Deloitte.

Fraud Risk in an Era of Operational Fiscal Constraint and Strategic Investment

I. Introduction[1]

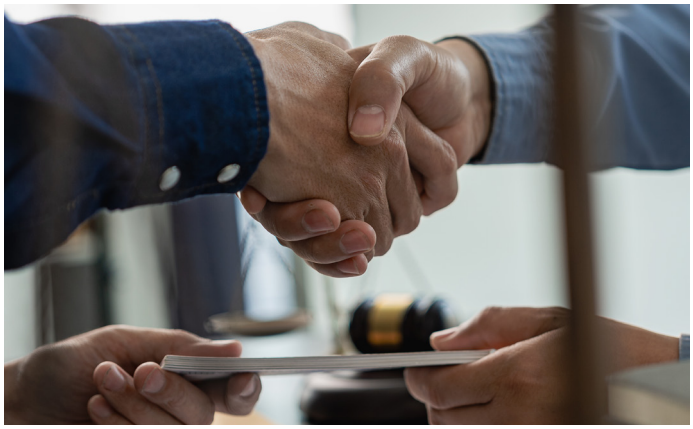
Fraud is an intentional act involving deception to obtain an unjust or illegal advantage, committed by individuals inside or outside the organization.[2] In the public sector, fraud is not simply a financial issue; it is a governance issue. Every dollar lost to fraud is a dollar not available for essential public services and it undermines confidence in public institutions and services. According to the Association of Certified Fraud Examiners (ACFE) Report to the Nations,[3] median losses in government[4] have steadily increased over the past 20 years. In 2004, government agencies and public administration experienced a median loss of $45,000 per case. By 2024, this figure had risen to $200,000, highlighting the growing financial impact of fraud on the public sector.[5] While Canada lacks a comprehensive, government-wide estimate of fraud, waste, and abuse,[6] a commentary published in 2023 on the Public Accounts of Canada 2022–23 pointed to a sharp rise in lost public money (a category that includes theft and fraudulent claims) with losses estimated at approximately $283 million, nearly double the prior fiscal year.[7]

Governments are stewards of the public trust. Public servants are entrusted with taxpayers' money through defined authorities and controls. Sustaining public confidence depends on how effectively these governance arrangements are designed, maintained, and monitored over time.

Today, this challenge is intensified by multiple simultaneous forces: fiscal pressure and complexity, a period marked by broad operational constraints, including workforce reductions and limited operating budgets, alongside targeted strategic investments in areas such as defense, economic development, and infrastructure. In addition, the increasing sophistication of fraud schemes, fueled by rapid technological advances, is further compounding the issue. Together, these elements are transforming both the opportunities for fraud and governments' ability to prevent it.

KEY TAKEAWAY

Fraud in the public sector is fundamentally a governance risk and not just a financial one. Multiple simultaneous forces, including fiscal pressure, operational constraints, and growing strategic investments, are increasing both the opportunity for fraud and the difficulty of preventing or detecting it.



1 The Authors: Dean Bowes is a Director in the Financial Crimes Practice at Deloitte Canada. Pavithra Chandramouli and Katheryn Nowell are Senior Managers in the same group. The authors would like to thank Mirelle Foorer, Analyst, at Deloitte for her contribution to this point of view.

2 https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud and https://publications.gc.ca/collections/collection_2019/bvg-oag/FA3-138-2018-eng.pdf

3 The ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training education and certification. They publish a global study on occupational fraud every year based on data collected through surveys across the globe (https://www.acfe.com/ and https://legacy.acfe.com/report-to-the-nations/2024/)

4 Refers to government agencies and public administration as an industry category as per the ACFE Report to the Nations (https://www.acfe.com/ and https://legacy.acfe.com/report-to-the-nations/2024/)

