

fmi  igf[®]

PD WEEK 2022

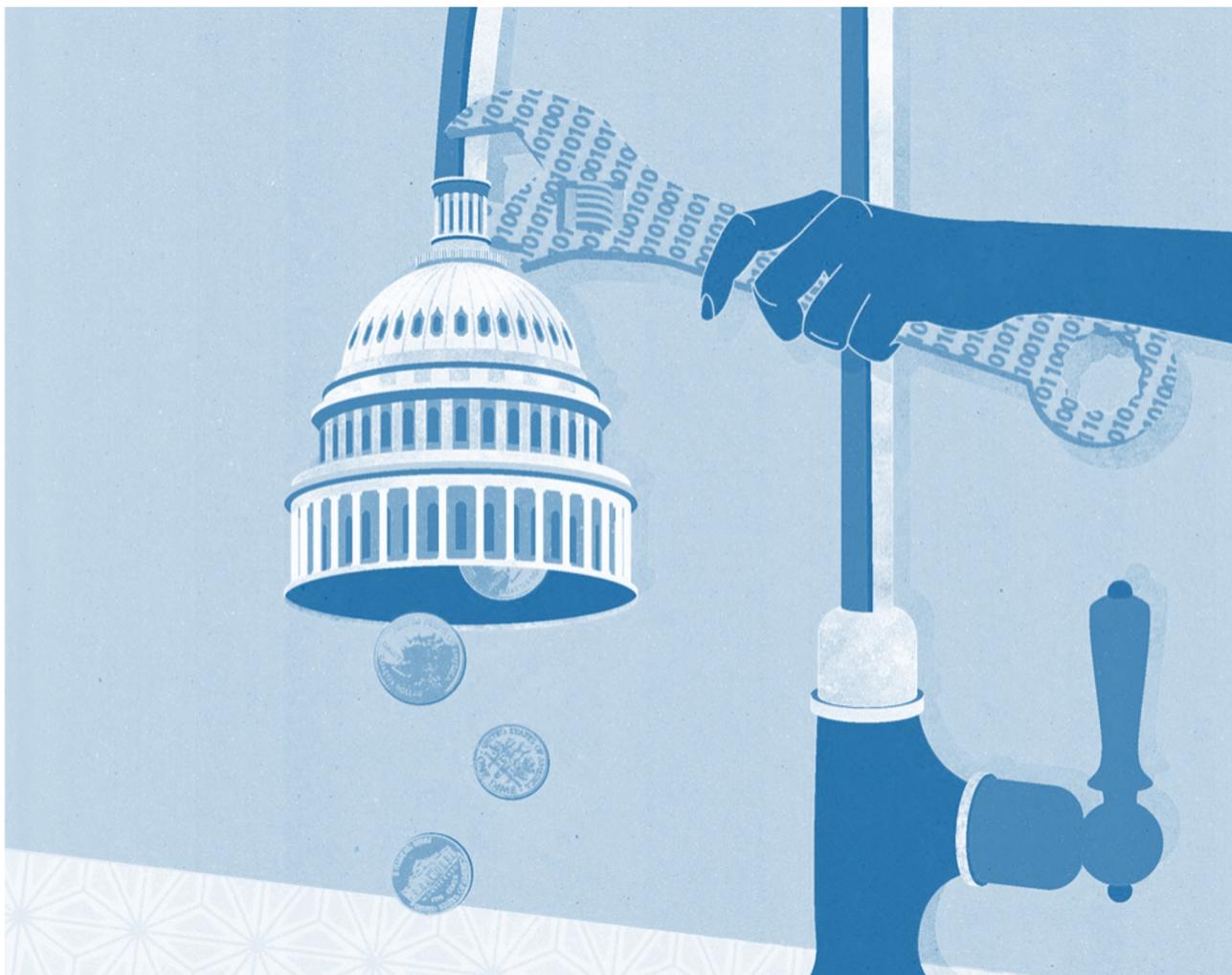
SEM AINE DE PP 2022

L'intégrité des programmes et la fraude

Nouveautés et moyens de prévention

Amanda Holden

Associée, Service de conseils en gestion des risques,
Deloitte



Qu'est-ce que l'intégrité des programmes ?

« L'intégrité à dessein vise à garantir que les avantages et les services sont fournis à la bonne personne, pour le bon usage, au bon moment et en bonne quantité. »

L'intégrité des programmes est essentielle.

Augmentation de la fraude, du gaspillage et des abus

Les organismes du secteur public au Canada ont l'opportunité de renforcer leurs évaluations des risques de fraude et leurs pratiques de prévention de la fraude.



