



International Public Sector Fraud Forum Guide to Designing Counter Fraud and Corruption Awareness Training for Public Bodies



February 2020

Crown copyright disclaimer

The information contained in the International Public Sector Fraud Forum documentation and training is subject to Crown Copyright 2020.

You should not without the explicit permission of the International Public Sector Fraud Forum:

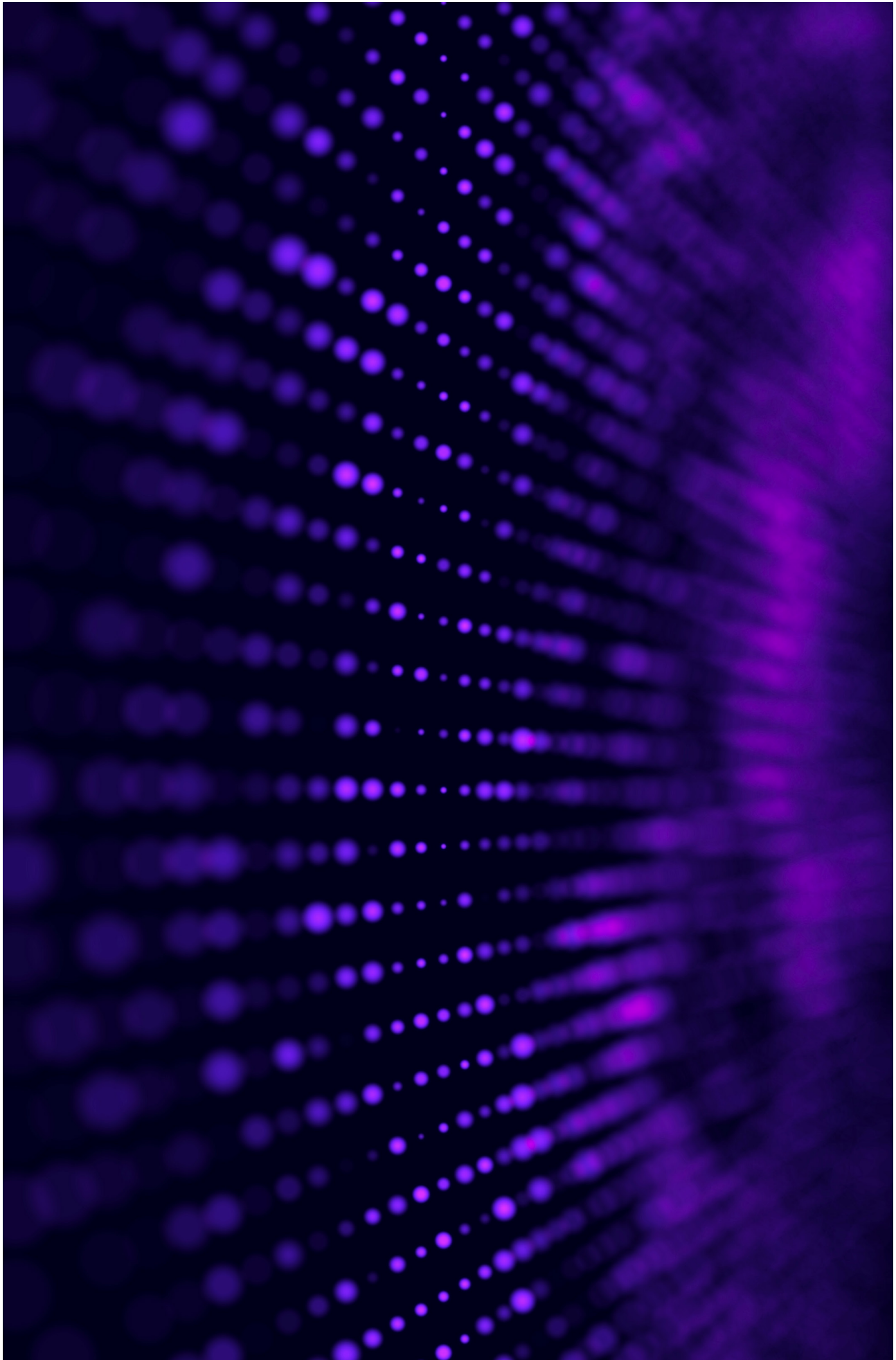
- copy, publish, distribute or transmit the Information;
- adapt the information;
- exploit the information commercially or non-commercially for example, by combining it with other information, or by including it in your own product or application.

The information should not be published or distributed in any way that could undermine the values and aims of the International Public Sector Fraud Forum.

This content consists of material which has been developed and approved by the International Public Sector Fraud Forum.

Contents

| | |
|---|-----------|
| The International Public Sector Fraud Forum | 5 |
| Foreword | 6 |
| Introduction | 8 |
| Part I – Value of a Counter Fraud and Corruption Awareness Training Program | 9 |
| Raising Sustained Awareness of Fraud and Corruption | 9 |
| The Wider Benefits of Fraud and Corruption Awareness Training | 10 |
| Seeking Senior Management Buy-In | 11 |
| Soliciting Employees’ Support | 13 |
| Top Tips for Implementing Fraud and Corruption Awareness | 14 |
| Part II – Planning and Designing a Counter Fraud and Corruption Training Program | 15 |
| Identifying Needs | 17 |
| Outlining Learning Goals and Objectives | 17 |
| Targeting the Audiences | 18 |
| Types of Adult Learners | 19 |
| Selecting the Methodology (Approach) | 20 |
| Determining the Frequency | 20 |
| Developing the Training Curriculum | 21 |
| Topics typically found in Counter Fraud and Corruption Training Programs | 24 |
| Evaluating a Counter Fraud and Corruption Awareness Training Program | 35 |
| Annex A – Questions to Ask in the Planning Phase | 38 |
| Annex B – Glossary | 40 |
| Annex C – Examples of Misconduct | 42 |
| Annex D – Examples of Fraud Controls | 44 |
| Annex E – Selecting the Training Delivery Methods, Techniques and Developing Exercises | 46 |
| Acknowledgement | 50 |





The International Public Sector Fraud Forum

The International Public Sector Fraud Forum (IPSFF) currently consists of representatives from organisations in the governments of Australia, Canada, New Zealand, the United Kingdom and the United States. The collective aim of the Forum is to come together to share best and leading practice in fraud management and control across public borders.

The Forum has established 5 principles for public sector fraud.



1. There is always going to be fraud

It is a fact that some individuals will look to make gains where there is opportunity, and organisations need robust processes in place to prevent, detect and respond to fraud and corruption.

2. 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.

3. 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 organisations under a spirit of collaboration.

4. Fraud and corruption are ever changing

Fraud, and counter fraud practices, evolve very quickly and organisations must be agile and change their approach to deal with these evolutions.

5. Prevention is the most effective way to address fraud and corruption

Preventing fraud through effective counter fraud practices reduces the loss and reputational damage. It also requires less resources than an approach focused on detection and recovery.

Foreword



Jeremy Sales

Director General, Integrity Services Branch
Employment and Social Development Canada / Service Canada

Fraud is a global reality. No government or organization is immune; rather the intensity level changes from one country to another. While governments and organizations have different contexts, needs and a counter fraud culture at varying levels of maturity, the threats they face are similar and very real.