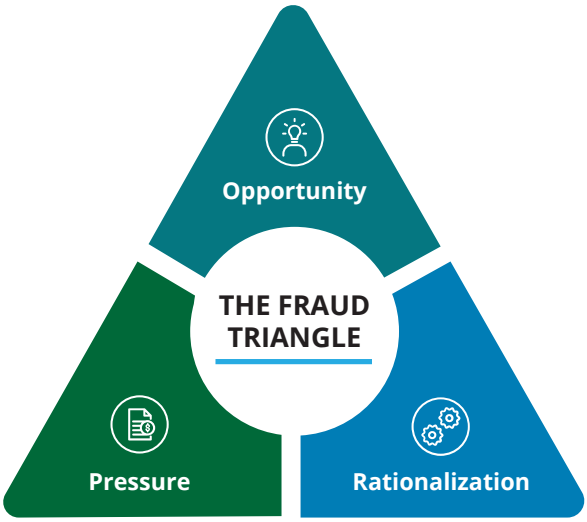
5 https://www.acfe.com/fraud-magazine/all-issues/issue/article?s=evolution-of-government-fraud

6 Deloitte's White Paper on Embracing fraud prevention: Program integrity in the Canadian public sector (2024), https://cdn.luminari.co/lumiq%2Fepisodes%2Famolkvf04J6eqBhWcKEa%2Frevisions%2F4546%2Fresources%2FnNMdn1kiuS.pdf

7 Laura Ryckewaert, "Federal revenue, property, money losses spike to $534.2 million in 2022–23," The Hill Times, November 15, 2023, https://www.hilltimes.com/story/2023/11/15/federal-revenue-property-moneylosses-spike-to-534-2-million-in-2022-23/402825.

II. Applying the Fraud Triangle During Operational Fiscal Constraints

Why can fraud risk increase during downsizing even without malicious intent? White collar fraud does not always begin with criminal intent. More often, it emerges at the intersection of pressure, opportunity, and rationalization – widely known as the Fraud Triangle.[8]



Pressure in the public sector may take many forms: financial stress, career stagnation, political mandates/targets, or organizational uncertainty. Austerity measures, hiring freezes, and restructurings can heighten professional and personal anxiety, particularly where job security and financial stability are perceived to be at risk. These conditions can create an environment in which ethical boundaries are more easily rationalized. A 2009 ACFE survey conducted during the economic recession found that about half of respondents cited increased pressure as the biggest factor contributing to the increase in fraud.[9]

Opportunity arises when internal controls weaken or governance and oversight becomes fragmented. This is where organizational design matters most. Segregation of duties, supervisory review, audit coverage, and data monitoring are not merely technical controls; they are structural barriers that limit the opportunity to commit fraud. When these elements erode, fraud does not become inevitable, but it becomes easier.

Rationalization allows individuals to justify wrongdoing. In government settings, this often takes the form of entitlement ("I am underpaid for the extra work I have to do with the downsized workforce"), normalization ("everyone cuts corners"), or displacement of blame ("the system is broken anyway"). Organizational culture plays a decisive role here. Tone at the top, ethical clarity, and consistent accountability can disrupt rationalization long before misconduct occurs.

Crucially, the Fraud Triangle reminds us that fraud is not solely about "bad actors." It is about systems that either constrain or enable unethical behavior. In periods of sustained pressure, individuals can experience ethical drift – where individuals who would not ordinarily rationalize misconduct may do so as personal and organizational pressures, workload, and perceived unfairness accumulate. This is why fraud risk can rise even in high-integrity organizations. The public sector is not immune to this risk, particularly in the context of current fiscal constraints.

While leaders cannot eliminate pressure during such periods, they can deliberately reduce opportunity and actively challenge rationalization through clear expectations, visible oversight, and consistent accountability.

KEY TAKEAWAY

Fraud risk increases during periods of sustained pressure not because organizations hire "bad actors," but because financial stress, weakened controls, and cultural rationalization combine to create conditions where **Ethical drift** becomes more likely even in high-integrity environments.

8 https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud
9 https://www.acfe.com/-/media/files/acfe/pdfs/occupational-fraud.pdf

III. Operational Fiscal Constraints and Their Unintended Consequences

During periods of fiscal constraint, governments are forced to make difficult trade-offs. Individually, these decisions are often reasonable and necessary to maintain service delivery and advance strategic priorities. However, when viewed collectively, workforce reductions, role consolidation, and deferred oversight can create conditions in which fraud is easier to commit and significantly harder to detect. When budgets tighten, several organizational shifts commonly occur:

- **Reduced segregation of duties**, as fewer staff are asked to perform multiple roles.
- **Loss of institutional knowledge**, when experienced staff depart and are not replaced.
- **Increased reliance on trust**, rather than verification, to maintain operational continuity.
- **Delayed or scaled back audits**, especially those perceived as low risk.
- **Postponement of fraud risk management activities**, as these may be considered non-essential.
- **Minimal or lack of resources** to pursue investigative or remedial actions.

