Deloitte.

Intégrité des programmes au Canada
Où en sommes-nous?

Amanda Holden | Associée, Services-conseils en gestion des risques et criminalité financière de Deloitte

UNE INFLUENCE MARQUANTE depuis 1845

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

« L’intégrité dès la conception vise à s’assurer que les prestations et les services appropriés sont fournis aux bonnes personnes, aux fins prévues et au bon moment. »

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Incidence du manque d'intégrité des programmes

Perte financière

Perte d'argent, coûts liés à une enquête, règlement, perte de productivité

Médias et réputation

Bonne volonté politique, manchette des journaux, réputation de la marque personnelle et de la marque du parti

Incidence sur les citoyens

Perte de prestations, délai d'obtention des prestations trop lent, incidence sur le mode de vie, la santé et le revenu

Enquêtes et affaires juridiques

Frais juridiques, retard dans l'obtention des résultats, frais généraux des enquêtes

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Vue d'ensemble des fraudes dues à des escroqueries

ROYAUME-UNI

*Les pertes dues à des escroqueries ont totalisé **1,2 G£** en 2022*[1]

*UK Finance a rapporté qu'en 2022, les fraudeurs ont volé 2 300 livres sterling aux consommateurs britanniques **chaque minute**. Plus de 80 % des pertes totales imputables à la fraude au Royaume-Uni sont dues à des escroqueries, si bien que la situation est devenue une **urgence nationale**. La majorité des pertes dues à des escroqueries découlent de manœuvres frauduleuses liées à des investissements, à l'usurpation d'identité et à des achats, et sont perpétrées au moyen de diverses formes de paiements numériques.*

ÉTATS-UNIS

*Les pertes dues à des escroqueries ont totalisé **6,2 G$** en 2022*[2]

*D'après les données de la Federal Trade Commission, les consommateurs ont perdu 3,8 milliards de dollars dans des **manœuvres frauduleuses liées à des investissements** en 2022, suivies par les **arnaques à l'imposteur** qui se sont chiffrées à 2,6 milliards de dollars. Environ 18 millions d'Américains ont été fraudés dans le cadre d'escroqueries impliquant des portefeuilles numériques et des applications de paiement de personne à personne.*

AUSTRALIE

*Les pertes dues à des escroqueries ont totalisé **3 G$** en 2022*[3]

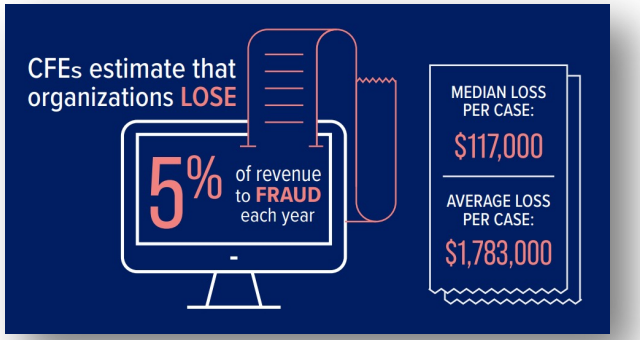
*96 % des Australiens ont été exposés à des escroqueries à la suite de récentes **atteintes à la sécurité des données** dans le pays. La plupart des pertes sont attribuables à des manœuvres frauduleuses liées aux investissements, aux accès à distance et aux **stratagèmes visant à rediriger des paiements** qui sont habituellement effectuées par textos et qui entraînent en moyenne une perte de 19 000 $ par fraude.*

En 2022, le Centre antifraude du Canada a signalé des pertes de plus de 530 millions de dollars dues à des escroqueries. Nous estimons cependant que l'exposition à des escroqueries au Canada totalise environ 1 milliard de dollars, si l'on compare avec l'Australie, dont la taille de l'économie est semblable.