Fraud is the result of human activity. As long as individuals are part of a business process, the risk of fraud exists.¹ Notwithstanding the presumption by some organizations that fraud issues do not exist within their program or organization, or that employees and stakeholders would never steal or commit fraud, the reality is that fraud occurs everywhere. Public bodies are most vulnerable when they invest the least amount

of action to develop solutions to prevent and detect fraud and do not see the need to invest in internal controls.²

Good governance principles require that public bodies encourage high ethical behaviour within the organization, as well as establish strong controls, to deter fraudulent behaviours or activities. Key to this is the development of enhanced fraud training within the organization. This is accomplished through the implementation and design of an effective counter fraud program, which demonstrates a strong stance against, and a real willingness to limit the risks of, fraud.³

Fraud and corruption are complex issues and must be the subject of a holistic approach by governments and organizations alike. Although not all fraud and corruption activities can be prevented, early detection and an expedited and targeted response can reduce losses. Moreover, the extended impacts of fraud do not just result in financial losses, but may also impact service delivery, public safety, the environment, and much

1 The Chief Financial Officers Council (CFOC) and the U.S. Department of the Treasury, Bureau of the Fiscal Service (2018), Program Integrity: The Antifraud Playbook.
2 Ibid.; ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program;
3 Julien de Meeûs d'Argenteuil et Nathalie Bailly 2011, L'Administration belge des douanes et accises : une approche singulière de la lutte contre la corruption, Pyramides [Online 07 septembre 2011], <http://journals.openedition.org/pyramides/228> [Free translation - Consulted November 14, 2019].

more. Public bodies will be better equipped to combat fraud and corruption if they have:

- A comprehensive understanding of the major fraud and corruption risks and threats they face;
- Knowledge of behavioural sciences and techniques designed to encourage compliance; and
- Effective controls in place to prevent, detect, deter and respond to fraud and corruption.

This Guide to Designing Counter Fraud and Corruption Awareness Training Programs for Public Bodies, is designed to assist those leading fraud control responses in public sector organisations to take the necessary measures to implement an effective and lasting counter fraud and corruption program, including effective counter fraud controls and a strong awareness and training program.

Introduction

The International Public Sector Fraud Forum (IPSFF) is comprised of representatives from the governments of Australia, Canada, New Zealand, the United Kingdom and the United States. The purpose of the IPSFF is to share amongst its members best practice in combatting public sector fraud in order to reduce the harm caused by fraud and corruption.

As part of achieving this purpose, the IPSFF has set out to develop products that can be used by public sector agencies in the fight against fraud. This Guide to Designing Counter Fraud and Corruption Awareness Training Programs for Public Bodies, is designed to assist those leading fraud control responses in public sector organisations to take the necessary measures to implement an effective and lasting counter fraud and corruption program, including effective counter fraud controls and a strong awareness and training program.

It is divided into two parts. **Part I** of the Guide emphasizes and focuses on the value and importance of implementing a counter fraud and corruption awareness training program for public bodies. It underscores the importance of delivering sustained fraud awareness at all levels of the organisation and the need to secure senior management and employee buy-in.

Part II of the Guide focuses more specifically on the steps required in planning, designing, developing and evaluating an effective counter fraud and corruption awareness training program, along with concrete examples to illustrate the various recommended approaches. This section will be of particular interest to a broader range of public officials, including individuals who are involved in designing internal training for employees (e.g., Learning Advisors, Human Resources, Values and Ethics, Internal Services, etc.) and those tasked with ensuring the effective design, administration and compliance of public policies, including programs and services (e.g., Audit and Evaluation, Finances, Grants and Contributions, Program/Service Managers, Policymakers, etc.).

The Guide speaks mainly to internal fraud. However, in some areas, information on external fraud is also provided. It should be noted that the strategies to prevent, identify, deter and address external fraud tend to differ, as the perspective when looking at internal versus external threat varies.



Part I – Value of a Counter Fraud and Corruption Awareness Training Program

Fraud and corruption occurs in every organisation, is increasingly complex and ever changing. It is simply not possible to detect, investigate and prosecute your way out of fraud and corruption.

Therefore fraud control leaders must create a counter fraud response focussed on prevention to effectively reduce the risks of fraud and corruption. A key component of this is effective communication and targeted training for all employees, which is designed to raise awareness of internal and external fraud risks. This approach is considered to be one of the most successful, efficient and effective methods to prevent, identify, deter and address fraud and corruption.⁴

Raising Sustained Awareness of Fraud and Corruption

Targeted counter fraud and corruption awareness training is a highly effective way to assist employees in better identifying suspicious activity and empowering them to act appropriately against potential fraud.⁵ Identifying fraud and corruption risks is key to improving integrity within an organization.

A targeted counter fraud and corruption awareness training program is an effective tool to communicate solutions, to assist in preventing and deterring fraud, and to resolve fraud cases more quickly, in order to enhance the successful delivery of a public body's mission.⁶

Communications specialists and learning advisors express the belief that developing an ongoing awareness program⁷ that focusses on fraud and corruption risks specific to the organisation or work program is key to encouraging and sustaining new behaviours and attitudes, as well as acting as a continuing reminder to all employees following training. Frequent exposure to counter fraud and corruption topics is key to raising awareness in employees and to ensuring that they absorb and apply what they learn.

Designing and adopting a counter fraud and corruption awareness training program allows for the elaboration of key messages, along with varying activities that can be adapted and framed to communicate different purposes and reach various audiences. An effective communication strategy will support employees by providing clear guidelines and tools to ensure privacy, security and protection of data and programs. It will also encourage

4 OECD (2019), Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit, OECD Publishing, Paris, <https://doi.org/10.1787/9ea76a8f-en>; United Nations Office on Drugs and Crime (2005), United Nations Convention against Corruption. https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf; Association of Certified Fraud Examiners—ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program – Responding to Ethics Breaches and Noncompliance. https://www.acfe.com/uploadedFiles/ACFE_Website/Content/review/diafp/09-Responding-to-Ethical-Breaches-and-Noncompliance.pdf; Employment and Social Development Canada—ESDC (2015), Self-Study Guide on Writing Learning Objectives, [internal document].

5 Ibid; ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program; OECD (2018), Behavioural Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption, OECD Publishing, Paris, <https://doi.org/10.1787/9789264297067-en>

6 Playbook CFOC (2018) Program Integrity: The Antifraud Playbook

7 In the context of this document awareness program and communication program are used interchangeably.

employees to adopt appropriate behaviours and attitudes and will support improved ethical decision-making. Finally, it enables employees to identify fraud risks and vulnerabilities in their daily functions or duties, as they are guided by information shared through effective training programs.

Reinforcing management's commitment to counter fraud activities and demonstrating the success of the controls in place are critical aspects of an awareness strategy. Therefore, as part of any communication program it is imperative that employees are periodically made aware of the statistics and types of fraud and corruption activities that occur in organizations and ideally the consequences (e.g., number of reprimands, suspensions, termination of employment, etc.), subject of course to privacy considerations.

When the highest political and management levels within the public sector demonstrate their dedication to combatting fraud and corruption, it enhances integrity. It also reduces the risks of fraud and corruption. An explicit senior level commitment to counter fraud and corruption influences and impacts how integrity is perceived across the public sector and, by extension, society⁸. If employees do not perceive senior officials as the personification of the organization and its counter fraud values, the efforts and resources invested to combat fraud and corruption may not achieve the intended objectives. Integrity should be at the foundation of the organizational culture. The “tone at the top” is imperative for building a

culture of integrity and has a trickle-down impact on employees, reinforcing that culture of integrity.

