



## Program Integrity in Canada How Are We Doing?

Amanda Holden | Partner, Deloitte Financial Crime and Risk Advisory



## What is Program Integrity?

*“Integrity by Design aims to ensure that benefits and services are delivered to the right person, for the right purpose, at the right time, and in the right amount”*

# The Impact of Lack of Program Integrity



## Financial Loss

Money lost, costs to investigate, settlement, productivity loss



## Citizen Impact

Lost benefits, benefits are too slow, impact to way of life, health, income



## Citizen Trust

Political impact, culture of the country, custodians of taxpayers' dollars

## Media & Reputation



Political good will, front page news, person and party brand reputation

## Investigations & Legal



Legal costs, delay in outcomes, overhead of investigations

# Global View of Fraud via Scams



## UNITED KINGDOM

**£1.2B** total scams losses in 2022<sup>1</sup>

*UK Finance reported that scammers steal £2,300 from UK consumer every minute in 2022. Over 80% of total fraud losses in the UK are due to scams and it has become a **national emergency**. The majority of scam losses are driven by investment scams, impersonation scams and purchase scams and perpetrated through various digital payments.*



## UNITED STATES

**\$6.2B** total scams losses in 2022<sup>2</sup>

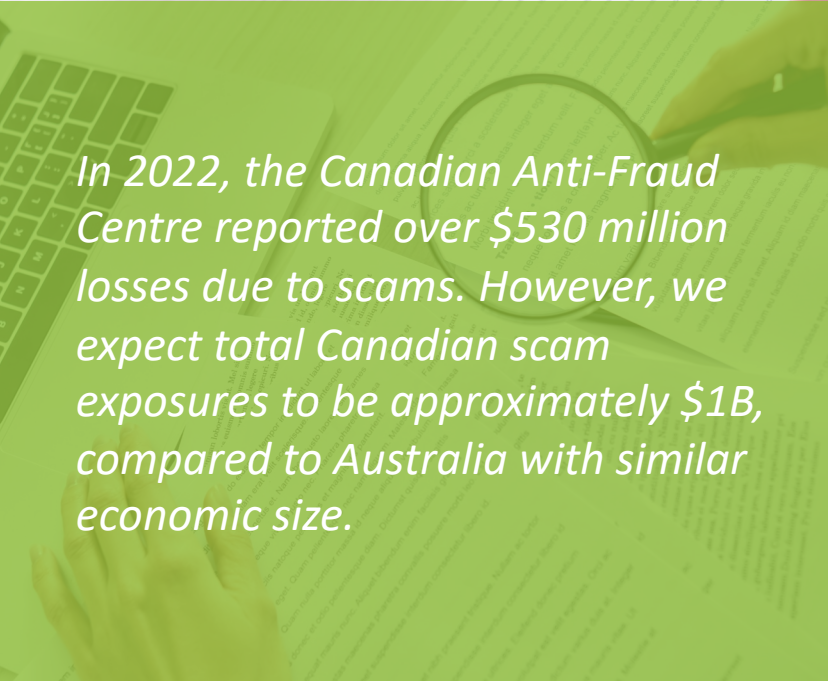
*The Federal Trade Commission data shows that consumers reported losing \$3.8 billion to **investment scams**, followed by \$2.6 billion to **imposter scams** in 2022. Approximately 18 million Americans were defrauded through scams involving digital wallets and person-to-person payment apps.*



## AUSTRALIA

**\$3B** total scams losses in 2022<sup>3</sup>

*96% of Australians were exposed to scams due to recent **data breaches** in the country. Most of losses are driven by investment, remote access, and **payment redirection schemes**, that are typically initiated through text message and on average result in \$19k loss per event*

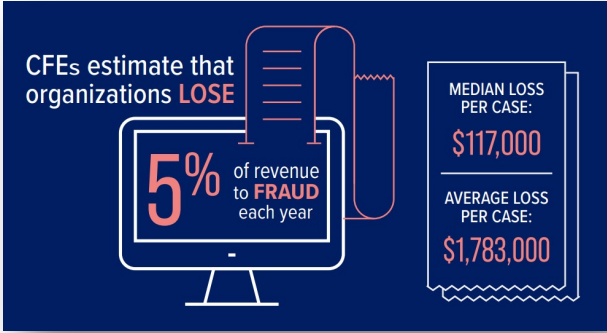


*In 2022, the Canadian Anti-Fraud Centre reported over \$530 million losses due to scams. However, we expect total Canadian scam exposures to be approximately \$1B, compared to Australia with similar economic size.*