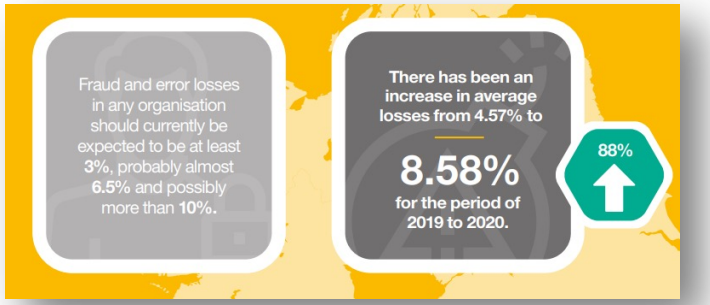
1. Over £1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online | Insights | UK Finance
2. FTC crunches the 2022 numbers. See where scammers continue to crunch consumers. | Federal Trade Commission
3. Scams are surging – CHOICE calls on banks to do more

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Comment évaluer l'ampleur du problème (ou de l'opportunité?)



https://legacy.acfe.com/report-to-the-nations/2022/



https://www.crowe.com/uk/insights/financial-cost-fraud-data-2021

Financial impact

Government entities generally lose between 0.5% and 5% of their spending to fraud and related loss based on international estimates. The majority of fraud is undetected and can be difficult to categorise. Measurement exercises can help entities uncover and more accurately estimate their potential fraud losses.

https://www.counterfraud.gov.au/total-impacts-fraud

Royal Canadian Mounted Police

Canada

Search

Services | Locations | A-Z site index | Careers | Help us

Home → News → Fraud Prevention Month 2023: Fraud losses in Canada reach another historic level

Fraud Prevention Month 2023: Fraud losses in Canada reach another historic level

February 27, 2023
Ottawa, Ontario

News release

In the past decade, technology has completely transformed the criminal landscape, making fraud easier to commit, more widespread, and more sophisticated than ever before.

In 2022, the Canadian Anti-Fraud Centre received fraud and cybercrime reports totalling a staggering $530 million in victim losses. Nearly a 40% increase from the unprecedented $380 million in losses in 2021. Unfortunately, the increase in financial loss isn't tied to an increase in reporting—the Canadian Anti-Fraud Centre estimates that only 5 to 10% of people report fraud.

The Canadian Anti-Fraud Centre, the Royal Canadian Mounted Police, and the Competition Bureau are once again joining forces this March to lead the 19th edition of Fraud Prevention Month. Under the theme "Tricks of the trade: What's in a fraudster's toolbox?", this year's campaign will expose fraudsters' tricks, tools and tactics, to help Canadians equip their own toolbox to protect themselves.

https://www.rcmp-grc.gc.ca/en/news/2023/fraud-prevention-month-2023-fraud-losses-canada-reach-historic-level

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Recherche de Deloitte : tirer parti du cadre du COSO

Gouvernance

Évaluation du risque de fraude

Évaluation et mise en œuvre des contrôles de prévention

Détection, enquête et communications

Suivi et amélioration

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Approches en matière d’intégrité des programmes

Culture réactive → **Culture proactive**

Principales caractéristiques réactives

- ✓ Manque de clarté
- ✓ Évaluations des risques rarement mises à jour
- ✓ Risques mal compris et non classés par ordre de priorité
- ✓ Degré plus élevé de complaisance (ou de manque de connaissances)
- ✓ Manque de leadership ou responsabilités mal définies

Principales caractéristiques proactives

- ✓ Risques bien définis et bien compris
- ✓ Évaluations des risques mises à jour régulièrement
- ✓ Valeurs claires et culture antifraude solide
- ✓ Examen minutieux et remise en question rigoureuse du conseil d’administration et de la direction
- ✓ Contrôles clairs appliqués en fonction des risques
- ✓ Séparation des tâches et établissement de mesures de protection

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Autorité internationale de lutte contre la fraude dans le secteur public

« Lorsque des gens commettent des fraudes contre le secteur public et les services publics, ils volent de l'argent aux services dont dépend le secteur public et ébranlent la confiance des citoyens envers le gouvernement. »

Il y aura toujours de la fraude – en effet, certaines personnes chercheront toujours à réaliser un gain si elles voient une occasion de le faire, et les organisations doivent se doter de processus robustes pour prévenir, détecter et combattre la fraude et la corruption.