The Wider Benefits of Fraud and Corruption Awareness Training

Among its many benefits for public bodies, a counter fraud and corruption training program can:

- Foster a culture of integrity, compliance, trust and honesty;
- Reinforce the organization's commitment to high ethical standards and a strong counter fraud and corruption stance;
- Increase compliance with laws, regulations and other initiatives, and reduces violations;
- Sustain the development of programs, policies and services more resistant to fraud;
- Protect an organization from regulatory scrutiny;
- Increase the quality of tips received;
- Avoid an organization being subject to corporate monitoring;
- Protect an organization from liability;
- Allow for a quick response to noncompliance; and
- Build trust with employees, stakeholders, citizens and other public bodies.⁹

8 Canada Revenue Agency (2019), Collaborative Approach to Ensuring Privacy and Security, [internal document].

9 Ibid; ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program; OECD (2018), Behavioural Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption, OECD Publishing, Paris, <https://doi.org/10.1787/9789264297067-en>.



Seeking Senior Management Buy-In

Specialists agree that commitment from senior management is the single most important factor in determining the success of a counter fraud and corruption communication program. Buy-in from senior management is also one of the key cornerstones to guaranteeing the implementation of a credible and successful counter fraud and corruption program. Ensuring that senior management endorses the value of counter fraud and corruption program may require a cost-benefits analysis and/or an illustration of the impacts of fraud on the public body's strategic outcomes. The benefits and impacts of implementing a counter fraud and corruption training program should serve to convince senior management of its added value.

Although quantifying the financial loss of fraud is essential, other impacts can be just as, if not more, harmful to public services, the government and the citizens they serve. For more guidance, the IPSFF Guide to Understanding the Total Impact of Fraud provides assistance to public bodies in identifying and measuring the impacts of fraud and/or the cost benefits of counter fraud activity and programming. The following summarizes some of the impacts of fraud that could be considered when seeking senior management buy-in:

Preventing or reducing costs

It is generally accepted that estimates of the costs of fraud can be challenging to quantify, despite significant financial and other losses encountered. As a result, it may be difficult to approve training or other related expenditures in the absence of known and tangible metrics on which an evidence-based decision can be made. If the actual state of fraud within a public body is unknown, it makes it onerous to tangibly demonstrate the value for money of implementing the necessary preventive controls and supporting resources, including counter fraud training. Despite these challenges, a counter fraud and corruption program contributes to preventing or reducing both direct (e.g., fines, financial penalties, jail sentences, if found guilty, etc.) and indirect (e.g., investigation, litigation, or remediation) costs of fraud.¹⁰

Avoiding reputation damage

The impact of fraud and corruption on a public body's reputation can be devastating. Damaging publicity is often more sensitive for senior management than almost any other issue, as it generally occurs when fraud could have been prevented or has been mismanaged. The aftermath of a fraud-related scandal tarnishes a public body's image and potentially decreases its credibility, leading to a loss of confidence and trust by other public bodies, industries, the public and politicians. Emphasizing the potential negative publicity and the devastating effect on an public body's reputation may increase the likelihood of gaining buy-in from senior management, since such training is meant to eliminate or reduce

10 CFOC (2018), Program Integrity: The Antifraud Playbook; ACFE (2019) Developing an Integrated Anti-Fraud, Compliance, and Ethics Program.

this effect.¹¹ Although not easily measurable or quantified in terms of costs, specialists evaluate the monetary value of a private organization's reputation at 60% of its stock price.¹²

Reducing human impacts

Individuals, families and communities' lives are impacted, sometimes destroyed, as a result of opportunistic individuals and organized crime groups committing fraudulent acts. More often than not, the victims are those already in precarious or challenging situations in their day to day lives. Demonstrating the far-reaching impacts of fraud beyond financial loss and taking into consideration the human impacts of fraud by illustrating how it leaves victims with a range of physical, psychological and emotional health problems (e.g., distress, stress, agitation, worry, anger, feeling of violation, anxiety, loss of self-esteem, fear, depression¹³) may help senior management approach fraud in a more meaningful way. Emphasizing the benefits of reducing human impacts on the delivery of services to the citizens an organization strives to serve may be effective in persuading senior management to endorse a counter fraud training program.

Limiting government systems and outcomes

Fraud compromises a government's ability to deliver services and achieve its intended outcomes. This can result in services not

being delivered, failure to achieve program objectives, or worse, the shut down of services and programs, negatively impacting the citizens who rely on them. Faulty infrastructure and capacity drain could also occur, affecting the client experience. All of these impacts can result in a loss of opportunities for a program or service and may lead to an increase in business costs arising from the resulting efforts to address financial and opportunities losses. Costs relating to investigation, audit, compliance reviews, adjudication, court proceedings and identification systems are expensive, in addition to increased costs for the prison and welfare systems.

Helping to attract and retain high-quality employees

In recent years, the factor that attracts most prospective employees is the culture an organization embodies and communicates. Employees are drawn to organizations that are supportive, motivational and team-oriented.¹⁴ When senior management fosters a culture of transparency and emphasizes ethical behaviours and compliance, employees are more likely to emulate these behaviours. An effective counter fraud and corruption training program supports this objective by striving to reduce non-compliance issues that negatively affect service delivery and improve employee decision-making, communication and collaboration – all of which generally

11 CFOC (2018) Program Integrity: The Antifraud Playbook, 2018; ACFE (2019) Developing an Integrated Anti-Fraud, Compliance, and Ethics Program.

12 ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program.

13 Deloitte (2012), Fraud Risk Management – Providing Insight into Fraud Prevention, Detection and Response, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/Forensic-Proactive-services/in-fa-frm-noexp.pdf> [Consulted June 2019].

14 CFOC (2018) Program Integrity: The Antifraud Playbook; ACFE (2019) Developing an Integrated Anti-Fraud, Compliance, and Ethics Program.



result in higher quality services. Horizontal collaboration with internal and external stakeholders, such as risk management, ethics, learning, finances, audit, program/service areas, and other public bodies, to strengthen the training curriculum can be leveraged for many purposes, including attracting and retaining high-quality employees.

From a behavioural sciences perspective, when seeking senior management buy-in it is important to consider that people are not motivated to act by the idea of gaining something new. Rather, it is their sense of loss avoidance that is likely to have the most influence on them.¹⁵ Research suggests that people actually care greatly about fairness and what others might lose, which can be capitalized on by emphasizing the risks of not implementing an effective counter fraud and corruption training program. Demonstrating how non-engagement and not reporting fraud and corruption might result in worse public service, loss of public funds that would otherwise be spent on programs and services for the more vulnerable peoples, and reduction of trust in the public sector by citizens, may prove to be more effective than presenting only the benefits of a counter fraud and corruption training program.¹⁶

Promoting the program across the organization from the top down, as well as across and within programs, is crucial to eliminating the perception that a public body relies on poor processes and controls. It is vital for public

bodies to be proactive in developing, implementing and reinforcing the elements of counter fraud and corruption programs by promoting awareness and training throughout the organization, at all levels, to foster a strong counter fraud and corruption culture.

Soliciting Employees' Support

It is equally important to obtain acceptance and support from employees to attend counter fraud and corruption training once the “tone at the top” is clear and buy-in at the senior management level is achieved. Involving the program management team to solicit employee support and acceptance helps to ensure program support and increases the sense of employee empowerment.

