CRIPP

Cadre de Référence International des Pratiques Professionnelles

Lignes directrices complémentaires

Guide pratique

Planification de la mission

Évaluation des risques de fraude

The Institute of Internal Auditors | Global

Table des matières

Synthèse 3

Introduction 4

Comprendre la fraude 5

Collecter les informations 7

- Évaluations et investigations précédentes 7
- Dispositifs d'alerte formels et entretiens 8
- Analyse préliminaire de l'environnement de contrôle 9
- Recours à des études externes et à des experts 10

Organiser des brainstorming sur les scénarios de fraude 10

Évaluation des risques de fraude 13

- Identifier les contrôles 15

Annexe A. Normes et lignes directrices de l'IIA 17

Annexe B. Glossaire 18

Annexe C. Exemples d'actes frauduleux 19

Annexe D. Termes à considérer comme des signaux d'alerte potentiels 21

Annexe E. Étude de cas : Mission d'assurance relative aux décaissements 22

Remerciements 26

Synthèse

La fraude peut perturber les activités, présenter des risques en matière de conformité, entacher la réputation d'une organisation et avoir des conséquences financières non négligeables pour cette dernière et ses parties prenantes. Alors que la direction générale, sous la supervision du Conseil, détient la responsabilité principale de la mise en place et du suivi d'un dispositif de contrôle efficace pour prévenir et détecter les fraudes, la fonction d'audit interne est tenue d'évaluer le risque de fraude, conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*). En outre, le responsable de l'audit interne doit rendre compte des risques significatifs, y compris les risques de fraude, et des contrôles correspondants à la direction générale et au Conseil (Norme 2060 – Communication à la direction générale et au Conseil).

Les *Normes* exigent de la fonction d'audit interne qu'elle évalue les risques de fraude au niveau de l'organisation ainsi qu'au niveau de la mission. Afin de garantir un examen adéquat des risques liés à chaque mission, les auditeurs internes devraient procéder à une évaluation des risques de fraude dans le cadre de la planification de la mission (Norme 2210.A1). Les connaissances acquises par la fonction d'audit interne au fil de certaines missions peuvent être compilées afin de réaliser une évaluation des risques de fraude plus solide et plus complète au niveau de toute l'organisation.

Ce guide pratique décrit les caractéristiques de la fraude et le processus d'identification et d'évaluation des risques de fraude lors de la planification de la mission. Les modalités précises d'intégration d'une évaluation des risques de fraude dans la planification de la mission peuvent varier selon les besoins de l'organisation, de la fonction d'audit interne et de la mission. Toutefois, le processus comprend généralement les étapes suivantes :

- Collecter les informations afin de comprendre le but et le contexte de la mission, ainsi que les processus pertinents de gouvernance, de management des risques et de contrôle relatifs au domaine ou processus audité.
- Organiser des *brainstorming* sur des scénarios de fraude afin d'identifier des risques potentiels de fraude.
- Évaluer les risques de fraude identifiés afin de déterminer quels risques nécessitent une évaluation plus approfondie pendant la mission.

Introduction

La fonction d'audit interne est chargée d'évaluer les processus de management des risques de l'organisation et leur efficacité, y compris l'évaluation des risques de fraude ainsi que la manière dont les risques sont gérés par l'organisation (Norme 2120.A2). Toutefois, l'évaluation des possibilités de fraude lors de la planification de chaque mission est tout aussi importante, dans la mesure où de nouveaux risques de fraude peuvent survenir à tout moment. Par conséquent, les auditeurs internes doivent tenir compte de la probabilité de fraude quand ils élaborent les objectifs de chaque mission (Norme 2210.A2).

Effectuer une évaluation des risques de fraude au début de chaque mission permet aux auditeurs internes de découvrir des risques de fraude qui n'étaient peut-être pas présents lors de la dernière mise à jour de l'évaluation des risques au niveau de l'organisation. En outre, des risques de fraude qui peuvent être insignifiants à l'échelle de l'organisation peuvent revêtir un caractère significatif dans un domaine ou processus précis.

Alors que les auditeurs internes doivent disposer des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation, ils ne sont pas censés posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes (Norme 1210.A2). Lors de l'évaluation des risques de fraude, les auditeurs internes doivent faire preuve de conscience professionnelle (Norme 1220.A1) et avoir une attitude impartiale et non biaisée (Norme 1120 – Objectivité individuelle). Les auditeurs internes doivent également faire preuve de scepticisme professionnel – état d'esprit curieux, non biaisé, qui ne présume pas de l'honnêteté intrinsèque du management ou des collaborateurs – dans la mesure où il permet une évaluation objective et critique du domaine ou processus audité.

Ce guide pratique donne un bref aperçu des caractéristiques de la fraude, puis présente la façon d'évaluer les risques de fraude dans le cadre de la planification de la mission. Il décrit comment collecter des informations, organiser des *brainstorming* sur les scénarios de fraude, identifier les risques de fraude et évaluer leur importance afin de déterminer quels risques de fraude devraient être évalués pendant la mission.

Comprendre la fraude

Parmi les nombreuses définitions, L'IIA définit la fraude comme « tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance ». La définition reflète ce qui fait de la fraude un risque particulier : l'intention. Les actes frauduleux impliquent des personnes dont l'intention est de contourner les dispositifs de contrôle ou d'exploiter les faiblesses de l'organisation. L'IIA ajoute également dans sa définition que « les fraudes sont perpétrées afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou lié à leur activité ».

Parce que les lois varient, la légalité d'un acte frauduleux peut être remise en question. Par exemple, une organisation multinationale, dont le siège est dans un pays où un acte est considéré comme illégal, pourra faire des affaires dans d'autres pays où le même acte ne viole pas les lois locales. Peu importe les distinctions juridiques, l'évaluation des risques de fraude vise à identifier la probabilité d'abus de confiance, d'exploitation des faiblesses et de contournement des contrôles.

