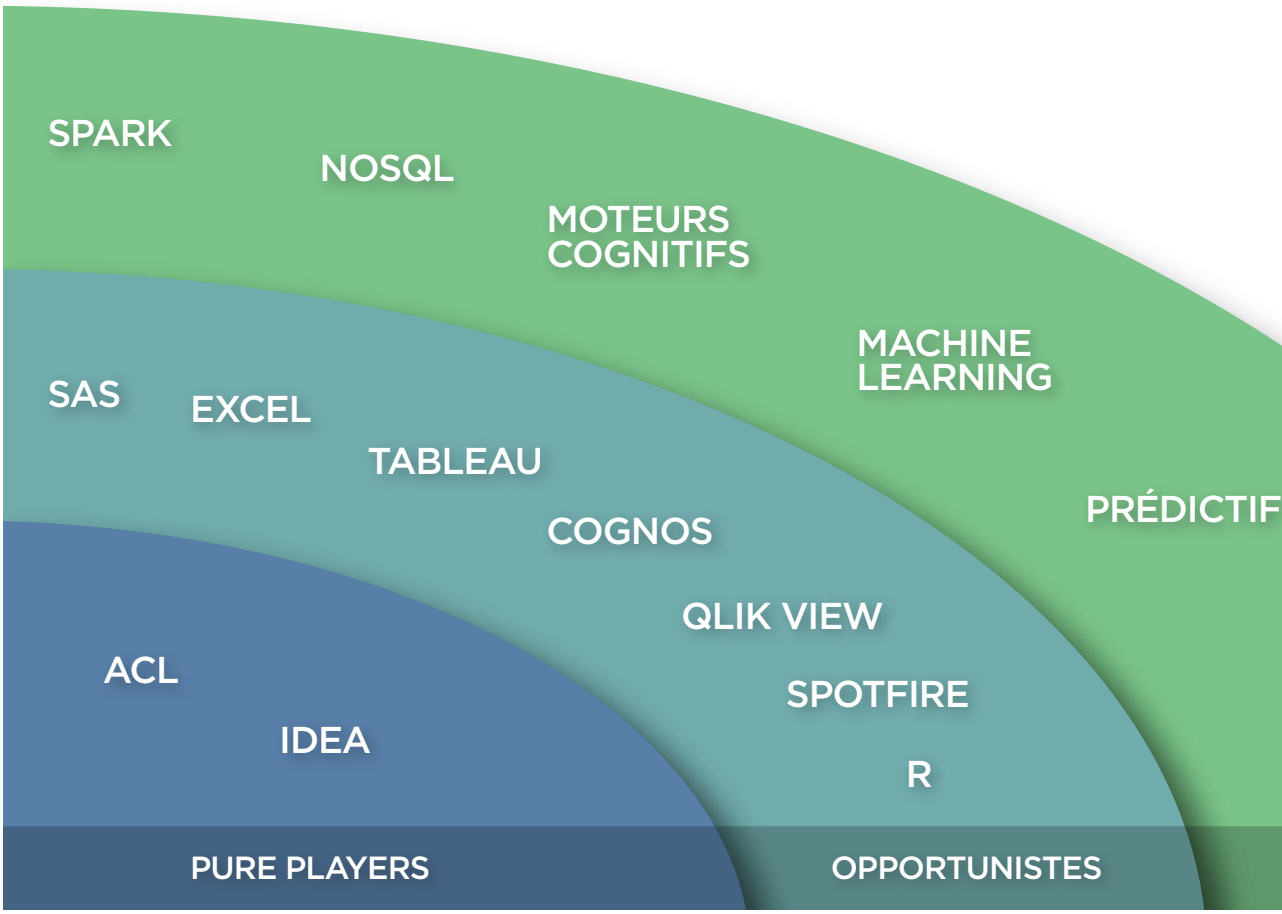
© Photo : Guy Bréhinier

LES PRINCIPAUX LOGICIELS UTILISÉS POUR LA DÉTECTION DE FRAUDES

Sur le marché coexistent aujourd'hui des logiciels développés spécifiquement pour les auditeurs externes et internes (pure players), des logiciels aux fonctionnalités plus larges (opportunistes) et des outils émergeants dédiés aux problématiques de gestion du «big data » tels que des moteurs cognitifs, des outils d'intelligence artificielle voire de machine learning (apprentissage automatique) ou d'analyse de signaux faibles.