These changes may appear incremental, but their cumulative effect collectively weakens the control environment. The result is not only a higher risk of fraud, but a lower likelihood of timely detection.

An analysis by the Center for American Progress found that budget cuts of approximately USD $6 billion between FY2011 and FY2014 led to an estimated USD $27 billion increase in fraud, waste, and abuse across four sectors: Internal Revenue Service, Inspector General, Program Integrity, and Government Accountability Office.[10] Audit findings from the Office of the Auditor General of Ontario also highlight weakened control environments, reduced oversight capacity, and heightened ethics and management risks as a result of lesser resources.[11] Additionally, reports from other federal or provincial-level governments in other countries have echoed similar concerns including their inability to pursue investigative and remediation efforts due to lack of resources.[12]

Both insider and external fraud schemes can proliferate in such vulnerable environments. Common **insider fraud risks** include misuse of organization-issued credit cards, expense reimbursement fraud, moonlighting,[13] and payroll fraud. **External/ collusive fraud risks** include billing fraud,[14] grants or contributions fraud, and social engineering tactics such as phishing or business email compromise attacks. Additionally, some departments face unique risks such as an increase in benefit claims, which may be falsified, as observed during the pandemic.

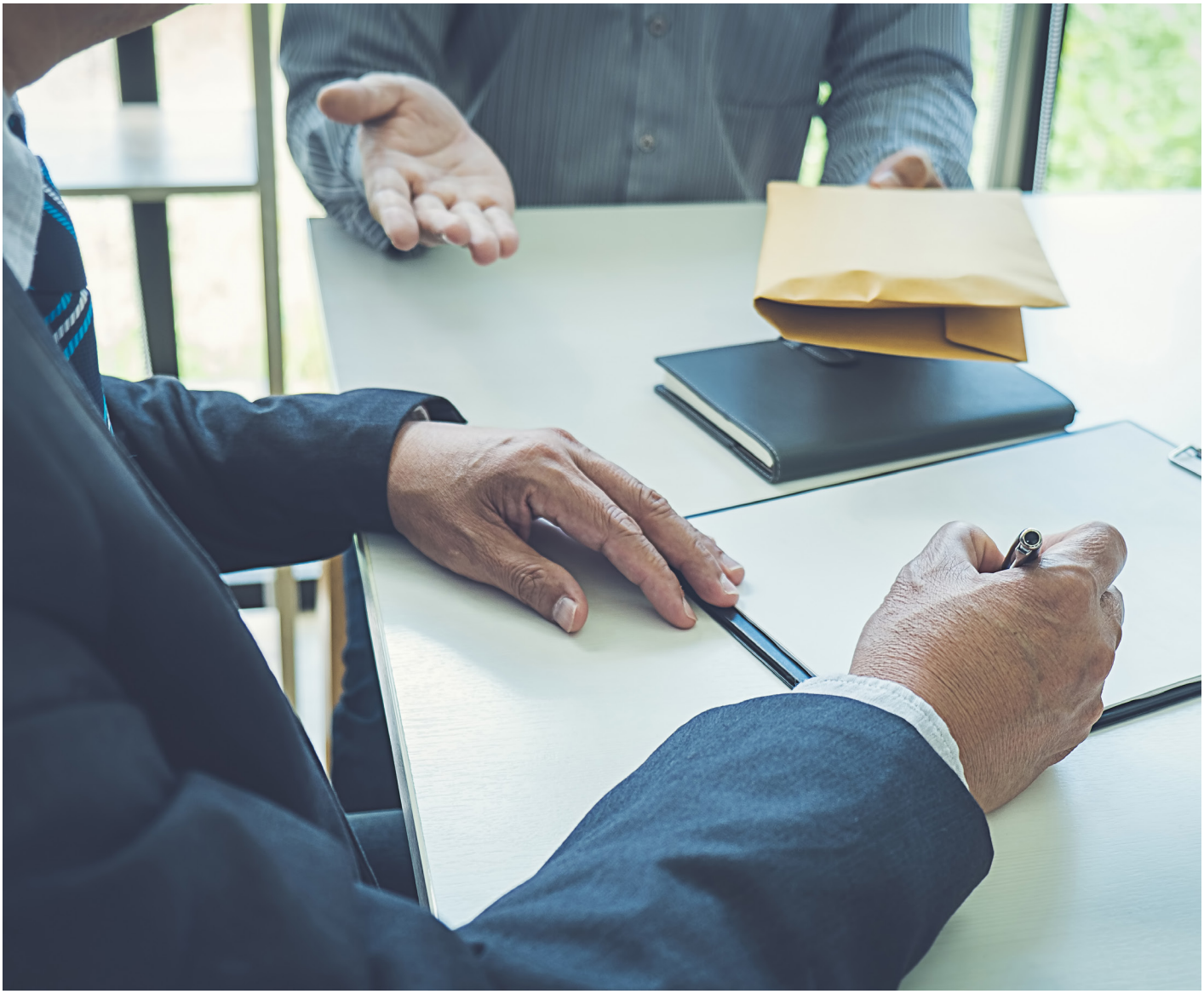
The departure of employees as part of downsizing initiatives could lead to diminished accountability, possible reduced segregation of duties, and increased workloads for remaining staff, all of which further exacerbate these vulnerabilities.