Trois facteurs sont toujours présents lorsque des fraudes sont commises : la pression ou l'incitation, la perception d'une opportunité et la rationalisation.[1]

Pression ou incitation – Un besoin réel ou apparent qui fournit une raison ou un motif, comme :

- la nécessité d'atteindre des objectifs de performance fixés par l'organisation ou d'ordre financier ;
- des difficultés personnelles ou des facteurs de stress externes (ex : problèmes financiers, de santé ou d'addiction) ;
- le désir d'avoir du pouvoir, de l'influence, l'estime de sa famille, ses amis, ses collègues ou de la direction (ex : les pirates informatiques qui fraudent avec l'intention de faire état de leurs capacités plutôt que de causer des dommages).

Opportunité – Une combinaison de circonstances ou de conditions qui donnent l'opportunité de commettre une fraude, telles que :

- une mauvaise conception des contrôles, l'absence de contrôles, des mécanismes de sécurité ou une séparation des tâches insuffisants, ou d'autres circonstances qui rendent possible une défaillance des contrôles ;
- un niveau de confiance, d'autorité, de connaissances et/ou d'accès aux processus de contrôle qui permettent aux collaborateurs de contourner ou d'outrepasser les contrôles existants ;
- une supervision, une formation ou une communication inadaptées concernant les règles de conduite professionnelles ainsi que les conséquences en cas de violations.

1 Cressey, D.R. « The Criminal Violation of Financial Trust », *American Sociological Review*, 15, n ° 6 (1950) : 738-743.

Rationalisation – Une justification inventée, convaincante et plausible, telle que :

- le sentiment d'un dû lié à un engagement envers l'organisation (ex : titularisation, nombre excessif d'heures non rémunérées, ou performance non récompensée) ;
- la conviction de l'acceptabilité des actions parce que « d'autres le font probablement aussi » ;
- la conviction de l'acceptabilité des actions parce qu'elles sont culturellement courantes ou ont été jugées comme telles dans des organisations précédentes ;
- la croyance selon laquelle les politiques et les procédures n'ont aucun sens ou ne sont pas justifiées ;
- la croyance selon laquelle les actions sont temporaires et/ou constituent un événement unique (par exemple : « emprunter de l'argent qui sera remboursé ensuite » ou « juste pour cette fois ») ;
- la croyance selon laquelle l'action ne fera aucune victime ou sera si insignifiante que personne ne la remarquera et/ou ne s'en souciera.

Parmi ces trois facteurs, les organisations ne peuvent exercer de contrôle direct que sur celui de l'opportunité. Le management peut concevoir des dispositifs de contrôle interne pour essayer de prévenir ces opportunités de fraude et détecter les activités frauduleuses si elles sont commises.

Les auditeurs internes doivent noter que ceux qui s'engagent dans des activités frauduleuses peuvent rationaliser leur fraude non seulement pour leur propre bénéfice, mais aussi pour le bénéfice de leur organisation, d'individus et d'organisations externes. La fraude commise au profit de l'organisation est habituellement exécutée en exploitant une opportunité d'acquérir un avantage, déloyal ou malhonnête, en trompant un tiers extérieur. Toutefois, même lorsque les collaborateurs invoquent une telle rationalisation, ils en tirent généralement un bénéfice personnel comme le fait d'atteindre un objectif de performance, une récompense financière, et/ou une promotion. L'Annexe C répertorie des exemples d'actes frauduleux et la façon dont ils sont rationalisés.

Collecter les informations

Afin d'identifier les risques de fraude dans le domaine ou processus audité, les auditeurs internes devraient appréhender l'organisation et le contexte dans lequel elle évolue (par exemple : le contexte juridique, politique, social, économique, le marché, le secteur d'activité et les environnements culturels). En outre, les auditeurs internes doivent comprendre les objectifs stratégiques et opérationnels de l'organisation et leur alignement avec les objectifs du domaine ou processus audité (Norme 2200 – Planification de la mission).

Afin d'atteindre ce niveau de compréhension, les auditeurs internes doivent collecter des informations à partir de sources diverses telles que :

- les évaluations et investigations précédentes ;
- les dispositifs d'alerte formels et les entretiens ;
- l'analyse préliminaire de l'environnement de contrôle ;
- le recours à des études externes et à des experts.

Lors de la collecte d'informations visant à réaliser l'évaluation des risques de fraude de la mission, l'audit interne est tenu d'évaluer les risques de fraude pertinents pour la mission plutôt que d'enquêter sur une fraude potentielle. Ainsi, les auditeurs internes devraient communiquer de manière discrète, maintenir la confidentialité et éviter d'exprimer le moindre soupçon ou accusation de fraude. Une communication négligente pourrait perturber une enquête éventuelle et faire naître inutilement des risques juridiques et de réputation non désirés.

Évaluations et investigations précédentes

L'évaluation des risques à l'échelle de l'organisation, documentant les risques significatifs identifiés et constituant la base pour le plan annuel d'audit interne (Norme 2010.A1), est un bon point de départ pour l'identification des risques qui pourraient être pertinents pour le domaine ou processus audité. Les évaluations dédiées uniquement aux risques de fraude, que ce soit au niveau de l'organisation ou du seul domaine ou processus audité, peuvent constituer une source d'informations utiles. Les auditeurs internes devraient prendre connaissance des évaluations des risques et des investigations sur les fraudes pertinentes effectuées par le management du domaine audité et par d'autres prestataires de services d'assurance et de conseil, tant internes qu'externes. Pour être efficaces, les auditeurs internes ne prennent généralement en compte que les évaluations récentes.

Bien que les investigations et les évaluations précédentes puissent fournir de précieuses indications, le caractère significatif des risques de fraude peut être affecté par de nombreux facteurs et peut changer rapidement. Ainsi, la réalisation d'une évaluation préliminaire des risques pour chaque mission est essentielle à la planification efficace de la mission.

Dispositifs d'alerte formels et entretiens

Le personnel de l'organisation peut fournir des informations utiles sur les risques de fraude. En effet, l'*Association of Certified Fraud Examiners* (ACFE) rapporte que, quels que soient la taille ou le type d'organisation, et indépendamment de l'existence d'un dispositif d'alerte formel, le personnel est à l'origine de plus de 50 % des informations ayant permis de détecter une fraude. Il s'agit du moyen de détection le plus fréquent[2] suivi de la fonction d'audit interne.