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](#)

# Can We Size the Problem (or Opportunity?)



<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

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 Research Leveraging the COSO Framework




Governance




Fraud Risk Assessments



Prevention Controls Assessment and Implementation



Detection, Investigation and Communications



Monitoring and Improvement

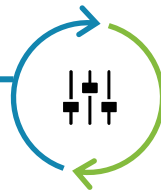
# A Range of Approaches to Program Integrity

## Reactive Culture

## Proactive Culture

### Main Reactive Characteristics

- ✓ A lack of clarity
- ✓ Risk assessments are rarely updated
- ✓ Risks are not fully understood and not prioritized
- ✓ Higher degree of complacency (or lack of awareness)
- ✓ No clear leadership or accountability



### Main Proactive Characteristics

- ✓ Risks are well defined and understood
- ✓ Risk assessments are reviewed regularly
- ✓ Clear values and a strong fraud culture
- ✓ Greater degree of board/leadership scrutiny and challenge
- ✓ Clear controls, applied based on risks
- ✓ Full segregation of duties/lines of defense set up

# The International Public Sector Fraud Authority

*“Where people commit fraud against the public sector and public services, they take money away from the services on which the public sector depends, and damage citizens’ trust in government.”*



**There is always going to be fraud** - It is a fact that some individuals will look to make gain where there is opportunity, and organizations need robust processes in place to prevent, detect and respond to fraud and corruption.

**Finding fraud is a good thing** - If you don't find fraud you can't fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.

**There is no one solution** - Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk. It also requires cooperation between organizations under a spirit of collaboration.

**Fraud and corruption are ever changing** - Fraud, and counter fraud practices, evolve very quickly and organizations must be agile and change their approach to deal with these evolutions.

**Prevention is the most effective way to address fraud and corruption** - Preventing fraud through effective counter fraud practices reduces the loss and reputational damage (although this can be difficult to measure). It also requires less resources than an approach focused on detection and recovery.



# Creation of a robust fraud risk management framework

**With the evolving fraud risk landscape in mind, organizations should ensure they have a fraud risk framework that:**

- a) is integrated into the overall risk management framework
- b) is embedded and visible within all areas of the organization
- c) develops a culture which supports the prevention, detection and deterrence of fraudulent behavior
- d) is regularly assessed, with controls redesigned their vulnerability to fraud is identified
- e) response to address fraud swiftly





# Take Action

What Can Your Organization Do?

# Be Aware of the Different Types of Fraud Risks

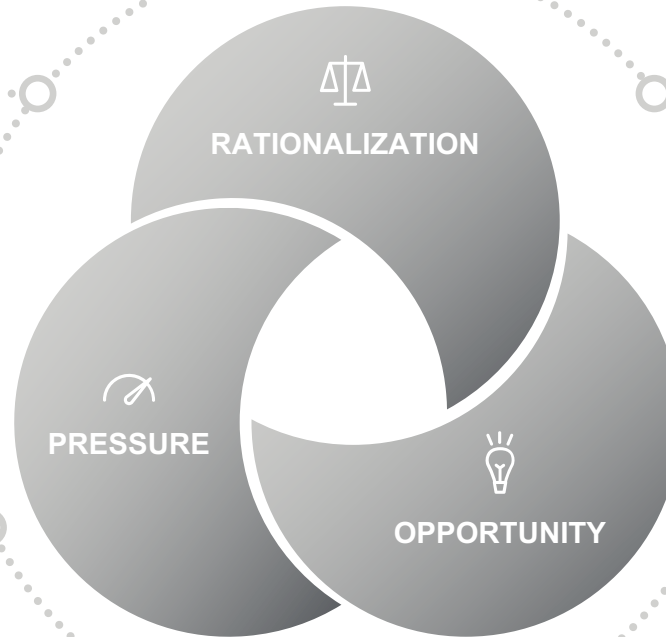
## Internal Fraud

Includes a wide range of risks where employees or vendors misappropriate assets, funds through internal processes and weak controls. Money that moves within the organization.