In parallel, increased strategic investments introduce their own fraud risks, including accelerated procurement, increased use of third parties, compressed timelines, and expanded program delivery at scale. Without commensurate attention to controls and oversight, strategic investment initiatives may inadvertently increase exposure to fraud, waste, and abuse.

10 https://www.americanprogress.org/article/how-shortsighted-spending-cuts-increase-waste-fraud-and-abuse/
11 Example OAG reports: https://www.auditor.on.ca/en/content/annualreports/arreports/en24/pa_ONimmigrant_en24.pdf, https://www.auditor.on.ca/en/content/annualreports/arreports/en25/pa_OPB_en25.pdf
12 Audit finds budget cuts limited Health Department's ability to combat fraud | Louisiana Department of Health
13 Moonlighting is defined as the act of working at an extra job, especially without telling your main employer (https://dictionary.cambridge.org/dictionary/english/moonlighting). While moonlighting itself may not be considered illegal or a fraudulent activity in Canada, it can lead to potential conflicts of interest or misuse of an employer's resources when an employee is performing one or more jobs during the same working hours (https://hrinsider.ca/create-policy-to-control-overemployment-and-moonlighting/).
14 Billing fraud refers to a scheme where vendors or external service providers submit false or inflated invoices.

KEY TAKEAWAY

- On one hand, incremental cost cutting decisions such as reduced segregation of duties, deferred audits, and loss of institutional knowledge can collectively weaken the control environment, increasing both the likelihood of fraud and the risk that it goes undetected.
- On the other, while strategic investments are necessary to advance public priorities, accelerated procurement, reliance on third parties, and compressed delivery timelines can introduce new fraud risks if integrity and oversight are not embedded from the outset.



IV. Technology: A Force Multiplier for Both Sides

Compounding these challenges, the tools available to commit fraud are becoming more sophisticated and accessible. Technologies such as generative artificial intelligence can now be used to create highly convincing documents, invoices, emails, and identities. These tools are now cheap, accessible and easy to use.

Social engineering schemes have evolved beyond generic phishing and have become more commonly available, making them accessible to an average person. Fraudsters can tailor messages using publicly available information, mimic writing styles, clone voices, and exploit moments of organizational disruption – making attacks more likely to succeed when staff are stretched thin. The increasing volume and speed of these attacks further amplify vulnerabilities across organizations.

Budget cuts can unintentionally worsen this technology-driven exposure, as training on emerging risks is often postponed or deprioritized. Meanwhile, fraudsters innovate continuously, unconstrained by procurement rules or funding approvals. The asymmetry is stark: governments are asked to do more with less, while fraud schemes become faster, cheaper, and harder to detect.

KEY TAKEAWAY

Emerging technologies, particularly generative AI and advanced social engineering, are dramatically lowering the cost and sophistication required to commit fraud, while fiscal constraints often delay training and defenses, creating a growing asymmetry between governments and fraudsters.

V. Getting Ahead of Fraud Risk: Practical Steps for Governments

Fraudsters do not wait for austerity drives to end; they exploit opportunities as they arise. To stay ahead, governments should use practical and cost-effective approaches to strengthen fraud prevention and detection. These are leadership and governance choices, not new programs or systems.