De nombreuses organisations ont mis en place des dispositifs formels (par exemple : des *hotlines* d'alerte, formulaires en ligne ou courriels) afin de faciliter le signalement d'actes suspectés comme étant frauduleux et des faiblesses de contrôle interne qui pourraient exposer l'organisation à des risques de fraude. Les signalements fréquemment rapportés concernent des allégations de dépenses injustifiées, d'abus de pouvoir, de détournement d'actifs, de collusion et d'autres comportements contraires à l'éthique ou douteux. Si un dispositif d'alerte formel existe, les auditeurs internes peuvent demander à la ou aux personne(s) responsable(s) de la gestion de ces dispositifs l'accès à toute information pertinente concernant le domaine ou processus audité, comme les appels téléphoniques ou les déclarations documentées.

Pour avoir un aperçu des activités frauduleuses passées ayant été présumées, découvertes, et/ou sujettes à investigation, les auditeurs internes interrogent généralement d'autres personnes de l'organisation en charge de la gestion des risques, des allégations et des survenances de fraude. Parmi elles, le département juridique, les ressources humaines, le responsable de la déontologie, le responsable des risques et de la conformité, le responsable de la sécurité et le responsable de la gestion des risques de fraude.

En outre, des entretiens avec le personnel à tous les niveaux du domaine ou processus audité permettent d'obtenir de précieuses informations, non disponibles par ailleurs. Les personnes exécutant les tâches

Expressions indiquant un signal d'alerte potentiel

Certaines expressions utilisées par les personnes interrogées peuvent indiquer d'éventuelles lacunes en matière de contrôle et/ou des risques de fraude :

- « Comme moyen de contournement... »
- « Juste pour cette fois... »
- « J'ai toujours fait ça comme ça... »
- « De temps à autre, nous... »
- « Officieusement... »
- « Il n'existe aucune règle ou procédure pour ce processus »
- « Quelqu'un m'a dit de faire comme ça, pour autant je ne suis pas sûr de savoir pourquoi »
- « Voilà la façon dont cela se passe réellement »
- « La manière dont c'est censé fonctionner... »

L'Annexe D dresse la liste des termes servant de signaux d'alerte potentiels.

2 Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2016), 20-25, http://www.acfe.com/rttn2016.aspx (consulté le 31 octobre 2017).

et fonctions quotidiennes du domaine ou processus audité fournissent souvent la description la plus précise et actualisée du fonctionnement réel du processus et des contrôles pertinents, par rapport à la façon dont ils devraient fonctionner. Comprendre le fonctionnement réel des activités permet de distinguer les diverses manières de contourner les contrôles. Pour identifier les personnes à interroger, les auditeurs internes peuvent se référer à un organigramme reprenant les rôles et responsabilités des collaborateurs associés au domaine ou processus audité, ou à une cartographie du processus dotée d'une liste des contrôles clés (qu'ils soient fournis par le management ou créés par l'audit interne).

Analyse préliminaire de l'environnement de contrôle

Les dispositifs d'alerte formels et les entretiens peuvent souvent mettre en évidence des problématiques liées à l'environnement de contrôle de l'organisation pouvant déboucher sur une fraude. Des signaux d'alerte supplémentaires peuvent être découverts grâce à un examen des éléments de l'environnement de contrôle, tels que la structure de l'organisation et les valeurs éthiques, ainsi que la philosophie du management et le style de management. Une évaluation de l'environnement de contrôle doit inclure l'évaluation de la maturité de l'environnement de contrôle et l'efficacité des contrôles pertinents. L'évaluation peut révéler d'éventuels comportements et/ou pressions pouvant conduire les collaborateurs à rationaliser les fraudes commises. Par exemple, les collaborateurs peuvent évoquer l'existence de pressions sur la performance ou des inquiétudes concernant des objectifs irréalistes qui pourraient pousser des individus à justifier un comportement frauduleux. Afin de mieux comprendre les pressions potentielles, les auditeurs internes doivent identifier les objectifs et les indicateurs clés de performance (ex : *Key Performance Indicators*), ainsi que les incitations associées au domaine audité.

Signaux d'alerte potentiels

Liés au management :

- Manque d'expertise du domaine
- Manque de supervision
- Historique d'infractions

Liés au personnel :

- Manque de vérification des antécédents
- Collaborateurs mécontents
- Réticence à partager les tâches

Liés au processus :

- Pas de séparation des fonctions
- Sécurité physique médiocre
- Contrôles d'accès médiocres

Dans la mesure où les auditeurs internes bénéficient d'une vision holistique de l'organisation et de son environnement de contrôle, ils peuvent déceler, au fil du temps, des changements culturels au sein de l'organisation. Ces changements pourraient accroître la probabilité d'occurrence des fraudes tout en passant inaperçus. Au niveau de la mission, les auditeurs internes peuvent être plus proches des opérations, des systèmes et des collaborateurs du domaine ou processus audité que de la direction générale (et d'autres responsables du management des risques de fraude au niveau de l'organisation). Ainsi, il est essentiel pour les auditeurs internes d'être attentifs aux discours ou aux actions des collaborateurs qui pourraient indiquer des faiblesses au niveau de l'environnement de contrôle. Si des faiblesses au niveau

de l'environnement de contrôle sont suspectées, le superviseur de la mission devrait communiquer ces informations au responsable de l'audit interne, dans la mesure où l'enjeu pourrait aller au-delà du périmètre d'intervention de la mission. Le Guide pratique de l'IIA « Audit de l'environnement de contrôle » couvre ce sujet plus en détail.

Recours à des études externes et à des experts

Les auditeurs internes ne sont pas tenus de posséder l'expertise d'une personne spécialisée dans l'investigation de la fraude. Toutefois, ils doivent avoir des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation (Norme 1210.A2). Les auditeurs internes peuvent acquérir ces connaissances en effectuant des recherches sur les fraudes qui ont eu lieu dans des organisations ou secteurs similaires et en étudiant les tendances en matière de fraude. En outre, les auditeurs internes peuvent utiliser des références pour comparer les pratiques de management des risques de fraude de l'organisation et du domaine audité avec celles d'organisations comparables et/ou plus matures. Les connaissances peuvent également être acquises en lisant les publications pertinentes, en se tenant au courant des changements réglementaires et en participant à des conférences et formations. Les organisations professionnelles appropriées fournissent souvent ce type d'outils et d'informations, ainsi que des normes professionnelles.