«Pure Players, Opportunistes ou Emergeants... des logiciels disponibles pour les auditeurs »

[NDLR]



© Photo : Guy Bréhinier

LA DÉMARCHE D'UTILISATION DU DATAMINING DANS LES SITUATIONS À RISQUE ÉLEVÉ

UN LOGICIEL DE DATAMINING ADAPTÉ AU TRAVAIL DE L'AUDITEUR DOIT PROPOSER LES FONCTIONNALITÉS SUIVANTES :

- la capacité à traiter de larges volumes de données en quelques minutes et à fournir une visualisation graphique des données collectées,
- la disponibilité en standard des fonctionnalités nécessaires à l'analyse de données,
- la traçabilité des travaux (ce qui exclut les tableurs),
- la capacité à être utilisé sans être un spécialiste IT.

CE LOGICIEL PERMET D'ANALYSER DEUX TYPES DE DONNÉES :

- des données structurées, c'est-à-dire déjà organisées en lignes et colonnes (bases de données, feuilles de tableur, listes, écritures comptables, journal de paie, inventaire permanent de stock, etc.),
- des données non structurées, c'est-à-dire non présentables sous forme de tableau (emails, factures, courriers, sms, etc.).

Les données se présentent sous la forme de caractères alphanumériques (fichiers) mais aussi sous la forme d'enregistrements de conversation, de photos, de vidéos, etc., pouvant requérir l'expertise complémentaire d'un spécialiste.

«L'absence de mise en place de système de contrôle en continu au sein d'une entreprise appelle à la vigilance car cela peut être la porte ouverte à des fraudes.»
... / ...
«Il faut rechercher l'existence ou l'absence d'indices de fraudes .»

Propos de **Jocelyn Grignon,** associé, audit & sécurité des systèmes d'information, Grant Thornton, le 14 avril 2016

SIGNAUX FAIBLES

EMERGEANTS

LA TECHNOLOGIE
AU SERVICE DE
LA DÉTECTION DES FRAUDES

Michel Retourné, diplômé d'expertise-comptable,
associé en charge de l'activité Systèmes d'information & fraude, PKF Ampersand.
© Photo : Guy Bréhinier

LA DÉMARCHE D'UTILISATION DU DATAMINING DANS LES SITUATIONS À RISQUE ÉLEVÉ

«Un grand soin est à porter sur la planification et la préparation car elles représentent 80% de la démarche.»

[NDLR]

LA DÉMARCHE D'UTILISATION DU DATAMINING S'INSÈRE DANS LA NEP 240. APRÈS AVOIR IDENTIFIÉ UN RISQUE DE FRAUDE, IL CONVIENT DE METTRE EN ŒUVRE UNE DÉMARCHE EN QUATRE PHASES QUI CONSISTE À :

- **1 / PLANIFIER :** cette phase est la clé de la réussite.
  Une requête efficace requiert une bonne identification des données disponibles, une définition précise des objectifs et du périmètre de l'audit à couvrir avec l'outil et une identification claire des indices à rechercher.

- **2 / PRÉPARER :** cette phase consiste à identifier les données pertinentes, obtenir du client les données à analyser, ce qui nécessite d'anticiper la demande, vérifier la qualité des données obtenues, les nettoyer et les normaliser.

  CES DEUX PHASES REPRÉSENTENT 80% DU TEMPS À CONSACRER À LA DÉMARCHE.