55 % n'effectuent pas d'évaluations formelles des risques de fraude. Sur ces 55 %, seuls 35 % procèdent à d'autres examens internes ou évaluent les risques de fraude dans le cadre de la vérification de leurs états financiers de fin d'année.¹



57 % ne disposent pas de politiques et de procédures à suivre en cas de fraude potentielle. Sur les 43 % qui ont des politiques, 60 % n'indiquent pas quand et comment appeler la police.¹



Aux États-Unis, **163 milliards de dollars** de prestations indûment versées durant la pandémie ont été principalement attribués à la fraude, ce qui représente un taux de paiements irréguliers de plus de 18,71 %.²



Près de **50 %** des cas de fraude en milieu de travail sont dus à l'absence de contrôles internes ou au contournement des contrôles existants.³



Au Royaume-Uni, on estime à **33 milliards de livres sterling** le montant annuel des pertes dues à la fraude et à des erreurs dans le secteur public.⁴

La fraude à l'encontre du secteur public augmente le coût des services publics. Il est donc essentiel de comprendre, trouver et réduire cette fraude pour assurer l'efficacité du gouvernement.⁴

¹ Source : Unemployment Insurance

² Source : Association of Certified Fraud Examiners

³ Source : Public Sector Fraud Authority Mandate – September 2022, Government of United Kingdom

⁴ Source : Public Sector Fraud Authority Mandate – September 2022, Government of United Kingdom

Confiance des citoyens

Répercussions politiques, culture du pays, gardiens de l'argent des contribuables



Perte financière

Pertes d'argent, coûts des enquêtes, règlements à l'amiable, pertes de productivité



Impact sur les citoyens

Pertes de prestations, prestations trop lentes, répercussions sur le mode de vie, la santé et le revenu



Médias et réputation

Bonne volonté politique, première page des journaux, réputation des personnes et des partis



Enquêtes et services juridiques

Frais juridiques, retard dans les résultats, coûts indirects des enquêtes

Parfois, « FRAUDE » est un gros mot.



Gaspillage

- Le fait d'employer ou de dépenser des ressources de façon négligente, extravagante ou inutile.
- Le gaspillage et les abus n'impliquent pas nécessairement une fraude ou des actes illégaux.



Abus

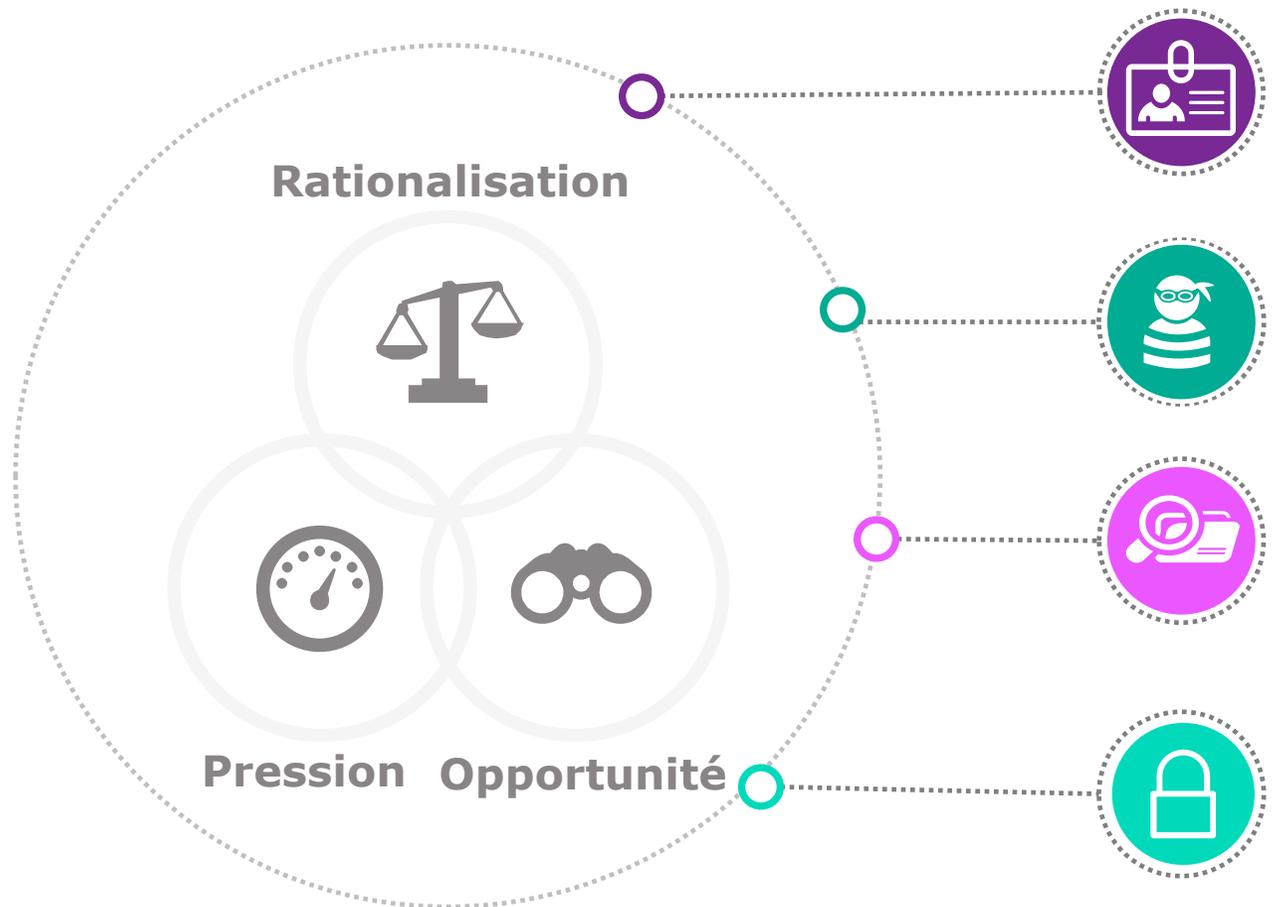
- Comportement déficient ou inapproprié qu'une personne prudente ne considérerait pas comme une pratique opérationnelle raisonnable et nécessaire, compte tenu des faits et des circonstances.
- Cela inclut l'abus d'autorité ou de pouvoir pour un gain personnel ou pour le bénéfice d'autrui.