Le responsable de l'audit interne doit s'assurer que la fonction d'audit interne possède ou acquiert collectivement les compétences nécessaires à l'exercice de ses responsabilités (Norme 1210 – Compétence) ainsi que l'avis et l'assistance de personnes qualifiées si les auditeurs internes ne disposent pas les compétences nécessaires pour s'acquitter de tout ou partie de leur mission (Norme 1210.A1). En plus d'offrir des opportunités de formation et de tutorat aux auditeurs internes, le responsable de l'audit interne peut faire appel à des experts du secteur ou du domaine ou processus fonctionnel concerné. Lorsqu'ils organisent des *brainstorming* sur les scénarios de fraude ou réalisent une mission qui comprend des risques de fraude, les auditeurs internes peuvent faire appel à ces experts, le cas échéant.

Organiser des *brainstorming* sur les scénarios de fraude

Sur la base des informations collectées, les auditeurs internes peuvent commencer à envisager des scénarios et des risques de fraude potentiels pertinents pour le domaine ou le processus audité. Organiser des *brainstorming* sur les scénarios de fraude est un moyen efficace de déterminer les caractéristiques et les circonstances propres au domaine ou processus audité pouvant créer des opportunités et des incitations à la fraude.

Le nombre de séances de *brainstorming*, leur complexité ainsi que les participants peuvent varier d'une mission à l'autre, selon les besoins de la fonction d'audit interne, de l'organisation et de la mission, ainsi que selon les connaissances des auditeurs internes du domaine ou processus audité. Pour obtenir

une liste exhaustive des scénarios de fraude, les auditeurs internes doivent échanger pendant ces séances avec des personnes dont les connaissances, les perspectives et les relations avec le domaine ou processus audité divergent des leurs.

Lors de ces séances, les participants devraient envisager les pressions et les opportunités potentielles de commettre une fraude dans le domaine ou le processus audité. Les participants devraient également considérer les scénarios de fraude impliquant des menaces informatiques internes et externes, tels que le contournement d'accès aux configurations du système permettant des transactions frauduleuses et/ou le vol d'informations sensibles sur l'organisation.

Participants potentiels au *brainstorming*

- Comptabilité et finance
- Audit interne
- Juridique et conformité
- Opérations
- Responsables de processus
- Direction générale
- Autres prestataires de services d'assurance

Les séances de *brainstorming* sont destinées à encourager la participation transparente et le partage de points de vue et d'idées sans aucune censure. Par conséquent, lorsqu'ils revoient les scénarios de fraude proposés, les auditeurs internes devraient tenir compte du fait que certains risques de fraude potentiels sont très peu probables, ne sont pas alignés avec les objectifs de la mission, ou vont au-delà du périmètre d'intervention et de l'allocation des ressources de la mission actuelle.

L'information recueillie au cours de séances de *brainstorming* pourrait servir à dresser une liste des scénarios des risques de fraude pour n'importe quel domaine ou processus pouvant être audité. En ce sens, le **Tableau 1** présente les scénarios de fraude et les risques correspondants qui pourraient être identifiés lors d'une séance de *brainstorming* dans le cadre d'une mission d'assurance relative aux comptes fournisseurs. L'Annexe E présente une évaluation des risques de fraude dans le cadre d'une mission relative au processus de décaissements.

Tableau 1 : Organiser des *brainstorming* sur les scénarios de fraude

Scénario de fraude	Risque de fraude
A. Notes de frais fictives.	A.1 Le processus d'émission des cartes de crédit professionnelles pour le règlement des notes de frais est volontairement inapproprié ce qui entraîne des dépenses frauduleuses.
	A.2 Des dépenses sont présentées pour des biens et services qui n'ont pas réellement été fournis ou réalisés.
	A.3 Plusieurs remboursements de frais sont effectués pour la même dépense.
B. Décaissements frauduleux.	B.1 Des vendeurs fictifs sont créés dans le système, ce qui amène à des dépenses frauduleuses.
	B.2 De faux remboursements et/ou des remboursements annulés sont traités.
C. Obligations et charges dissimulées.	C.1 Une créance douteuse est intentionnellement omise.
	C.2 Des dépenses sont immobilisées.
D. Transactions entre parties liées.	D.1 Une des parties reçoit un avantage qu'elle n'obtiendrait pas dans une transaction réalisée dans des conditions de concurrence normales.
E. Malversation.	E.1 Des collaborateurs effectuent des dépenses personnelles grâce à des fonds de l'organisation et falsifient les états financiers pour les dissimuler.

Évaluation des risques de fraude

Dans la mesure où la mission ne peut pas couvrir tous les risques, les auditeurs internes évaluent le caractère significatif des risques de fraude identifiés au cours du *brainstorming* afin de déterminer quels risques devraient être évalués plus en détail pendant la mission. Un moyen efficace pour élaborer et documenter l'évaluation des risques de fraude est de créer une matrice des risques de fraude énumérant les scénarios de fraude et les risques associés, puis de l'élargir pour y inclure des indicateurs du caractère significatif des risques.

Une matrice des risques de fraude peut être créée à l'aide d'une feuille de calcul ou d'un document du même type, avec ou sans un logiciel d'audit. Le format de la matrice peut varier, mais il comprend généralement une ligne pour chaque risque et une colonne pour chaque indicateur de risque, comme l'impact et la probabilité.

Le **Tableau 2** montre comment les scénarios de fraude documentés dans le Tableau 1 peuvent être élargis pour y inclure les cotations de l'impact et de la probabilité des risques.