La détection de la fraude est une bonne chose – on ne peut pas combattre la fraude si on ne la détecte pas. Un changement de perspective est requis afin que la détection de la fraude soit considérée comme une réalisation positive et proactive.

Il n'y a pas de solution unique – la lutte contre la fraude nécessite une réponse globale qui comprend la détection, la prévention et la réparation et qui est étayée par une solide compréhension du risque. Elle exige également que les organisations coopèrent dans un esprit de collaboration.

La fraude et la corruption évoluent constamment – les méthodes de fraude et de lutte contre la fraude évoluent très rapidement, et les organisations doivent être agiles et changer leur approche pour faire face à ces changements.

La prévention est le moyen le plus efficace de lutter contre la fraude et la corruption – la prévention à l'aide de méthodes efficaces de lutte contre la fraude réduit les pertes et les dommages à la réputation (bien que cela puisse être difficile à mesurer). Elle nécessite également moins de ressources qu'une approche axée sur la détection et la réparation.

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Création d’un cadre de gestion des risques de fraude robuste

Compte tenu de l’évolution du contexte, les organisations doivent s’assurer d’avoir un cadre de gestion des risques de fraude qui :

a) est incorporé au cadre global de gestion des risques;

b) est intégré et visible dans tous les secteurs de l’organisation;

c) instaure une culture soutenant la prévention, la détection et la dissuasion des comportements frauduleux;

d) est évalué régulièrement, et dont les contrôles sont redéfinis dès qu’une vulnérabilité à la fraude est repérée;

e) permet de réagir rapidement pour traiter les cas de fraude.

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Passez à l’action

Que peut faire votre organisation?

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

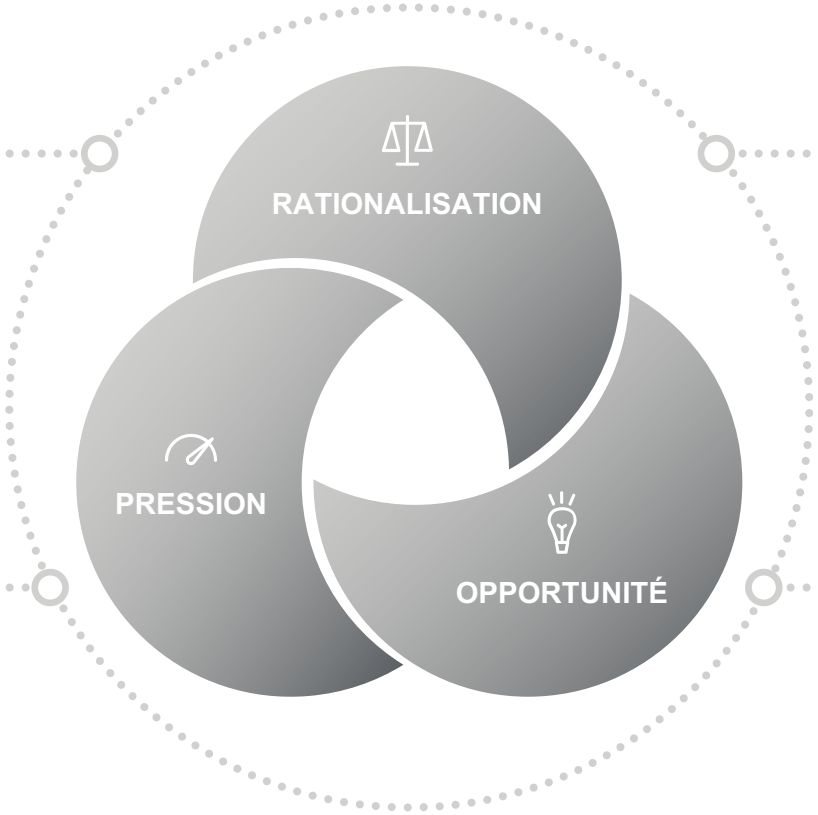
Prenez connaissance des différents types de risques de fraude