- **3 / TESTER LES DONNÉES ET INTERPRÉTER LES RÉSULTATS OBTENUS :**
  il faut rechercher l'existence ou l'absence d'indices de fraudes et rester en alerte d'indices non identifiés. Si la requête révèle trop d'anomalies, il convient de s'interroger sur la qualité du test réalisé.

- **4 / ANALYSER :** cette dernière phase consiste à exploiter les indices par des interviews, une revue de documents, etc. Elle se conclut par la rédaction d'un rapport d'analyse des données dans un langage compréhensible par tous et la recommandation de contrôles en continu ou périodiques.

CONFÉRENCE

© Photo : Guy Bréhinier

L'absence de mise en place de système de contrôle en continu au sein d'une entreprise appelle à la vigilance car cela peut être la porte ouverte à des fraudes.

A contrario, l'existence d'un tel système témoigne d'une réelle politique de gestion des risques de fraudes et des erreurs en temps réel.

«un tel système témoigne d'une réelle politique de gestion des risques de fraudes.»

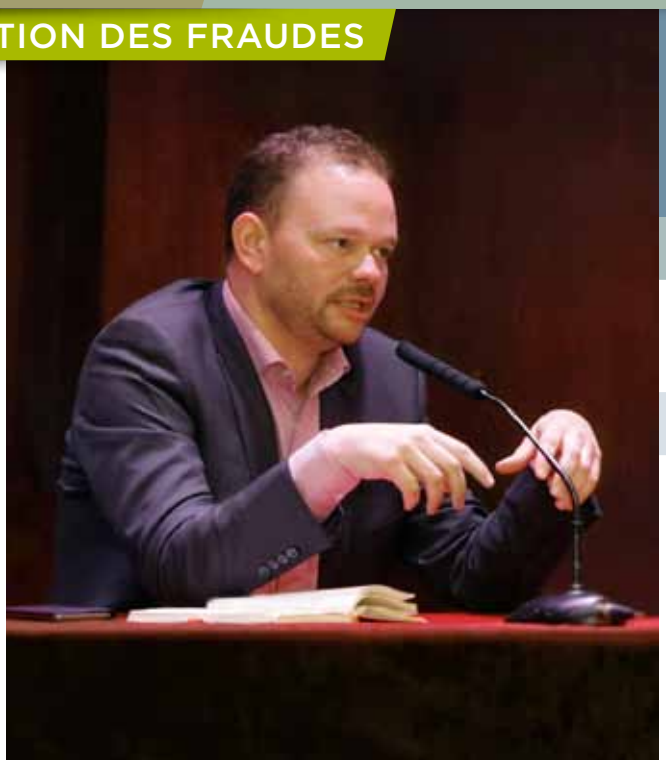
Propos de **Jocelyn Grignon,** associé, audit & sécurité des systèmes d'information, Grant Thornton, le 14 avril 2016

Conférence organisée par la Compagnie régionale des commissaires aux comptes de Paris et le Chapitre français de l'Association of Certified Fraud Examiners (ACFE).

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
PARIS

ACFE
Association of Certified Fraud Examiners
Chapitre français

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES



Jocelyn Grignon,
associé, audit & sécurité
des systèmes d'information,
Grant Thornton.
© Photo : Guy Bréhinier

«Les logiciels de datamining servent aussi à contrôler la facturation, calculer des valorisations de droits sociaux, des variations de stocks, provisions, etc.»

Propos de **Jocelyn Grignon,** associé, audit & sécurité des systèmes d'information, Grant Thornton, le 14 avril 2016

QU'EST-CE QUE LE DATAMINING ?