L'évaluation de l'impact peut être compliquée car elle implique des facteurs aussi bien quantitatifs que qualitatifs. Les auditeurs internes devraient prendre en compte non seulement l'impact financier, opérationnel et réglementaire des risques potentiels de fraude, mais également les impacts non financiers, comme l'atteinte à la réputation de l'organisation ou aux relations avec les clients et fournisseurs. Par exemple, un risque de fraude

Tableau 2 : Matrice des risques de fraude des comptes fournisseurs

Scénario de fraude	Risque de fraude	Impact (F, M, E)	Probabilité (F, M, E)
A. Notes de frais fictives.	A.1 Le processus d'émission des cartes de crédit professionnelles pour le règlement des notes de frais est volontairement inapproprié ce qui entraîne des dépenses frauduleuses.	F	M
	A.2 Des dépenses sont présentées pour des biens et services qui n'ont pas réellement été fournis ou réalisés.	E	M
	A.3 Plusieurs remboursements de frais sont effectués pour la même dépense.	M	E
B. Décaissements frauduleux.	B.1 Des vendeurs fictifs sont créés dans le système, ce qui amène à des dépenses frauduleuses.	E	E
	B.2 De faux remboursements et/ou des remboursements annulés sont traités.	F	E
C. Obligations et charges dissimulées.	C.1 Une créance douteuse est intentionnellement omise.	E	F
	C.2 Des dépenses sont immobilisées.	E	F
D. Transactions entre parties liées.	D.1 Une des parties reçoit un avantage qu'elle n'obtiendrait pas dans une transaction réalisée dans des conditions de concurrence normales.	M	M
E. Malversation.	E.1 Des collaborateurs effectuent des dépenses personnelles grâce à des fonds de l'organisation et falsifient les états financiers pour les dissimuler.	M	M

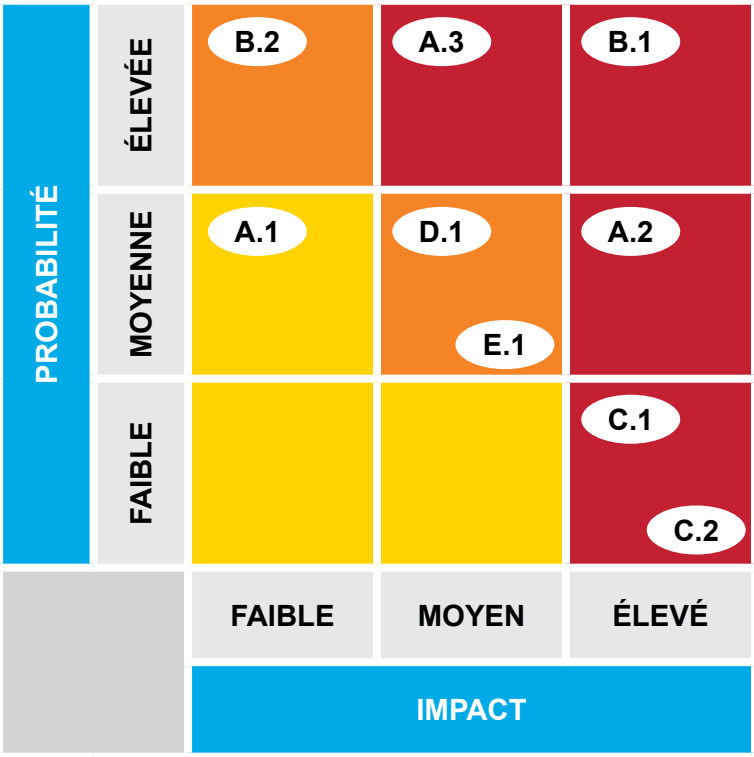
ayant un impact financier direct et négligeable pour l'organisation pourrait tout de même nuire considérablement à sa réputation et entrer dans la catégorie « impact élevé ».

Les facteurs à considérer lors de l'évaluation de la probabilité incluent les allégations ou les occurrences passées de fraudes, l'existence de fraudes similaires dans le secteur d'activité, la complexité ainsi que le nombre de personnes impliquées dans le processus.

La cotation des risques de la matrice des risques de fraude peut être ensuite représentée sur un graphique basique, comme une carte des points critiques. En traçant l'impact de chaque risque le long d'un axe et sa probabilité sur l'autre axe, les auditeurs internes représentent de manière claire le caractère significatif global du risque ou sa priorité. De manière générale, le caractère significatif combiné de l'impact et de la probabilité est indiqué au moyen d'un système de couleurs : le rouge indique les priorités absolues, le orange renvoie à des risques suffisamment importants pour être considérés et le jaune évoque des risques qui ne représentent pas de menace significative.

Le **Tableau 3** représente une carte des points critiques créée à partir de l'information contenue dans la matrice des risques de fraude présentée dans le Tableau 2. La carte des points critiques devrait figurer dans les documents de travail de la mission parce qu'elle justifie les décisions des auditeurs internes quant au caractère significatif du risque.

Tableau 3 : Carte des points critiques



Une des limites de cette carte est que l'impact et la probabilité revêtent la même importance. Ceci peut être vrai parfois, mais l'impact est généralement plus important que la probabilité. Par exemple, dans la plupart des cas, un risque dont l'impact est élevé et la probabilité faible (E, F) devrait passer avant un risque dont l'impact est faible et la probabilité élevée (F, E).

Une autre limite de la carte des points critiques est qu'elle ne montre que deux variables à la fois (dans le cas présent, l'impact et la probabilité). Il peut être souhaitable ou nécessaire d'envisager également des variables telles que la rapidité, la vulnérabilité, la volatilité, l'interdépendance, et/ou la corrélation lors que l'on détermine le caractère significatif d'un risque.

En s'appuyant sur une carte des points critiques complète, les auditeurs internes peuvent aisément visualiser les risques de fraude significatifs à intégrer à la mission pour des tests plus poussés. Le **Tableau 4** illustre la matrice des risques de fraude ajustée pour refléter uniquement les risques de fraude priorisés dans l'exemple de la mission relative aux comptes fournisseurs.