## External Fraud

External actors including misguided citizens, criminals and organized crime take advantage of payments in the form of benefits, grants, loans, tax refunds/ exemptions, etc. Money that moves from within to outside the organization.



## Insider Risk

The practice of examining risks in employee performance, activities, data/systems access, communications including sentiment analysis, etc., to prevent inappropriate activities that may result in fraud, other operational risks or reputational and reduced program integrity.

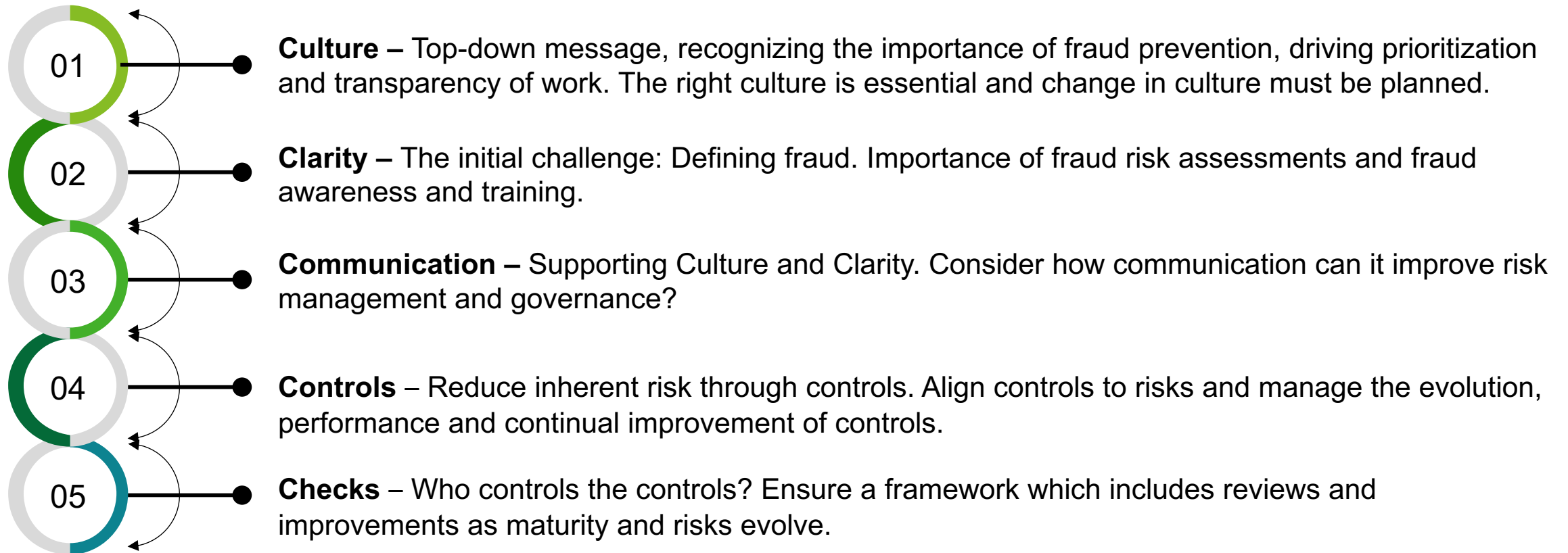


## Cyber Threats

Securing the organization's technology from inappropriate access and manipulation. Cyber attacks may be a predicate activity to fraud &/or may facilitate internal or external fraud.



# Be Aware of the Different Types of Fraud Risks



# Contacts



**Amanda Holden**

*Partner  
Financial Crime*

[amholden@deloitte.ca](mailto:amholden@deloitte.ca)

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

416-276-2092



# Contacts



**Dean Bowes**

*Director*

*Financial Crime*

[dbowes@deloitte.ca](mailto:dbowes@deloitte.ca)

613-786-7517



# Contacts



**Katheryn Nowell**

*Manager*

*Financial Crime*

[knowell@deloitte.ca](mailto:knowell@deloitte.ca)

613-751-5366