01. Prioritize fraud awareness, training and reporting channels

Awareness is one of the most cost-effective fraud controls. Training employees to recognize red flags and social engineering tactics equips them to handle potential fraud risks and resolve ethical dilemmas. It also helps employees recognize that fraud is common and real and reinforces the tone from the top around fraud and business ethics. Even brief, targeted training can yield disproportionate benefits by turning staff into active defenders of public resources.

Reinforce the importance of reporting concerns and the channels available. According to the 2024 ACFE Report to the Nations, tips remain the most common method of initial fraud detection, accounting for **43% of cases**. Notably, more than half of these tips come from employees, underscoring the importance of staff engagement and awareness.[15] A 2022 focus group study by the Office of the Public Sector Integrity Commissioner, conducted in the context of the Public Servants Disclosure Protection Act (PSDPA), found that many federal public servants reported low awareness of formal disclosure mechanisms for protected disclosure and reprisal protection, and that fear of reprisal was the most frequently cited concern influencing decisions to report wrongdoing. The study also noted that participants recommended improved training and awareness related to whistleblowing and reporting wrongdoing, as well as efforts to normalize reporting as an acceptable part of workplace culture.[16]

02. Treat fraud risk as a core governance issue

Clear expectations, consistent consequences, and visible leadership commitment are critical, especially during organizational stress.

Fraud risk should be part of the organization's annual risk assessment and management processes, not addressed only after incidents occur. Conduct regular environmental scans to identify high-risk areas and use focused fraud risk assessments (FRAs) to ensure risks are identified and mitigation measures are documented and understood. Conducting risk-based, targeted FRAs is more effective than deferring action to complete a single, organization-wide FRA.

Where new programs or initiatives are launched as part of strategic investments, leaders should adopt an **integrity-by-design** approach: identifying and addressing fraud risks early, before delivery pressures, scale, or complexity limit effective oversight.

03. Use data/automation strategically, not expansively

Governments do not need costly, enterprise-wide systems to improve fraud detection. Targeted analytics on high-risk transactions can compensate for reduced staffing and resources. Leverage data analytics for anomaly detection and focus efforts where the risk is greatest.

Where fiscal restraints create opportunities for automation including via artificial intelligence, ensure risk mitigation is considered early and leverage automation for fraud mitigation (it's two sides of the same coin).

04. Implement effective and efficient remediation measures

Ensure your reporting channels are working and the team responsible for investigation and remediation is well-prepared when suspected fraud is reported. Procedures should be clearly outlined for intake, triage, investigation, reporting, and remediation. In times of operating budget constraints, streamlined and effective processes are essential to maximize impact with limited resources.