Tableau 4 : Risques de fraude significatifs

Risque de fraude	Impact (F, M, E)	Probabilité (F, M, E)
B.1 Des vendeurs fictifs sont créés dans le système, ce qui amène à des dépenses frauduleuses.	E	E
A.2 Des dépenses sont présentées pour des biens et services qui n'ont pas réellement été fournis ou réalisés.	E	M
A.3 Plusieurs remboursements de frais sont effectués pour la même dépense.	M	E
C.1 Une créance douteuse est intentionnellement omise.	E	F
C.2 Des dépenses sont immobilisées.	E	F
D.1 Une des parties reçoit un avantage qu'elle n'obtiendrait pas dans une transaction réalisée dans des conditions de concurrence normales.	M	M
E.1 Des collaborateurs effectuent des dépenses personnelles grâce à des fonds de l'organisation et falsifient les états financiers pour les dissimuler.	M	M

Les auditeurs internes peuvent communiquer au management les risques de fraude identifiés pour qu'il envisage de les inclure dans l'évaluation des risques au niveau de l'organisation. Les risques de fraude qui ne sont pas sélectionnés pour une évaluation approfondie dans le cadre de cette mission, peuvent être transférés à l'inventaire des risques de fraude de l'audit interne, ou à la liste des sujets à surveiller pour de futures missions.

Si les informations découvertes lors de l'évaluation des risques de fraude révèlent un acte potentiellement frauduleux, les auditeurs internes devraient suivre les protocoles internes pour alerter sur les cas de fraude et déclencher les investigations. En général, les auditeurs internes rapportent les éventuels dysfonctionnements et la preuve préliminaire au responsable de l'audit interne, qui décide ensuite si la question doit être remontée à la direction générale et/ou au Conseil.

Identifier les contrôles

Après que les auditeurs internes ont examiné les scénarios de fraude, identifié et priorisé les risques de fraude, ils devraient déterminer quels contrôles sont mis en place pour atténuer ces risques.

Le **Tableau 5** illustre l'extension de la matrice du Tableau 4 pour inclure les contrôles existants.

Tout comme la carte des points critiques, la matrice des risques et des contrôles de fraude devrait figurer dans les documents de travail de la mission. Les informations issues de la matrice sont ensuite intégrées

à l'évaluation préliminaire des risques, utilisée pour établir les objectifs et le périmètre d'intervention de la mission. Le Guide pratique de l'IIA « Planification de la mission : Définir les objectifs et le périmètre d'intervention » donne des informations détaillées sur la façon de définir les objectifs et le périmètre d'intervention de la mission à partir de l'évaluation des risques. En outre, la carte des points critiques des risques et la matrice des risques et des contrôles pourront soutenir les résultats et les conclusions de la mission, conformément à la Norme 2330 – Documentation des informations.

Tableau 5 : Matrice des risques et des contrôles de fraude des comptes fournisseurs

Risque de fraude	Impact (F, M, E)	Probabilité (F, M, E)	Contrôle
B.1 Des vendeurs fictifs sont créés dans le système, ce qui amène à des dépenses frauduleuses.	E	E	Séparation des tâches dans la gestion des fournisseurs.
A.2 Des dépenses sont présentées pour des biens et services qui n'ont pas réellement été fournis ou réalisés.	E	M	Confirmation de la réception des biens et services.
A.3 Plusieurs remboursements de frais sont effectués pour la même dépense.	M	E	Contrôles automatisés visant à détecter les présentations de frais en double.
C.1 Une créance douteuse est intentionnellement omise.	E	F	Surveillance régulière et approbation des calculs des créances irrécouvrables.
C.2 Des dépenses sont immobilisées.	E	F	Révision et approbation de toutes les entrées de capitalisation par le management.
D.1 Une des parties reçoit un avantage qu'elle n'obtiendrait pas dans une transaction réalisée dans des conditions de concurrence normales.	M	M	Une évaluation *(due diligence)* des transactions entre parties liées.
E.1 Des collaborateurs effectuent des dépenses personnelles grâce à des fonds de l'organisation et falsifient les états financiers pour les dissimuler.	M	M	Séparation des tâches dans les comptes créditeurs et approbation du management requise pour les dépenses personnelles.

Annexe A. Normes et lignes directrices de l'IIA

Normes associées de l'IIA

Les *Normes internationales pour la pratique professionnelle de l'audit interne* pertinentes dans le cadre de ce guide pratique sont listées ci-dessous. Afin de contribuer à leur mise en œuvre, l'IIA conseille aux auditeurs internes de se référer au guide de mise en œuvre de chaque Norme.

1210 – Compétence

1210.A1

1210.A2

1220 – Conscience professionnelle

1220.A1

2120 – Management des risques

2120.A2

2200 – Planification de la mission

2210 – Objectifs de la mission

2210.A1

2210.A2

Principales Lignes directrices de l'IIA concernées

Guide pratique, « Auditer l'environnement de contrôle »

Guide pratique, « Planification de la mission : définir les objectifs et le périmètre d'intervention »

Guide pratique, « L'audit interne et la fraude »

Annexe B. Glossaire

Les termes marqués d'un astérisque (*) sont issus du glossaire du *Cadre de référence internationale des pratiques professionnelles* de l'IIA, édition 2017.

Contrôle* – Toute mesure prise par le management, le Conseil et d'autres parties afin de gérer les risques et d'accroître la probabilité que les buts et objectifs fixés seront atteints. Le management planifie, organise et dirige la mise en œuvre de mesures nécessaires pour donner une assurance raisonnable que les buts et objectifs seront atteints.

Environnement de contrôle* – L'attitude et les actions du Conseil et du management au regard de l'importance du dispositif de contrôle dans l'organisation. L'environnement de contrôle constitue le cadre et la structure nécessaires à la réalisation des objectifs primordiaux du système de contrôle interne. L'environnement de contrôle englobe les éléments suivants :

- intégrité et valeurs éthiques ;
- philosophie et style de direction ;
- structure organisationnelle ;
- attribution des pouvoirs et responsabilités ;
- politiques et pratiques relatives aux ressources humaines ;
- compétence des collaborateurs.

Fraude* – 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 lié à leur activité.

Risque* – Possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.

Annexe C. Exemples d'actes frauduleux

Les exemples suivants d'actes frauduleux ne constituent en aucun cas une liste exhaustive ou priorisée. Au lieu de cela, ils sont fournis pour stimuler la prise de conscience des risques de fraude classés par type de rationalisation.