Obtaining staff buy-in to attend counter fraud and corruption training starts by providing them with the value-added rationale and reasons to adopt the change and/or behaviour(s) advocated.¹⁷ The foundation for achieving a successful culture of integrity and compliance begins with an emphasis on transparency and communication in an organization. This lays the groundwork for an effective counter fraud and corruption training program. When employees see the importance placed on transparency and communication, counter fraud and corruption training can serve to motivate improvements in business operations.¹⁸ It can inspire staff, resulting in better awareness and common knowledge, which, in turn, encourages

15 Nieves Zúñiga - Transparency International (2018), Behavioural Changes against Corruption, <https://knowledgehub.transparency.org/assets/uploads/helpdesk/behavioural-changes-against-corruption-2018.pdf> [Consulted June 2019]

16 Ibid.

17 CFOC (2018) Program Integrity: The Antifraud Playbook, ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program; Radhika Kapur (2018), Designing and Implementation of Training Programs in Organizations, https://www.researchgate.net/publication/323833964_Designing_and_Implementation_of_Training_Programs_in_Organizations. [Consulted June 2019].

18 CFOC (2018), Program Integrity: The Antifraud Playbook.

ethical decision-making. It can also serve to improve employees' job satisfaction, while reinforcing their sense of right and wrong.¹⁹

Employees should feel engaged and inspired when taking training in the workplace. Seeing counter fraud and corruption awareness training as a vital stepping-stone to career development or soliciting ways to turn training into being viewed as something valuable and positive keeps employees engaged as agents of integrity and increases the "feel good" feeling. A culture of integrity and compliance can also raise morale and enhance productivity.²⁰

Defining, supporting, controlling and enforcing public integrity sends a clear message that integrity is valued and protected within the organization. Early intervention methods, such as counter fraud and corruption training, have become a best practice commonly accepted to prevent, identify, deter and respond to fraud and corruption. These types of methods diminish risk, sustain integrity, and support professional development. By adopting effective awareness and training programs, public bodies are in a better position to reduce liability, mitigate risk, and enhance the integrity and reputation of the organization.

Top Tips for Implementing Fraud and Corruption Awareness

- Receive and ensure endorsement from senior management;
- Are communicated consistently throughout the organization, from leadership to employees at all levels;
- Target relevant employees, considering their job functions, roles and responsibilities;
- Base messaging upon the results of organisation or work program specific fraud risk assessments;
- Tailor initiatives and activities to best fit the needs of a public body and its employees;
- Integrate awareness initiatives and activities with other communication efforts, whenever possible; and
- Ensure regular, frequent, and effective awareness activities in a variety of settings, using multiple methods and techniques.²¹

19 ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program

20 Ibid.

21 KPMG (2014), Fraud Risk Management – Developing a strategy for prevention, detection and response. <https://assets.kpmg/content/dam/kpmg/pdf/2014/05/fraud-risk-management-strategy-prevention-detection-response-O-201405.pdf>. The Chief Financial Officers Council (CFOC) and the U.S. Department of the Treasury, Bureau of the Fiscal Service (2018), Program Integrity: The Antifraud Playbook.

Part II – Planning and Designing a Counter Fraud and Corruption Training Program

Part II of the Guide outlines the steps to plan, design, support and evaluate a counter fraud and corruption training program.

This section also describes key concepts and controls to prevent, identify, deter and respond effectively to fraud and corruption. Public bodies may consider including them in a counter fraud and corruption training program. Informative text boxes, as well as complementary fraud and corruption-related information and statistics, are presented throughout to assist public officials who wish to strengthen their respective training curriculum. Additional information to enhance the training objectives and content is available in the annexes of this Guide. We recommend that you consult with a learning expert when planning and designing a training program, as they can provide expert advice and guidance.

Targeted counter fraud and corruption awareness training is essential to helping an organization's employees better identify suspicious activity and feel empowered to act appropriately against potential wrongdoing. Public bodies should design and use counter fraud and corruption awareness training to leverage and support staff by:

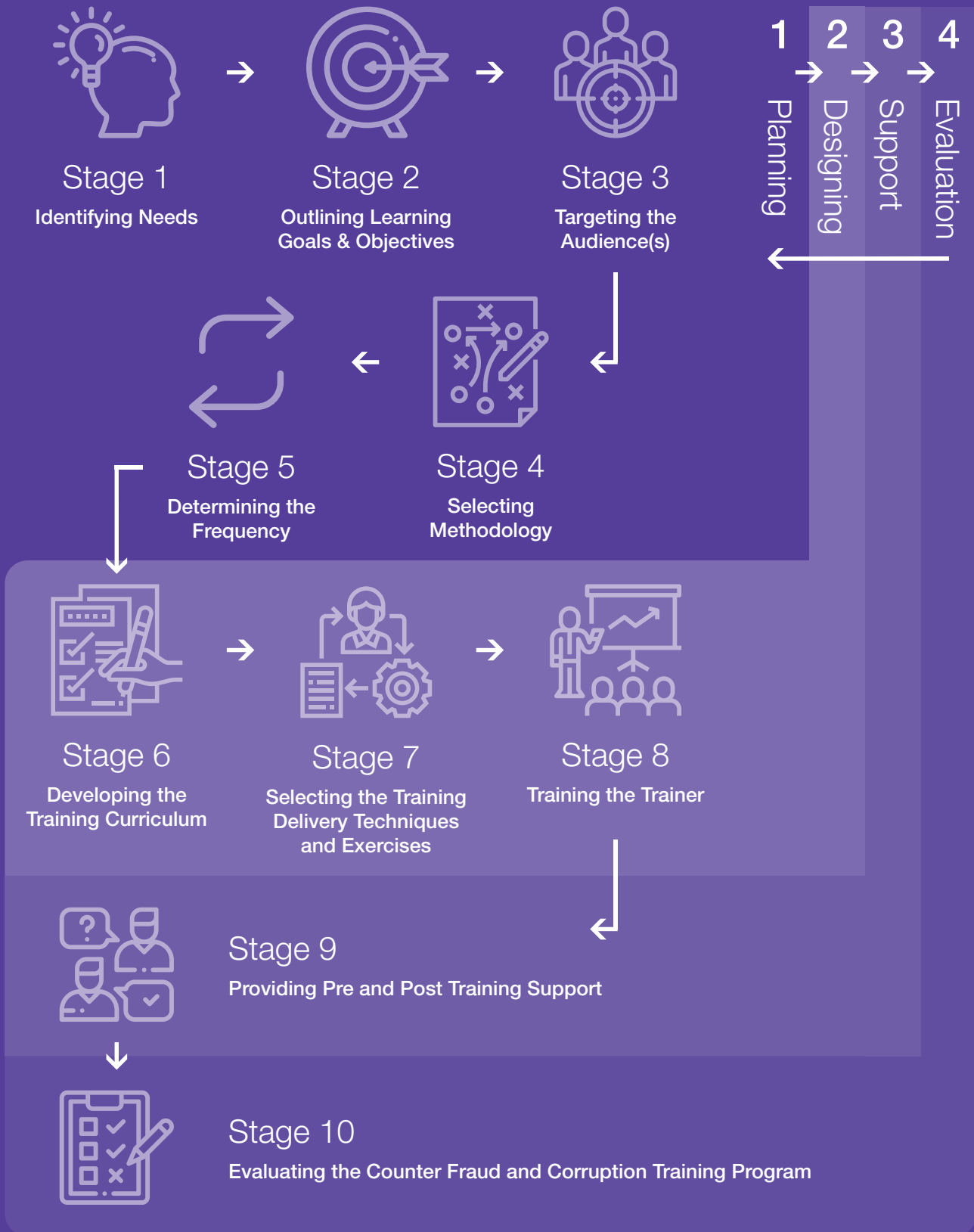
- Educating them about why integrity, ethics and compliance are important to the organization and to them;
- Providing definitions and explaining the types of fraud and corruption they may encounter within their organization;
- Raising awareness of the organization's fraud policy and the consequences associated with its violation;

- Explaining to them how uncovering fraud is good for the organization and the public sector as a whole;
- Making them aware of the behavioural red flags of fraudsters and the controls in place to prevent, detect, deter and address fraud and corruption;
- Informing them about the consequences and impacts of fraud and corruption on the public sector, public servants, targeted victims, and the public at large; and
- Providing the processes, mechanisms and tools to report and respond to fraud and corruption.