Fraude

- Le fait d'obtenir quelque chose de valeur par une déclaration délibérément fausse.
- La question de savoir si un acte est effectivement une « fraude » est une décision qui doit être prise par le système judiciaire ou un autre système juridictionnel, et va au-delà de la responsabilité professionnelle de la direction en matière d'évaluation des risques.

Le « triangle de la fraude » représente les ingrédients de la fraude et se traduit par de nombreux types de fraude.



Fraude interne

Comprend un large éventail de risques où des employés ou des fournisseurs détournent des actifs ou des fonds par le biais de processus internes et de contrôles faibles. *L'argent qui circule au sein de l'organisation.*

Fraude externe

Des acteurs externes, notamment des citoyens malavisés, des criminels et le crime organisé, profitent de paiements sous forme de prestations, de subventions, de prêts, de remboursements/d'exonérations d'impôts, etc. *L'argent qui circule de l'intérieur à l'extérieur de l'organisation.*

Risques d'initiés

La pratique consistant à examiner les risques liés aux performances, aux activités, à l'accès aux données/systèmes et aux communications des employés (y compris l'analyse de sentiments, etc.) afin de prévenir les activités inappropriées qui pourraient entraîner une fraude, d'autres risques opérationnels ou une atteinte à la réputation et à l'intégrité des programmes.

Cybermenaces

Protéger la technologie de l'organisation contre les manipulations et les accès inappropriés. Une cyberattaque peut être une activité sous-jacente à la fraude ou faciliter la fraude interne ou externe.



Recherche

- Consulter les fraudes
- Protégez-vous
- Signaler une fraude
- Que faire si vous êtes victime

Le Centre antifraude du Canada recueille de l'information sur la fraude et le vol d'identité. Il fournit des renseignements sur les fraudes passées et courantes touchant les Canadiens. Si vous pensez avoir été victime d'une fraude, [signalez-le!](#)

Fraudes récentes



Répercussions de la fraude depuis le début de l'année

En date du 30 septembre 2022

Signalements de fraude :

68 259

(107 187 en 2021)

Victimes de fraude :

43 476

(68 069 en 2021)

En pertes financières liées aux fraudes :

362,7 M\$

(383 M\$ en 2021)

A catalogue of 2022's latest cons and scams

6.14.2022 | CPA CANADA

Crypto scams, real estate renter fraud, fake time share buyers, and more, in this roundup



The popular Netflix show Squid Game inspired a crypto token that saw more than US\$3 million snatched from investors (Alamy)

"I HAVE BEEN HACKED."

WHAT IS BUSINESS EMAIL COMPROMISE?



ILLEGAL ACCESS

Criminals gain entry to a victim's devices or systems – through hacking, phishing websites, malware – then deceive the victim into transferring money into their bank account.



SOCIAL ENGINEERING

Criminals can target their victims based on information they share on social media platforms.



URGENT REQUEST

The criminal impersonates a supplier requesting an urgent payment or change to banking details, or a senior employee in the company with authority to authorize payments.