Exemples de fraude au bénéfice direct d'une personne :

- Détournement intentionnel de fonds normalement destinés à générer des profits pour l'organisation, au bénéfice d'un collaborateur, d'une partie prenante ou d'un tiers.
- Malversation (ex : détournement de fonds ou de biens, et falsification des états financiers pour dissimuler l'acte).
- Espionnage, y compris concernant la recherche et le développement.
- Dissimulation intentionnelle ou falsification relative à des événements, des transactions ou des données.
- Réclamations soumises pour des services ou biens qui n'ont pas réellement été fournis à l'organisation.
- Action intentionnellement omise alors qu'une intervention est requise selon les instructions internes ou réglementaires.
- Utilisation non autorisée ou illégale d'informations confidentielles ou exclusives.
- Manipulation non autorisée ou illégale de réseaux ou systèmes d'exploitation informatiques.
- Vol.
- Acceptation de pots-de-vin ou de dessous-de-table.

Exemples de fraude au bénéfice direct de l'organisation :

- Déclaration frauduleuse concernant les données financières ou extra-financières, comprenant l'évaluation des transactions, des actifs, des passifs, des revenus ou des données statistiques (plus particulièrement en cas de fusions et acquisitions).
- Manipulation des prix de transfert (c.-à-d., la valeur des marchandises échangées entre des organisations apparentées) afin de permettre au management d'améliorer les résultats au détriment d'organisations concurrentes.
- Transaction avec les parties liées dans laquelle une des parties reçoit un bénéfice qu'elle n'obtiendrait pas dans des conditions de concurrence normales.
- Absence d'enregistrement ou de divulgation précis et exhaustif d'informations importantes, pouvant améliorer, de manière fictive, la présentation de l'organisation vis-à-vis de tiers.
- Vente ou cession d'actifs fictifs ou dissimulés.
- Action intentionnellement omise alors que celle-ci est requise selon les instructions internes ou réglementaires.

- Inexactitude significative dans la présentation d'activités financières ou relatives à la conformité, dans le but d'améliorer le cours des actions, d'obtenir un avantage concurrentiel ou de réduire les impôts ou les amendes dus.
- Activités qui enfreignent les lois, les règlements ou qui violent les contrats conclus avec le gouvernement.
- Contributions politiques illégales, pots-de-vin fournis à des clients ou fournisseurs ou avantages payés à des fonctionnaires ou à leurs intermédiaires.

Annexe D. Termes à considérer comme des signaux d'alerte potentiels

Le tableau suivant fournit des exemples de mots choisis par les personnes interrogées pouvant éveiller le scepticisme professionnel d'un auditeur interne dans certaines circonstances ou contextes, justifiant ainsi des questions supplémentaires.

Termes à considérer comme des signaux d'alerte potentiels		
Adapté	Devancer	Parfois
Agressif	Difficile	Pas sûr
Approche différente	Dissimuler/Dissimulation	Peut-être
Assumer	Evolutif	Préoccupation
Atténuer	Fragmenté	Problématique
Atypique	Incertain	Réallouer
Complexe	Indépendant	Reconsidérer
Conjoncturel	Interprétation	Réserves
Contourner	Marginal	Risqué
Contraint	Modifier	Subjectif
Déconnexion	Nouvelle approche	Temporaire
Délicat	Officieusement	Tisser
Dépend	Original	Transitoire

Annexe E. Étude de cas : Mission d'assurance relative aux décaissements

L'étude de cas suivante illustre comment les risques de fraude pourraient être identifiés et documentés lors de la planification d'une mission d'assurance d'un processus de décaissements. L'étude de cas ne couvre pas tous les risques de fraude d'un processus réel de décaissements et n'est pas destinée à être utilisée comme un modèle ou un programme d'évaluation des risques. Dans la mesure où les caractéristiques de chaque organisation sont différentes, les risques de fraude le sont également.

Collecter les informations

Lors de la planification de la mission d'assurance relative aux décaissements, les auditeurs internes ont rassemblé les informations suivantes :

- Il n'y a aucune trace d'évaluations internes ou externes ou d'investigations précédentes.
- Les collaborateurs qui ont la capacité de mettre à jour les informations relatives aux fournisseurs dans le fichier maître des fournisseurs ont également la possibilité de traiter les paiements dans le système.
- Plusieurs collaborateurs ont des droits d'accès super-utilisateur aux fonctions des comptes fournisseurs : gestion du fichier maître des fournisseurs, facturation, contournement de la validation des factures et mise à jour des informations de paiement.
- Le mécanisme d'approbation est appliqué de manière incohérente et fréquemment contourné dans le système.
- Les révisions et approbations des décaissements sont effectuées de manière incohérente.
- Le chiffre d'affaires a considérablement diminué depuis l'année précédente, tandis que les charges d'exploitation ont augmenté de façon inattendue pendant la même période.
- Les primes sont octroyées uniquement si les objectifs financiers sont atteints.
- Les entretiens avec le personnel des ressources humaines ont montré que le superviseur des comptes fournisseurs a été accusé d'être de connivence avec les collaborateurs qui lui sont rattachés.
- Le superviseur se montre assez amical et confiant envers le personnel du service des comptes fournisseurs.

Organiser des *brainstorming* sur les scénarios de fraude

Les auditeurs internes ont documenté les informations suivantes dans le cadre des *brainstorming* sur les scénarios de fraude.

Facteurs de fraude	Contrôle
Pression	Des primes significatives sont octroyées si les objectifs financiers sont atteints.
	Certains collaborateurs s'inquiètent de l'avancement professionnel limité et/ou craignent de perdre leur emploi.
	Les primes peuvent ne pas être payées cette année.
	Un collaborateur a récemment été se vanter de son train de vie somptueux auprès de ses collègues.
Opportunité	Les fonctions ne sont pas correctement séparées.
	Les relations entre les collaborateurs et le management peuvent être inappropriées. Un collaborateur entretient une relation particulièrement étroite avec son manager.
	Plusieurs collaborateurs partagent un accès administrateur. Or, les données de traitement des paiements et les informations bancaires peuvent être modifiées par les collaborateurs disposant d'un tel accès.
	Le ficher maître des fournisseurs peut être mis à jour par tous les collaborateurs et le système ne garde pas l'historique des modifications.
Rationalisation	Des collaborateurs peuvent percevoir du favoritisme et se sentir négligés ou éprouver du ressentiment.
	Des collaborateurs peuvent percevoir que le management affiche une exemplarité négative au plus haut niveau.
	Un comportement inapproprié semble être monnaie courante.