C'est un outil informatique d'exploration de données à même de trouver des structures originales et des corrélations informelles entre les données. Il permet de mieux comprendre les liens entre des phénomènes en apparence distincts, voire d'anticiper des tendances encore peu discernables. Utilisé pour explorer les grands volumes de données, ses domaines d'application s'étendent du secteur médical/pharmaceutique (explication ou prédiction de la réponse d'un patient à un traitement, identifications de thérapies à succès…), à celui de banque/finance (gestion du risque lié à l'attribution de prêts par scoring, détection de règles de comportement boursier par l'analyse des données du marché, détection d'usage frauduleux de cartes bancaires…), ou encore de la vente/marketing (détection d'associations de comportement d'achats, identification de profil de prospects…). Dans sa lutte contre la fraude aux finances publiques, la DNLF (Délégation Nationale à la Lutte contre la Fraude) a mis en place un groupe de travail interministériel dédié au datamining qui associe les administrations financières et les organismes de protection sociale.

UN LOGICIEL DE DATAMINING SERT-IL À D'AUTRES CONTRÔLES ?

Au-delà de la recherche de fraude, ces logiciels sont utiles pour auditer une masse importante de données. Ils servent à contrôler la facturation, calculer des valorisations de droits sociaux, des variations de stocks, provisions, etc., exploiter des écarts. L'exploitation des logs (rechercher qui s'est connecté sur quel dossier, pendant combien de temps, etc.) permet de rapprocher temps passé et niveau de facturation, et d'identifier d'éventuels problèmes. De même, il peut conduire à vérifier la séparation des fonctions : certaines personnes peuvent avoir des droits d'accès qu'elles n'ont pas vocation à utiliser car en dehors de leur champ d'actions.

© Photo : Guy Bréhinier

LA DÉMARCHE DE DATAMINING EN PRATIQUE

AVEC LES INTERVENTIONS DE :

Jean-Romain Cure,
certified fraud examiner, ex-global compliance auditor - Nortel,
internal audit manager - Puma Energy.

Mauro Molinari,
certified fraud examiner, data mining engineer.

Jocelyn Grignon,
associé, audit & sécurité des systèmes d'information,
Grant Thornton.

LE DATAMINING ET LES CONTRÔLES CLÉS DANS LES PME

Les outils de datamining permettent de mettre en place un audit continu et de réaliser quelques contrôles critiques à la portée des PME.

LES CAS SUIVANTS PRÉSENTENT DE FORTES PRÉSOMPTIONS DE FRAUDE :

- trésorerie : rapprochements bancaires incomplets ou forte densité des flux comptables de trésorerie non lettrés avec le compte bancaire,
- clients ventes : encaissements non lettrés (une bonne vente est une vente encaissée),
- achats fournisseurs : paiements non lettrés, modification des références bancaires fournisseurs, commandes a posteriori,
- stocks : expéditions sans facturation (risque de fraude directe par perte de marchandise commerciale), vérifiables par les états de sortie de stock et éventuellement par les inventaires,
- réceptions sans facturation : risque de conflits avec les fournisseurs, de détournement,
- personnel : avances de salaire non apurées, rapprochement de la paie avec les présences, apurement des avances sur missions avec les notes de frais,
- opérations diverses (OD) : utilisation abusive du journal d'OD pour contourner les contrôles sur les journaux auxiliaires (e.g. vente, paie, trésorerie).

«Les outils de datamining permettent de mettre en place un audit continu et de réaliser quelques contrôles critiques à la portée des PME.»

Propos de **Jean-Romain Cure,** certified fraud examiner, le 14 avril 2016

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

Mauro Molinari, certified fraud examiner, data mining engineer.

LE DATAMINING DANS LES CONTRÔLES FISCAUX

«Certains logiciels de caisse permissifs permettent de retirer des lignes de vente avant l'édition du journal de bord contenant le cumul des ventes de la journée, ouvrant la voie à des fraudes par le gérant voire à des vols d'espèces par les salariés»

Propos de **Mauro Molinari,** certified fraud examiner, data mining engineer, le 14 avril 2016

Dans le cadre d'un contrôle fiscal, se pose la question des fraudes internes pouvant mener à des redressements. En cas de contrôle fiscal des comptabilités informatisées, la présentation dématérialisée de la comptabilité et du fichier des écritures comptables (FEC) est obligatoire. Le format du FEC est imposé par l'administration fiscale qui, à partir de ce fichier, réalise des opérations afin de vérifier la concordance des documents comptables avec les déclarations fiscales déposées et de détecter d'éventuelles incohérences.