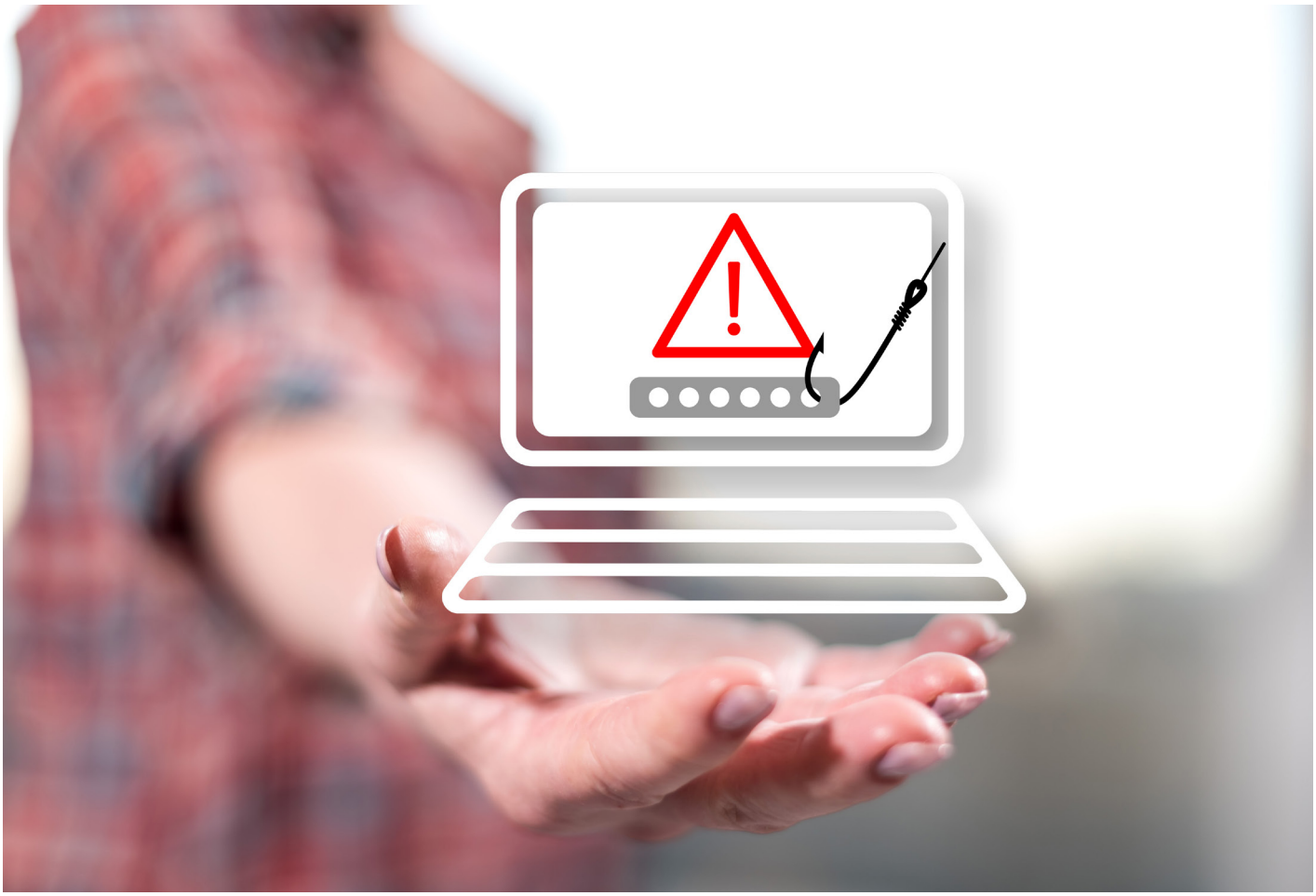
15 ACFE Occupational Fraud 2024: Report to the Nations (https://legacy.acfe.com/report-to-the-nations/2024/)

16 Final report on focus group discussions held in spring 2022 (https://www.psic-ispc.gc.ca/en/resources/corporate-publications/2022-focus-group-final-report)

KEY TAKEAWAY

Even during times of fiscal constraint, governments can reduce fraud risk through focused, leadership driven actions that strengthen awareness, governance, data use, and remediation without relying on large, resource intensive investments. In practice, this means:

- Keeping fraud risk visible through targeted awareness, training, and trusted reporting channels that empower employees to identify and report concerns early
- Treating fraud risk as an ongoing governance issue by conducting regular, risk based and iterative fraud risk assessments rather than deferring action
- Using data, analytics, and automation strategically (i.e., by focusing on high risk areas) and embedding fraud prevention early when new technologies or processes are introduced
- Ensuring reporting, investigation, and remediation processes are clear, efficient, and ready to act when concerns arise, even with limited resources



VI. CONCLUSION

Fraud risk does not rise in isolation. It grows where pressure intensifies, controls erode, and technology accelerates opportunity. Operational constraints and strategic investment both test control discipline. In this environment, fraud risk management is not a back-office function but a leadership responsibility. How leaders balance control discipline with effective oversight will determine whether today's fiscal decisions are remembered as responsible stewardship or costly false economies that erode public trust.

Contacts

Dean Bowes
Director

Risk, Regulatory and Forensics
Email: dbowes@deloitte.ca
Ph: +1 613 786 7517

Amanda Holden
Partner

Risk, Regulatory and Forensics
Email: amholden@deloitte.ca
Ph: +1 416 360 1336

Pavithra Chandramouli
Senior Manager

Risk, Regulatory and Forensics
Email: pchandramouli@deloitte.ca
Ph: +1 613 751 6669

Katheryn Nowell
Senior Manager

Risk, Regulatory and Forensics
Email: knowell@deloitte.ca
Ph: +1 613 751 5366

Deloitte.

www.deloitte.ca