Évaluation des risques de fraude et identification des contrôles

Les auditeurs internes ont créé la matrice suivante des risques et des contrôles des fraudes à inclure dans le plan de la mission.

Scénario de fraude	Risque de fraude	Impact (F, M, E)	Probabilité (F, M, E)	Contrôle
A. Fournisseurs non approuvés	A.1 Des vendeurs fictifs sont créés dans le système, ce qui peut entraîner des paiements frauduleux.	E	E	• Séparation des tâches. • Revue périodique du fichier maître des fournisseurs.
	A.2 Les adresses des fournisseurs sont remplacées par des adresses de collaborateurs ; ou les informations de paiement sont remplacées par des comptes bancaires de collaborateurs.	M	M	• L'approbation du management est requise pour les mises à jour des adresses des fournisseurs et des données de transfert électroniques de fonds.
B. Paiements inappropriés	B.1 Des remboursements fictifs sont traités pour paiement.	M	M	• L'approbation du management est requise pour les paiements.
	B.2 Des approbations de factures fictives ou dupliquées sont contournées dans le système.	E	E	• L'approbation du management est requise avant que le paiement soit effectué.
C. Collusion	C.1 Le superviseur est de mèche avec un collaborateur pour contourner les contrôles existants.	E	M	• Aucun.

Incorporer les résultats au plan de la mission

Après avoir créé la matrice des risques et des contrôles des fraudes, les auditeurs internes ont intégré l'évaluation des risques de fraude et les résultats préliminaires dans le plan de mission d'assurance relative aux décaissements, ainsi que les remarques suivantes :

- Examiner le fichier maître des fournisseurs avec les noms et adresses afin de vérifier si des fournisseurs apparaissent plusieurs fois.
- Revoir les noms similaires des fournisseurs mais dont les adresses et/ou informations de paiement diffèrent.
- Vérifier les adresses et les coordonnées bancaires des fournisseurs pour voir si elles correspondent à celles d'un collaborateur.
- Rechercher les adresses de fournisseurs qui semblent être des adresses de particuliers ou des boîtes postales.
- Examiner l'historique des factures et les montants de paiement correspondants afin de rechercher des numéros de facture en double ou des montants de paiement répétés.
- Parcourir le processus de paiement et rechercher des problématiques liées à la séparation des tâches en lien avec les niveaux de délégation.

Remerciements

Équipe de projet

Glenn Ho, CIA, CRMA, Afrique du Sud (Chairman)
Doug Hileman, CRMA, CPEA, États-Unis (Project Lead)
Caroline Glynn, CIA, États-Unis
John Mickevice, CIA, CRMA, États-Unis
Daniel Samson, CIA, Etats-Unis

Contributeurs

Awad Elkarim Mohamed Ahmed, CIA, CCSA, ACPA, CGAP, CRMA, Émirats Arabes Unis
Elastos Chimwanda, CIA, Zimbabwe
Dana Lawrence, CIA, ACPA, CRMA, États-Unis
Barry Smit, CIA, Afrique du Sud
Dr. Gokhan Sungun, CIA, CCSA, CRMA, États-Unis
Oliver Sznitkies, France

Collaborateurs de l'IIA Global en charge des Normes et des lignes directrices

Christine Hovious, CIA, CRMA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Lauressa Nelson, Technical Writer
Christina Brune, Technical Writer

Réviseurs de la traduction française

Marie-Elisabeth Albert, CIA
Bouchra Bajjou
Bruno Buresi, CISA
Christophe Butikofer, CIA
Julien Cornuché, CIA, CISA
Béatrice Ki-Zerbo, CIA
Sébastien Lepers, CIA

L'IIA aimerait remercier les organes de surveillance suivants pour leur soutien : Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'*Institute of Internal Auditors* (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA, dont le siège mondial se situe à Lake Mary (Floride, États-Unis), compte actuellement quelque 190 000 membres dans plus de 170 pays et territoires. Plus d'informations sont disponibles sur le site www.globaliia.org / www.theiia.org.

À propos des lignes directrices complémentaires

Les lignes directrices complémentaires font partie intégrante du Cadre de référence international des pratiques professionnelles (CRIPP) et proposent des recommandations supplémentaires (facultatives) pour la réalisation des activités d'audit interne. Si elles reflètent les *Normes*, ces lignes directrices complémentaires ne visent pas directement la mise en conformité auxdites *Normes*. Elles couvrent au contraire des domaines particuliers, ainsi que des questions sectorielles, et contiennent des procédures et processus détaillés. Ces lignes directrices ont été officiellement révisées et approuvées par l'IIA.

Guides pratiques

Les guides pratiques constituent un type particulier de lignes directrices complémentaires et détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Dans le cadre des dispositions du CRIPP, la conformité aux guides pratiques est recommandée (mais non obligatoire). Ces guides pratiques ont été officiellement révisés et approuvés par l'IIA.

Le Global Technologies Audit Guide (GTAG) est un type de guide pratique qui aborde, dans un langage courant, une question d'actualité liée à la gestion, au contrôle ou à la sécurité des technologies de l'information.

Pour de plus amples informations sur les documents de référence proposés par l'IIA, vous pouvez consulter notre site Web, www.globaliia.org/standards-guidance ou www.theiia.org/guidance ou www.ifaci.com.

Avertissement

L'*Institute of Internal Auditors* publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et est seulement destinée à servir de guide. L'*Institute of Internal Auditors* vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'IIA dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

Copyright

Le copyright de ce guide pratique est détenu par l'*Institute of Internal Auditors* et par l'IFACI pour sa version française.

Pour l'autorisation de reproduction, prière de contacter l'*Institute of Internal Auditors* à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com

Janvier 2018 - ISBN : 978-2-915042-85-6