LE FEC, UN OUTIL MAL ADAPTÉ À LA RECHERCHE DE FRAUDES

Dans le cadre de ses contrôles, il appartient au commissaire aux comptes de vérifier que la société puisse produire le FEC et qu'il soit exploitable par l'administration fiscale (validation de la forme et du contenu). Le FEC doit être une photo de l'activité de l'entreprise. Toutefois, comme il n'est que le reflet de la comptabilité, un certain nombre d'éléments qui concourent directement ou indirectement au résultat n'y figurent pas (en fonction du niveau d'auxiliarisation des données). Si le commissaire aux comptes peut utiliser le FEC pour tester les procédures comptables ou les OD, il doit aussi en connaitre les limites s'il envisage d'identifier plus largement les anomalies et les fraudes car ce fichier ne rassemble pas toutes les données produites par l'entreprise.

PRENDRE EN COMPTE LES LOGICIELS DE CAISSE

Le périmètre d'investigation comprend la comptabilité générale et d'autres logiciels tels que des logiciels métier qui contiennent des données importantes pour la comptabilité (ex : chez les opérateurs telecoms, analyse de la correspondance entre les systèmes de gestion des appels et les résultats comptabilisés en fin de journée).

Le commerce de détail, les entreprises du secteur de la distribution ou les cafés, hôtels, restaurants utilisent des logiciels de caisse. Ces logiciels, qui enregistrent les ventes de la journée, font partie du système d'information de l'entreprise d'un point de vue comptable et fiscal. Or, ils ne sont pas supervisés par l'expert-comptable et souvent ne présentent pas d'interface avec le logiciel que celui-ci utilise. Certains logiciels de caisse permissifs permettent de retirer des lignes de vente avant l'édition du journal de bord contenant le cumul des ventes de la journée, ouvrant la voie à des fraudes par le gérant voire à des vols d'espèces par les salariés (cf. détournement de fonds dans l'opération

Jean-Romain Cure, certified fraud examiner, ex-global compliance auditor - Nortel, internal audit manager - Puma Energy.

Caducée). Contrôler la correspondance entre le journal de bord de la caisse et la comptabilité générale reste difficile même s'il est possible de retrouver des traces de ces manipulations dans les systèmes informatiques en effectuant des investigations poussées. Pour s'assurer que le journal de bord correspond bien à l'activité de la société, il sera obligatoire, à partir de 2018, d'utiliser un logiciel de gestion ou un logiciel de caisse certifié, satisfaisant aux conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données, attestées par un certificat délivré par un organisme accrédité ou par une attestation individuelle délivrée par l'éditeur.

LE DATAMINING ET L'AUDIT CONTINU DANS LES GRANDES ENTREPRISES

L'audit continu est une approche simplifiée mais systématique de l'audit interne, basée sur des rapports d'exceptions automatiques et une communication « à flux tendu » : les exceptions sont directement envoyées aux usagers.

Seul un réel engagement de la direction garantira son effectivité. La démarche est dématérialisée, la plupart des transactions se faisant en ligne et en temps réel. Elle est assez rigide d'un point de vue disciplinaire : elle laisse peu de place pour les exceptions aux processus-clés, ne permet aucune clôture simplifiée, laisse peu de comptes en suspens.

QUELQUES EXEMPLES D'OUTILS DE L'AUDIT CONTINU

- Outils de datamining intégrant les fonctionnalités d'audit continu (automatismes et workflow).
- Un ERP global qui touche tous les domaines de l'ensemble : Comptabilités Générale et Auxiliaires, Achats, Immobilisations, Trésorerie...
- Informatique RH : Administration du Personnel.
- Logiciels experts Opérations : mesures statiques (stocks) et dynamiques (flux entrants et sortants).
- Tableaux de bord : Ventes, Crédit, Stocks… y compris des tableaux spécifiques à l'audit.
- Requêteur : Outil utilisé avec les ERP qui génère des rapports d'exception à partir de grands volumes de données.