The following illustration demonstrates the key steps to designing an effective counter fraud and corruption training program, presented in the sections below, including:

- Identifying needs;
- Outlining learning goals and objectives;
- Targeting the audiences;
- Selecting the methodology;
- Determining the frequency;
- Selecting the training delivery techniques;
- Training the trainer;
- Providing Pre-and Post-training support; and
- Evaluating the training program.

Key steps to designing an effective counter fraud and corruption training program



Identifying Needs

An effective counter fraud and corruption awareness training program for employees begins with identifying the specific needs of the organization and the individuals and groups within it. In order to identify the needs of a public body, it is essential to do the following:

- Identify and develop a full and formal understanding of the organization’s current knowledge base and its ideal knowledge base in relation to counter fraud and corruption;
- Pinpoint, at the onset, the context and/or urgency for counter fraud and corruption training; and
- Enable the organization to bring its staff to the desired level of performance, behaviour and/or approach.²²

Some elements to look for when identifying needs for counter fraud and corruption awareness training include (may vary based on a public body’s context):

- The existence (or not) of essential policies, directives and guidelines, legislation and regulations, rules, procedures, processes, roles and responsibilities, controls and measures, etc.;
- Whether training is already offered within the organization, other public bodies and/or the public sector’s training college; and
- Identification of stakeholders who should be involved (subject matter experts in the field of counter fraud, learning advisors, management, finances, audit, program areas, internal services, etc.).



A list of questions to consider when identifying needs is provided in **Annex A – Questions to Ask in the Planning Phase.**

Outlining Learning Goals and Objectives

Once the needs for counter fraud and corruption awareness training are clearly identified, the learning goals and objectives must be set. Although similar and often used interchangeably, the terms “learning goals” and “objectives” differ. Learning advisors²³ have clearly defined both concepts to help design internal training for employees:

Learning Goals

Broad, general statements articulating what the program, course or activity intends to accomplish, without providing the specifics on how to achieve them. They provide a framework for determining the more specific objectives of a program. They outline the learning target(s) that the training is aiming to reach:

- Example: Learners will become familiar with the organization’s key concepts and principles of its counter fraud and corruption program and policies.

²² ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program; Kapur 2018

²³ ESDC (2015), Self-Study Guide on Writing Learning Objectives.

- Example: Policymakers understand regulations, policies and principles to protect against, detect and address fraud and corruption within the organization.

Learning Objectives

Clearly articulated specific, measurable and attainable descriptions of what the learner will know or be able to do by the end of the training. They can also act as benchmarks to measure progress towards the achievements of larger goals:

- Example: This training will enable employees to identify potential fraud or corruption activities, and report them through appropriate channels, knowing they are protected against potential reprisal.

Targeting the Audiences

Targeting and knowing the audiences are critically important for the counter fraud and corruption training awareness program's success. Selecting the right audiences enables the identification of the learning styles and types of adult learners. This will later help to identify the appropriate delivery methods, techniques and exercises in the design process.

Given the importance and applicability of the training, and how widespread and indiscriminate fraud and corruption can be, participation should be mandatory for every employee. No one should be exempt from attending some form of counter fraud and corruption awareness training. However, recognizing that employee training costs money, it is important to ensure that

organization-wide training effectively concentrates resources where needed most.²⁴ When designing a training program, a public body should determine:

- The training elements that are most appropriate for every employee; and
- Those that are most appropriate for specific targeted groups (i.e., one size may not fit all).

It is important to keep in mind that a minimum understanding is required for every employee to effectively fight against fraud and corruption. Over and above that baseline understanding, employees may need additional training based on their respective roles and/or functions and the risks of fraud inherent to their position.

Employees may not necessarily have the same needs and interests, nor the same level of knowledge of counter fraud and corruption principles and concepts. Realistically, some topics may only benefit employees whose positions might require specific knowledge. Thus, there is unlikely a need to address these topics in an organization-wide training course.

²⁴ ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program.



Types of Adult Learners



Doer

Primarily engaged through practice and applying concepts, including practicing the new information acquired.



Thinker

Relies on logic and reason. Interested in logical thinking, problem solving, suggestions, viewpoints, analysis, evaluation. When assigned work, performs on an independent basis. Prefers training to enhance skills and abilities.



Feeler

People-orientated, expressive, and communicative, knows how to express feelings and perspective. Enhances knowledge in open and unstructured environment. Does not need well-organised training program. Prefers personal experiences, group exercises, role plays.



Observer

Learns by observing supervisors and colleagues, capable to inculcate task within their mindset to perform it later. Patient, persistent, takes time to understand. Prefers lectures, discussions and problem solving, taking notes and observe any practical conducts.

Styles of Adult Learning



Visual (spatial):

Prefers using pictures, images and spatial understanding.



Aural (auditory-musical):

Prefers using sound and music.



Verbal (linguistic):

Prefers using words, both in speech and writing.



Physical (kinaesthetic):

Prefers using their body, hands and sense of touch:



Logical (mathematical):

Prefers using logic, reasoning and systems.



Social (interpersonal):

Prefers to learn in groups or with other people.



Solitary (interpersonal):

Prefers to work alone and use self-study.

Selecting the Methodology (Approach)

Once a public body's needs, goals, objectives and audiences are identified, it is important to establish the training methodology (approach).

The training methodology describes what the high-level training strategy is, and should:

- Be built on the needs and requirements of the organization;
- Be based on the feasibility to change the learning objectives into outcomes;
- Connect the contents with the audiences; and
- Not be mistaken with the delivery methods/techniques or exercises, which will support the methodology later in the design phase, by providing direction on how the training will be delivered to employees.²⁵

Regardless of the size of an organization, training is more effective when delivered in real-time in a small group. However, a combination of approaches might be more appropriate, such as:

- Instructor-led;
- Technology-based;
- Simulations; and
- On-the-job training.

Determining the Frequency

As mentioned above, counter fraud and corruption awareness training should be mandatory for all employees, ideally shortly after joining the organization and being appointed to a new position. In addition to mandatory training, best practices suggest that frequent exposure to counter fraud and corruption topics are key to ensuring employees absorb, retain and apply what they learn.²⁶

For a training program to be effective, therefore, it is recommended that a yearly refresher or periodic targeted learning sessions be developed and delivered to address organization-specific fraud concerns, change in circumstances or key risks, or if and when new risks arise.²⁷ It is important to point out that fraud and corruption are not perpetrated in static ways, as schemes and activities continually evolve and emerge. Therefore, it is crucial to ensure that training is fresh, ongoing and current. If the same information is conveyed repetitively year after year, it will not be effective. Employees generally have limited hours available for training and they need proof of the value added when removed from their daily job for training purposes.

25 Ibid; Kapur 2018; Employment and Social Development Canada 2015.

26 Leyland 2012; ACFE (2019), *Developing an Integrated Anti-Fraud, Compliance, and Ethics Program*; ESDC (2015), *Self-Study Guide on Writing Learning Objectives*.