Fraude interne

Comprend un large éventail de risques liés aux employés ou aux fournisseurs qui détournent des actifs ou des fonds par l'intermédiaire de processus internes et de contrôles déficients. L'argent change de place au sein de l'organisation.

Fraude externe

Des acteurs externes, y compris des citoyens malavisés, des criminels et des membres du crime organisé, profitent de paiements sous forme de prestations, de subventions, de prêts, de remboursements d'impôt ou d'exemptions fiscales, etc. L'argent passe de l'intérieur à l'extérieur de l'organisation.



Menace interne

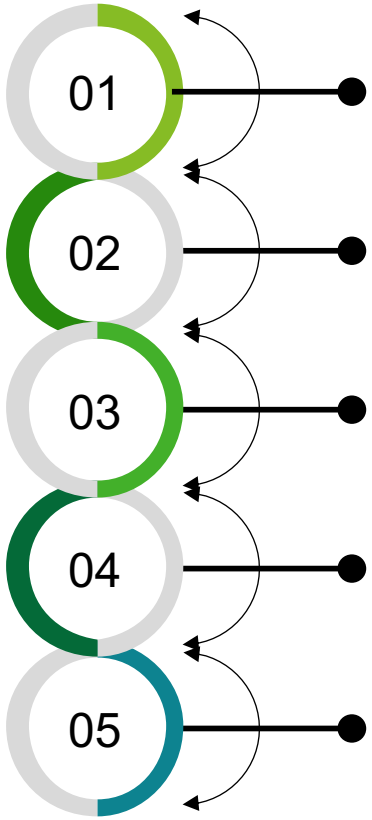
Pratique qui consiste à examiner les risques liés au rendement, aux activités, à l'accès aux données et aux systèmes et aux communications des employés, y compris l'analyse des sentiments, etc., afin d'éviter les activités inappropriées qui pourraient entraîner des fraudes, d'autres risques opérationnels ou une atteinte à la réputation et une réduction de l'intégrité du programme.

Cybermenaces

Protéger les technologies de l'organisation contre les accès et les utilisations inappropriés. Les cyberattaques peuvent être liées à une fraude ou faciliter la fraude à l'interne ou la fraude externe.

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Prenez connaissance des différents types de risques de fraude



Culture – message des dirigeants reconnaissant l'importance de la prévention de la fraude, favorisant l'établissement des priorités et la transparence du travail. Une bonne culture est essentielle, et le changement de culture doit être planifié.

Clarté – le premier défi : définir la fraude. L'évaluation des risques de fraude et la sensibilisation et la formation en matière de fraude sont primordiaux.

Communication – soutenir la culture et la clarté. Déterminer comment la communication peut améliorer la gestion des risques et la gouvernance.

Contrôles – réduire les risques inhérents au moyen de contrôles. Aligner les contrôles sur les risques et gérer l'évolution, le fonctionnement et l'amélioration continue des contrôles.

Vérifications – qui contrôle les contrôles? Veillez à ce qu'il existe un cadre qui comprend des examens et des améliorations à mesure que la maturité et les risques évoluent.

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Contacts

Amanda Holden

Partner
Financial Crime

amholden@deloitte.ca
linkedin.com/in/amandajholden/

416-276-2092

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Contacts

Dean Bowes

Directeur

Crime Financier

dbowes@deloitte.ca

613-786-7517

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Contacts

Katheryn Nowell

Directrice

Crime Financier

knowell@deloitte.ca

613-751-5366

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.