«L'objectif est d'observer chaque transaction afin de décourager les fraudeurs.»

Propos de **Jean-Romain Cure,** certified fraud examiner, le 14 avril 2016

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

Jean-Romain Cure,
certified fraud examiner, ex-global compliance auditor - Nortel, internal audit manager - Puma Energy.

«Les systèmes d'audit continu prédictifs offrent la possibilité d'identifier ce qui ne ressort pas comme exception mais reste anormal.»

Propos de **Jean-Romain Cure,** certified fraud examiner, ex-global compliance auditor - Nortel, internal audit manager - Puma Energy, le 14 avril 2016

UNE BONNE DÉTECTION DES INDICATEURS DE FRAUDE

L'audit continu couvre un large domaine d'applications. Cela permet de suivre les exceptions générées sur une base quotidienne, hebdomadaire, mensuelle ou trimestrielle dans un grand nombre de domaines et offre une bonne détection des fraudes. A titre d'exemple, il est possible de repérer les pertes excessives en dépôt ou en transit, les « écritures insensées » (dates comptables futures, lieux de stockage sans marchandise mais avec une valeur...) et les marges insolites, de lister les paiements non lettrés (émis ou reçus), de pister les rapprochements bancaires tardifs, de vérifier les avances au personnel abusives ou non soldées.
Les systèmes d'audit continu prédictifs offrent la possibilité d'identifier ce qui ne ressort pas comme exception mais reste anormal, tels que des limites de crédit éphémères, des états de stocks "trop beaux pour être vrais". L'objectif est d'observer chaque transaction afin de décourager les fraudeurs mais aussi d'accompagner ceux qui font des erreurs.

DOMAINES D'APPLICATION DE L'AUDIT CONTINU

- Rapprochements bancaires
- Flux de trésorerie non lettrés
- Réconciliations GL/Auxiliaires
- Écritures directes au GL
- Écritures clients non lettrées
- Créances échues
- Débloqueur de crédit
- Limites de crédit éphémères
- Paramètres clients
- Commandes a posteriori
- Fournisseurs à solde débiteur
- Saisie tardive des factures
- Écritures fournisseurs non lettrées
- Factures fournisseurs bloquées
- Paramètres fournisseurs
- Références bancaires fournisseurs
- Marchandise expédiée non facturée
- Stocks en transit
- Revalorisation des stocks
- Marchandise reçue non facturée
- Ajustements de stock (ou pas...)
- Stocks à faible rotation/négatifs
- Base de données dynamiques des opérations
- Immobilisations – valeur nette négative
- Immobilisations – en-cours à plus de 5 mois
- Soldes comptables des employés
- Profils des employés dans le logiciel de paie
- Profils des usagers (ERP)
- Droits d'accès réseau (active directory)
- Intérimaires et prestataires
- Intégrité des comptes consolidés
- Marchandise - valeurs unitaires insolites
- Marchandise - marges sur ventes insolites

UNE COMPLÉMENTARITÉ AVEC L'AUDIT INTERNE

L'audit continu offre une bonne complémentarité avec l'audit interne. La communication immédiate et permanente des informations permet à l'audit interne de mieux définir et gérer ses priorités. Par exemple, donner la priorité aux éléments physiques/matériels et faire des recommandations d'amélioration.

Il permet également de développer des bonnes pratiques et d'affiner les procédures de l'entreprise. Les utilisateurs deviennent plus vigilants et peuvent s'auto-contrôler (ils peuvent relancer les extractions par eux-mêmes). Les contrôles préventifs informatiques sont plus efficaces (règles d'accès, «placer les serrures loin des portes»). En cas d'intégration de nouvelles entités, la propagation d'outils communs est plus rapide.