27 ACFE (2019), *Developing an Integrated Anti-Fraud, Compliance, and Ethics Program*; OECD (2018), *Behavioural Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption*; CFOC (2018), *Program Integrity: The Antifraud Playbook*; ESDC (2015), *Self-Study Guide on Writing Learning Objectives*.

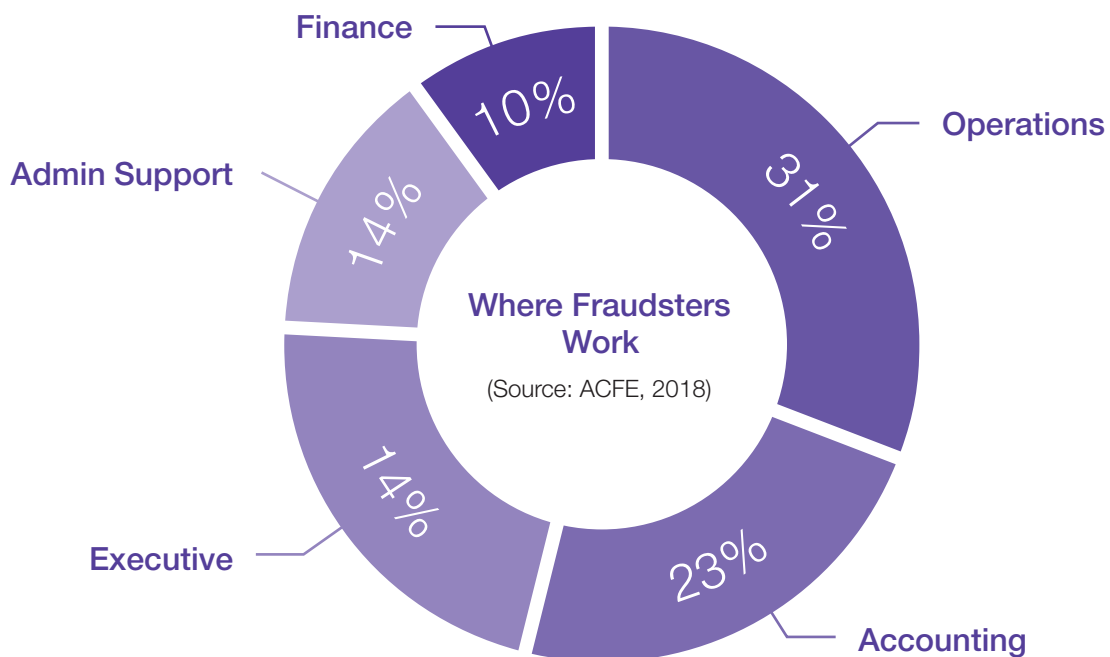
Developing the Training Curriculum

While it may be tempting to purchase a generic program or to emulate a counter fraud and corruption awareness training package from another organization, it is generally less effective than developing a customized curriculum that addresses the specific needs, objectives, priorities and maturity level of a given public body.

The curriculum should do more than just inform about specific rules. A segment of the training contents should be delivered systematically to all staff, ensuring they receive the same information to set the necessary knowledge baseline for other material presented as part of the organization’s counter fraud and corruption program.

Specialists agree that consultation and collaboration with experts in counter fraud and corruption, values and ethics practitioners, experienced learning advisors and other relevant stakeholders within the organization will help to design and develop an effective training program,²⁸ which will be reinforced and informed through their expertise and input.

Most public bodies have developed enterprise risk management functions and have financial reporting, improper payment, and internal control programs. Look for quick wins and work with program managers and leaders to gather lessons learned, processes, tools, and existing data from others’ efforts tailored to the organization. Building on these undertakings will avoid reinventing the wheel. It will not only be more effective; it will likely also increase adoption and support from those already working in these areas.²⁹



28 ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program; ESDC 2015; Kapur 2018.

29 CFOC (2018), Program Integrity: The Antifraud Playbook.

The following are some considerations to keep in mind when developing curriculum contents:

- Set clear expectations with respect to content.
- Limit content to what is directly related to the learning objectives:
 - *Tailor to the organization and the audiences;*
 - *Focus on highest-risk areas; and*
 - *Link to employees' work, roles and responsibilities.*
- Make content as interesting and interactive as possible.
- Incorporate design flexibilities to reach different types and styles of learners.
- Consider including:
 - *Links between compliance, ethics and fraud and ethical decision-making;*
 - *What to do or not with realistic scenarios and/or simulations;*
 - *Protection of information and data;*
 - *Cybersecurity;*
 - *Insider trading;*
 - *Procurement and contracts; and*
 - *Compliance with laws and policies.*³⁰

As noted above, it is recommended that opportunities for segmented or targeted training be explored. Some topics are likely to be of primary benefit only to those whose positions might require such knowledge. In these cases, there may not be a need to address them in the broader, organization-wide training.³¹ The following examples offer some suggestions for targeted training:

- For those working directly with citizens: How to recognize suspicious information on benefit applications;
- For newly appointed investigators: How to conduct an investigation; and
- For counter fraud specialists: How to interpret data obtained from advanced and predictive analytics.

Evidence suggests that senior management is generally involved in the most devastating fraud and/or corruption violations, causing ripple effects throughout an organization.³² It typically results in a breakdown of corporate culture. For that reason, senior officials should receive specialized training covering executive-specific topics, such as policies and roles and responsibilities for building, reinforcing and actively communicating the organization's commitment to counter fraud and corruption.³³

30 ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program.

31 Ibid.

32 ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program

33 Ibid.



Canada Border Services Agency: Insider Threat and Security Concerns

In 2013, the Canada Border Services Agency (CBSA) designed and implemented its Insider Threat and Security Concerns awareness training, which provides a good model of internal training to fight fraud and misconduct.

What makes the CBSA awareness training stand out is how well it is planned, designed and delivered. First, the learning goals and objectives are clearly defined to ensure that employees know how to detect, report, avoid and mitigate situations of fraud and misconduct. It communicates and reinforces the expected behaviour for all employees – on and off duty. It also makes them aware of issues that may have an impact on them.

Subsequently, the frequency and methodologies were also adapted to the needs of the organization and the target audiences. For instance, the course is systematically offered in-person to all new recruits by the end of their formal training, before beginning their duties. A mandatory online version is also available for all employees.

The contents are adapted to the Agency's mandate and the target audiences, while the methods of delivery and exercises allow the training to reach different types of learners, stimulate discussions and encourage sharing of experiences.

Topics typically found in Counter Fraud and Corruption Training Programs

In sections 1-7 below we have given some examples of topics that would typically be found in a Fraud and Corruption Awareness training program:

Definitions of Fraud and Corruption

It is of the utmost importance to provide a clear definition of fraud and its different forms in the context of the public body to ensure the same baseline knowledge and understanding of all employees. To assist public bodies that may not have explicit meanings for fraud-related terminology adapted to their context, the [IPSEF](#) provides some useful definitions:

- **Bribery:** Persuading someone in a position of trust or power (e.g., a public official) to act in one's favour by a gift of money or other inducement.
- **Collusion:** Secret agreement between parties to conspire to engage in actions aimed to deceive or commit fraud, with the objective of illicit financial gain.
- **Corruption:** Abuse of entrusted power, for personal, private or political gain.
- **Economic Crime:** Crime and financial crime, including money laundering, international counterfeit currency.
- **Fraud:** Making a false representation or failing to disclose relevant information, or abuse of position, in order to achieve a financial gain or misappropriate assets.
- **Fraud Control / Counter Fraud:** Preventing, detecting, disrupting, investigating, reporting and responding to

fraud. It includes managing the risks and reducing harm caused by fraud, corruption and economic crime.