#BECareful



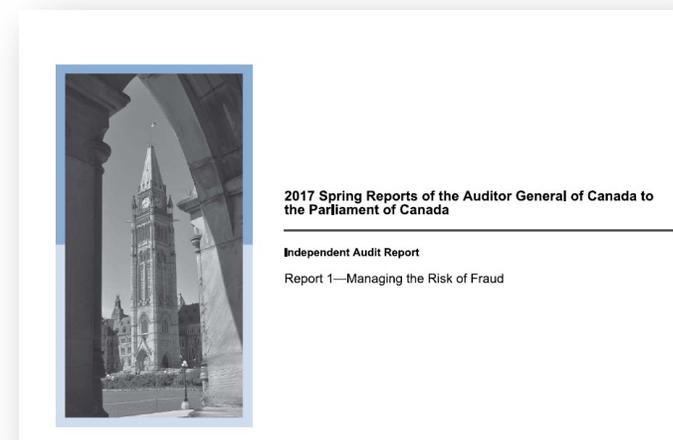
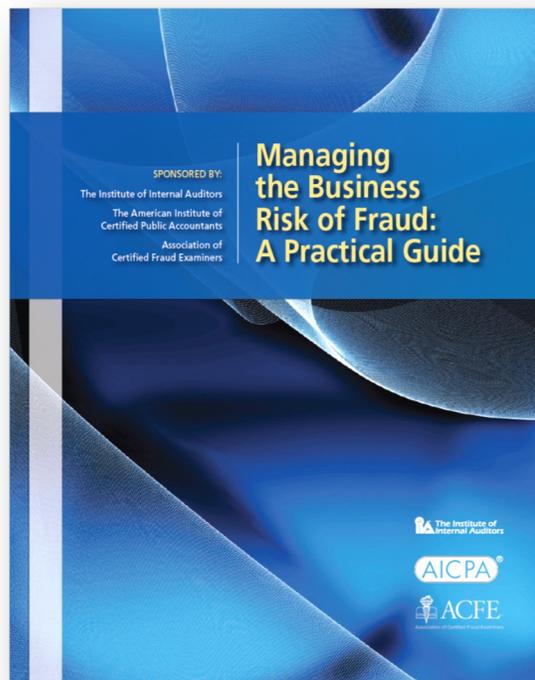
INTERPOL

Prenez des mesures

Que peut faire votre organisation ?

Cadre gouvernemental pour la gestion de la fraude

Document du secteur axé sur la vérification
(ACFE + IAI + AICPA)



Guide de gestion des risques de fraude au Bureau du vérificateur général du Canada

Programme de gestion des risques de fraude du BVG

Gouvernance

- Surveillance
- Politiques relatives à l'éthique des affaires
- Politiques et procédures relatives à la fraude
- Politiques/procédures relatives aux conflits d'intérêts

Évaluation des risques de fraude

- Politique/procédure d'évaluation des risques de fraude
- Évaluation des risques de fraude
- Réévaluation périodique
- Examen de la politique d'évaluation des risques de fraude

Contrôles de prévention et de détection de la fraude

- Activités de formation et de sensibilisation
- Contrôles internes de prévention et de détection de la fraude
- Gestion des conflits d'intérêts
- Détection de la fraude

Réponse aux allégations de fraude, de gaspillage ou d'abus

- Procédures et mécanismes de signalement
- Tri initial des allégations
- Enquêtes
- Établissement de rapports
- Mesures/solutions correctives

Source : https://www.oag-bvg.gc.ca/internet/Francais/acc_rpt_f_42986.html

5 éléments

Le **cadre de gestion des risques d'entreprise du COSO** comporte 5 éléments principaux.



Gouvernance



Évaluation des risques de fraude



Évaluation et mise en œuvre des contrôles de prévention



Détection, enquête et communication



Contrôle et test



17 principes

Ces éléments établissent 17 principes de gestion des risques adaptés à la gestion de la fraude, qui aident à clarifier la conception et la mise en œuvre d'une stratégie, des contrôles et des processus de lutte contre la fraude.



85 activités

Ces 17 principes aident à définir 85 activités dans les fonctions de première et de deuxième ligne, qui sont conçues pour maximiser la probabilité de prévention et de détection de la fraude en temps opportun et créer un fort effet de dissuasion grâce à une surveillance efficace, tout en tirant parti des synergies de l'entreprise.

Poser les jalons pour renforcer l'intégrité des programmes et réduire les risques de fraude



Sensibiliser, des échelons supérieurs aux échelons inférieurs



Comprendre et évaluer vos risques



Mettre en place les éléments de base (politique, cadre, modèle opérationnel)



Passer du modèle « payer et poursuivre » à la prévention grâce aux données et à l'analytique



Garantir l'efficacité de vos enquêtes



Amanda Holden

Associée

Service la criminalité financière

amholden@deloitte.ca

[linkedin.com/in/amandajholden/](https://www.linkedin.com/in/amandajholden/)

416-276-2092