LA COOPÉRATION AUDITEUR – ENTREPRISE : LE DATAMINING FAIT CAUSE COMMUNE

Le datamining présente des bienfaits mais aussi des limites pour les auditeurs externes. Cela requiert des compétences spécifiques ou en tout cas une aisance avec les outils informatiques pour manipuler ces technologies, et de tels profils sont rares sur le marché. Il n'est pas toujours aisé d'accéder à la donnée chez les clients, ni de vérifier que les données fournies sont bien celles demandées et qu'elles sont utilisables. Mener à bien ces analyses exige du temps dans un agenda contraint. Lorsque des risques de fraudes sont identifiés, les communiquer au client, dans la phase post analyse, peut s'avérer délicat.

Devant certaines de ces difficultés, une grande entreprise a déployé une initiative innovante pour accompagner la démarche et non la subir. En effet, elle trouvait l'approche pertinente mais les équipes souffraient des demandes répétées des commissaires aux comptes. Le projet a consisté à connecter l'ensemble des systèmes de production en vue d'automatiser la révision comptable et mettre en place une plateforme commune avec les commissaires aux comptes.

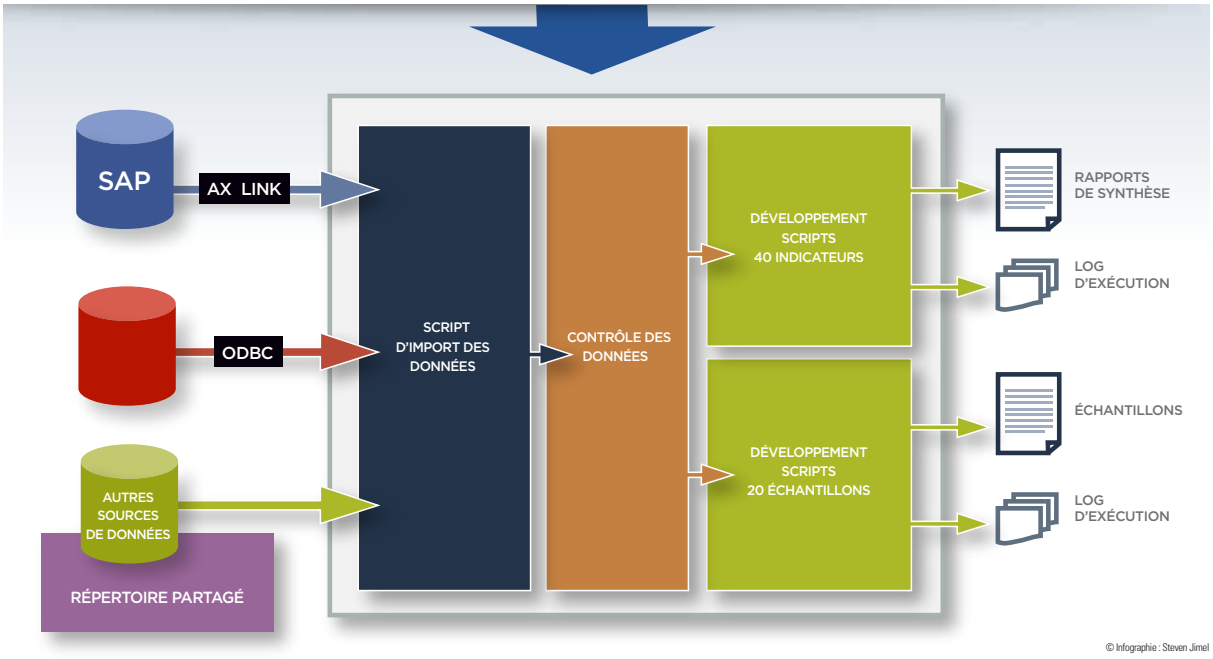
Résultat : les relations entreprise/commissaires aux comptes sont plus transparentes et les contrôles plus pertinents. 32 millions d'ecritures comptables sont, en moyenne, testées tous les jours grâce à une plateforme facile à utiliser et peu coûteuse à développer. Les contrôles sont optimisés : l'entreprise dispose de 40 indicateurs et de 20 échantillons examinés de manière hebdomadaire, partagés dans les dossiers de révision. Autre conséquence : le nombre de réviseurs comptables a été divisé par deux.