- **Public Bodies / Public Sector:** Government department, agency, arms-length body, or any other entity, including public officials, civil servants, the police, military, public roads and transit authorities, schools and healthcare system, that use public funds to provide public services and programs.

Annex B – Glossary provides more fraud-related definitions.

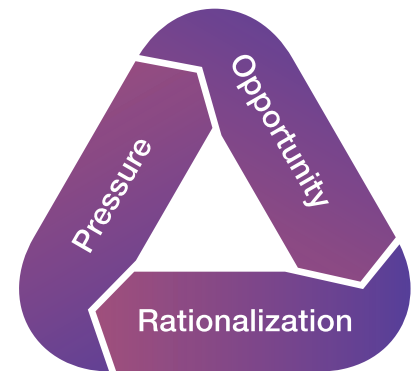
Based on the definitions, consider including exercises or discussion on:

- What is and is not fraud in the context of the public body;
- How fraud links to noncompliance;
- What are acceptable work behaviours and what are not;
- What examples of internal fraud have employees witnessed; and
- What types of internal fraud could happen in the conduct of their duty (provide clear examples).

Fraud Triangle Model

As mentioned earlier, in order to fight fraud effectively, public bodies must first acknowledge that fraud occurs. The Fraud Triangle³⁴ is fundamental to understanding how to identify fraud schemes, explaining how and why fraud occurs, and the factors that, when combined (and sometimes in isolation), can lead to fraudulent behavior:

All three components must be present at the same time for someone to commit fraud.



Pressure(s):



The “need” or “needs” that an individual attempts to satisfy by committing a fraudulent act. Pressure is the first motivation behind a fraudulent act. Examples may vary depending on a public body’s context and include:

- Expensive medical bills;
- Expensive tastes;
- Addiction problems;
- Living beyond one’s means;
- High personal debt or credit;
- Substantial financial losses;
- Undue pressure to succeed;
- Greed; and
- A feeling of entitlement.

Opportunity:



The belief that an act of fraud can be committed and remain undetected. Opportunity is the method for how a fraudulent act takes place. Examples may vary based on a public body’s context and include:

- Using one’s position and/or authority as a means to engage in fraudulent activity;
- Capitalizing on a perceived lack of monitoring/oversight; and
- Using one’s ability to deceive, using minimal effort.

34 Donald R. Cressey (1973), *Other People’s Money*, Montclair: Patterson Smith, p. 30.

Rationalization:



The ability to justify a fraudulent act. Rationalization is the conviction of not being a “criminal”. Evidence tends to demonstrate that the majority of individuals who engage in a fraudulent act are usually first-time offenders. Examples may vary based on a public body’s context and include:

- “I do not care”;
- “I am just borrowing the money”;
- “Everybody does it”;
- “I am not hurting anyone”;
- “It is for a good cause”;
- “It is not really a serious matter”;
- “The organization can afford it”; and
- “I deserve it”.

Different Types of Fraud

Risks and vulnerabilities to different types of fraud and corruption are unique to each organization. Focusing on the ones that are most likely to occur in a specific public body within the context of the counter fraud and corruption training will strengthen a learner’s knowledge of their existence and increase the chances of early detection. It may also facilitate avoidance, if prevented and identified before damage is done to the organization.

One way to identify the types of fraud to which an organization is susceptible to, is to “think like a fraudster”. This facilitates the development of realistic fraud schemes, customized to the organization’s environment that can then be used for the training contents.

Fraud schemes are scenarios centred around specific programs or processes. They underline potential entryways for fraudulent or corrupt acts that consider the actor and the victim. Fraud schemes can be either internal (perpetrated by employees, managers,

officers or stakeholders) or external (perpetrated by citizens, customers, vendors, other parties) that directly impact the organization, or indirectly impact the citizen’s interaction with the public body, and they are not all financial in nature (e.g., organization’s reputation or national security).³⁵

The IPSFF Public Sector Fraud Playbook outlines best practices in fighting fraud by breaking down and defining fraud scenarios based on different types of fraud relevant to public bodies.

35 CFOC (2018), Program Integrity: The Antifraud Playbook.

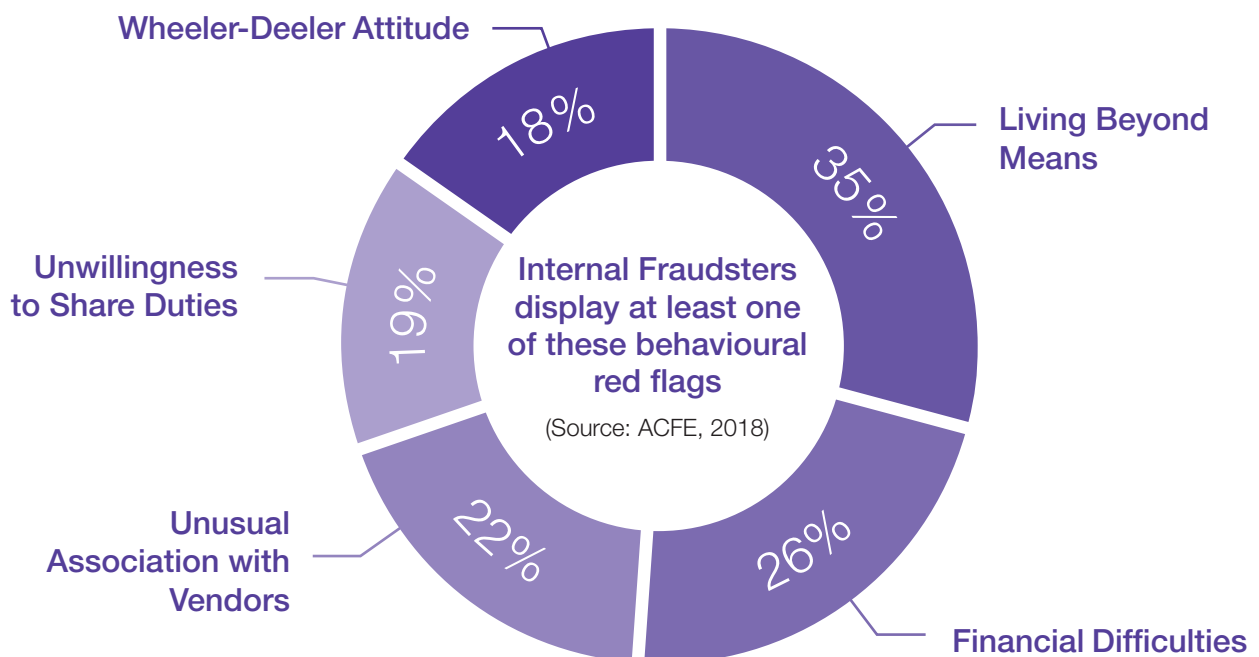
Behavioural Red Flags of Fraud

Identifying the behavioural red flags of fraud, with concrete cases or examples, based on the organization’s context, will bring more clarity and support employees capacity to prevent and identify suspected fraudulent acts.

The IPSFF [Guide to Managing Fraud for Public Bodies](#) presents in **Annex A**: ‘Red Flags in Internal Fraud’ (reproduced below), as well as, ‘Red Flags in Policy Design’ and ‘Red Flags in Contracting/Accounting.’