«Lorsque des risques de fraudes sont identifiés, les communiquer au client, dans la phase post analyse, peut s'avérer délicat.»

Propos de **Jocelyn Grignon,** associé, audit & sécurité des systèmes d'information, Grant Thornton, le 14 avril 2016

LA TECHNOLOGIE AU SERVICE DE LA DÉTECTION DES FRAUDES

EXEMPLE DE PLATEFORME MIXTE ENTREPRISE / CAC



«Moins de 1% d'écritures contrôlées par 90 réviseurs comptables, contre un contrôle systématique pour seulement 45 réviseurs comptables pour un résultat totalement transparent.»

Propos de **Jocelyn Grignon,** associé, audit & sécurité des systèmes d'information, Grant Thornton, le 14 avril 2016

AVANT

90

RÉVISEURS COMPTABLES

☛ MOINS DE 1% D'ÉCRITURES CONTRÔLÉES

APRÈS

45

RÉVISEURS COMPTABLES

☛ CONTRÔLES SYSTÉMATIQUES

☛ RÉSULTATS TRANSPARENTS

Jocelyn Grignon,
associé, audit & sécurité
des systèmes d'information,
Grant Thornton.
© Photo : Guy Bréhinier

COMMENT FORMULER SA REQUÊTE ET IDENTIFIER LE BON INTERLOCUTEUR DANS L'ENTREPRISE ?

Formuler simplement sa question reste un gage de compréhension. A qui poser la bonne question ? L'interlocuteur idéal n'est sans doute pas l'interlocuteur traditionnel du commissaire aux comptes mais plutôt celui qui saura traduire la requête aux informaticiens, c'est-à-dire faire l'interface entre l'audit et l'informatique. Il est également important d'identifier la personne qui connaît l'architecture des différents objets de la base de données. Le dictionnaire détaillé des objets est à cet égard une donnée clé. Dans tous les cas, il est nécessaire de s'assurer que les données fournies sont celles attendues, d'où le besoin d'anticiper sa demande dans le cadre de ses travaux.

«Il est important d'identifier la personne qui connaît l'architecture des différents objets de la base de données.»

Propos de
Jean-Romain Cure,
certified fraud
examiner,
le 14 avril 2016

ACFE
Association of Certified Fraud Examiners
Chapitre français

L'ACFE EN BREF

L'Association of Certified Fraud Examiners (ACFE) est une association internationale spécialisée dans la formation et la professionnalisation en matière de lutte contre la fraude. C'est la seule institution habilitée à délivrer la certification CFE (Certified Fraud Examiner) reconnue par les professionnels du monde entier. Elle rassemble plus 75 000 professionnels de la lutte contre la fraude toutes spécialités et organisations confondues (entreprises, cabinets de conseil, institutions publiques et organisations non gouvernementales), notamment : experts-comptables, auditeurs, juristes et avocats, consultants, universitaires, agents gouvernementaux.

Le chapitre français, présidé par Francis Hounnongandji, certified fraud examiner, chartered financial analyst, met à la disposition de ses membres des ressources de référence sur le thème de la fraude, et organise des formations et des conférences.

FIN DU DOCUMENT

COMPAGNIE RÉGIONALE
DES COMMISSAIRES AUX COMPTES
DE PARIS / CRCC-PARIS.FR
50 RUE DE LONDRES - 75008 PARIS - TÉL. : 01 53 83 94 33

CRCC
COMPAGNIE
REGIONALE DES
COMMISSAIRES AUX
COMPTES
PARIS