To add to the IPSFF evergreen list of Red Flags, this Guide includes an explanation of Red Flags in Social Engineering and Red Flags in Grooming to guide public bodies as they determine which ones may be more relevant to their specific context.

- **Red Flags in Internal Fraud:** Internal fraud is committed by employees, managers, officers or stakeholders in the course of their duties or employment. Some of the most common behavioral red flags in internal fraud include, but are not limited to:
 - *Refusal to take leave;*
 - *Refusal to implement internal controls (e.g. skipping approvals);*
 - *Failure to keep records or receipts;*
 - *Seeking access to areas to which an individual does not require access or is not authorized to access; and*
 - *Strong sense of entitlement.*



- **Red Flags in Social Engineering:** Social engineering fraud typically consists of using authority to gain trust and compliance to influence and shock victims suddenly in order to make them disclose sensitive information, pay funds, or grant a fraudster unauthorized access. Offenders usually take on the identity of an organization, then threaten people into submitting to their demands. They use fear as a strong motivating factor.³⁶ Examples of red flags in social engineering include:
 - Using “stressor events”, which play on victims’ emotions to make them act irrationally;
 - Trying to rush the victim by claiming that they are going to be arrested or worse, that need to obey quickly, or by threatening that the deal will be called off if victims don’t act soon;
 - Forcing the victim to send or receive money in an unconventional way (e.g., payment in gift cards or bitcoin); and
 - Fraudsters remaining difficult to contact, unwilling or unable to speak on the phone or meet in person.
- **Red Flags in Grooming:** Grooming consists of isolating another individual, making them dependent, likely to trust, and more vulnerable to abusive behavior.³⁷ Abusers target and manipulate vulnerable people (senior citizens for instance) for exploitation, using a mix of positive and abusing behaviors.³⁸ At first, all behaviors are positive. Subsequently, subtle abusive behaviors are slightly integrated without pushing the alarm to a high level. Overtime, the “wrong” comes to feel “right”.³⁹ Examples of red flags in grooming include:
 - Wanting to see, text or message the victim frequently;
 - Seeming interesting, smart, charismatic, and charming;
 - Seeming to have a good job, a professional project, and a lot of money;
 - Making promises and/or offers in relation to something the victim needs; and
 - Changing the situation suddenly (romantic, economical), and then asking for money

In addition, public bodies may refer to **Annex C – Examples of Misconduct** and/or consult the [Fraudster Personas](#) and the [Red flags of internal fraud](#) webpages from the Australian Commonwealth Fraud Prevention Centre to strengthen their contents on red flags.

36 Hadnagy, Christopher (2011), Social Engineering, the Art of Human Hacking, Wiley Publishing, U.S. Indiana

37 Al-Khateeb Haider, and Gregory Epiphaniou (2016), How technology can mitigate and counteract cyber-stalking and online grooming, Volume 2016, Issue 1, Pages 14-18.

38 Ibid.

39 Molly Dragiewicz, Kelly Richards (2018), Understanding Romance Fraud: Insights From Domestic Violence Research, The British Journal of Criminology, Volume 58, Issue 6, November, Pages 1303–1322.



Fraud and Corruption Controls

Counter fraud and corruption controls are the plan(s) or program(s) in place, which are shaped to protect an organization's integrity and assets. They act as measures to prevent, identify, deter and address fraud and corruption. A counter fraud and corruption awareness training program should draw attention to the controls in place within the organization with the objective of reducing the risk of fraud from occurring.⁴⁰

Experts in counter fraud recommend making the fraud controls, plan or program easily available and readily accessible.⁴¹ A research project currently underway in Canada shows that two opposing approaches currently exist when disclosing fraud controls information.⁴² On the one hand, the findings show that specialists in the field of ethics recommend disclosing (as much as possible) the mechanisms and controls in place during training to deter potential fraudsters from committing violations. Criminologists, on the other hand, suggest only highlighting high level information, without too much detail. The latter has the objective of denying potential fraudsters the necessary information to identify gaps and circumvent the weaknesses, making it harder for them to exploit organizations. In the end, the level of detail divulged when disclosing the counter fraud control measures depends on the mission and the risk tolerance of the organization, as well as the needs and objectives of the training program.

While some public bodies may feel uneasy disclosing that fraud has occurred, communicating fraud incidents can assist in preventing and deterring fraud. A public body should not view the detection of fraud as a sign of failure. Instead, in some cases, detecting fraud should be viewed as evidence of a strong fraud control system.⁴³ In addition to being an effective deterrent to fraud and corruption, communicating and reporting fraud and corruption also allow organizations to:

- Demonstrate the organization's commitment to a culture of integrity;
- Raise awareness of the likelihood of getting caught;
- Stress the consequences of dishonest behaviours;
- Show that disciplinary action is taken against those found guilty;
- Motivate further disclosure of suspected fraud and corruption;
- Preserve public trust that fraud is taken seriously and is being handled accordingly;
- Describe current trends in ethical issues; and
- Inform counter fraud and corruption awareness and training programs.⁴⁴

40 "Six Strategies for Fraud Prevention in Your Business" Cg—A New Jersey Accounting Firm, <https://www.cgteam.com/six-strategies-for-fraud-prevention-in-your-business/>. [Consulted December 17, 2020].

41 "Fraud Control Plan" Australian Government, Attorney-General Department, <https://www.ag.gov.au/Integrity/counter-fraud/better-practice/Pages/fraud-control-plan.aspx>. [Consulted December 17, 2019]

42 ESDC (2019), The State of Knowledge on Organized Crime as Potential Risk for the Public Sector Research Report, [internal document]

43 "Communicating Identified Fraud Incidents" Australian Government, Attorney-General Department, <https://www.ag.gov.au/Integrity/counter-fraud/better-practice/Pages/communicating-identified-fraud-incidents.aspx>. [Consulted December 17, 2019]

44 Ibid.

Annex D – Examples of Fraud Controls

presents some preventive, detective and responsive measures that could potentially be presented in the context of a counter fraud and corruption training program.

The Australian [Commonwealth Fraud Prevention Centre](#) provides guidance on [better practice for fraud control](#) and lists examples of [fraud counter measures](#) to help public bodies to prevent, detect and respond effectively to fraud.

Whistleblower and Anonymous Tip-Offs

Whistleblowing and anonymous tip-offs are preventive measure controls, and it is worth emphasizing their importance in the prevention, identification, deterrence and response to fraud in the training program.

According to the Association of Certified Fraud Examiners (ACFE) 2018 Report to the Nations, tips received from employees are the most common fraud detection controls.⁴⁵ The report highlights that more fraud is exposed by anonymous tips than through any other channels, and that fraud training for employees results in a 41% reduction in median losses from fraud schemes.

Fostering an open and transparent culture of integrity where disclosure of potential fraudulent acts is encouraged, calls not only for a top-down approach, but also for sufficient protection for the whistleblower against potential negative pressures, reprisals

and repercussions from the perpetrator(s).⁴⁶ Providing discreet and confidential ways for employees to report fraud and corruption is essential, as employees are the optimal fraud detectors in an organization.

Consequently, counter fraud and corruption awareness training should address organization-specific fraud concerns and educate employees, as well as third parties, about reporting systems and how to report fraud. Some examples of reporting counter measures include establishing a/an:

- Dedicated anonymous reporting line (ideally toll-free);
- Dedicated page on the organization's website;
- Dedicated page on the organization's intranet;
- Senior Disclosure Official / Ombudsperson; and
- Public Sector Integrity Official.

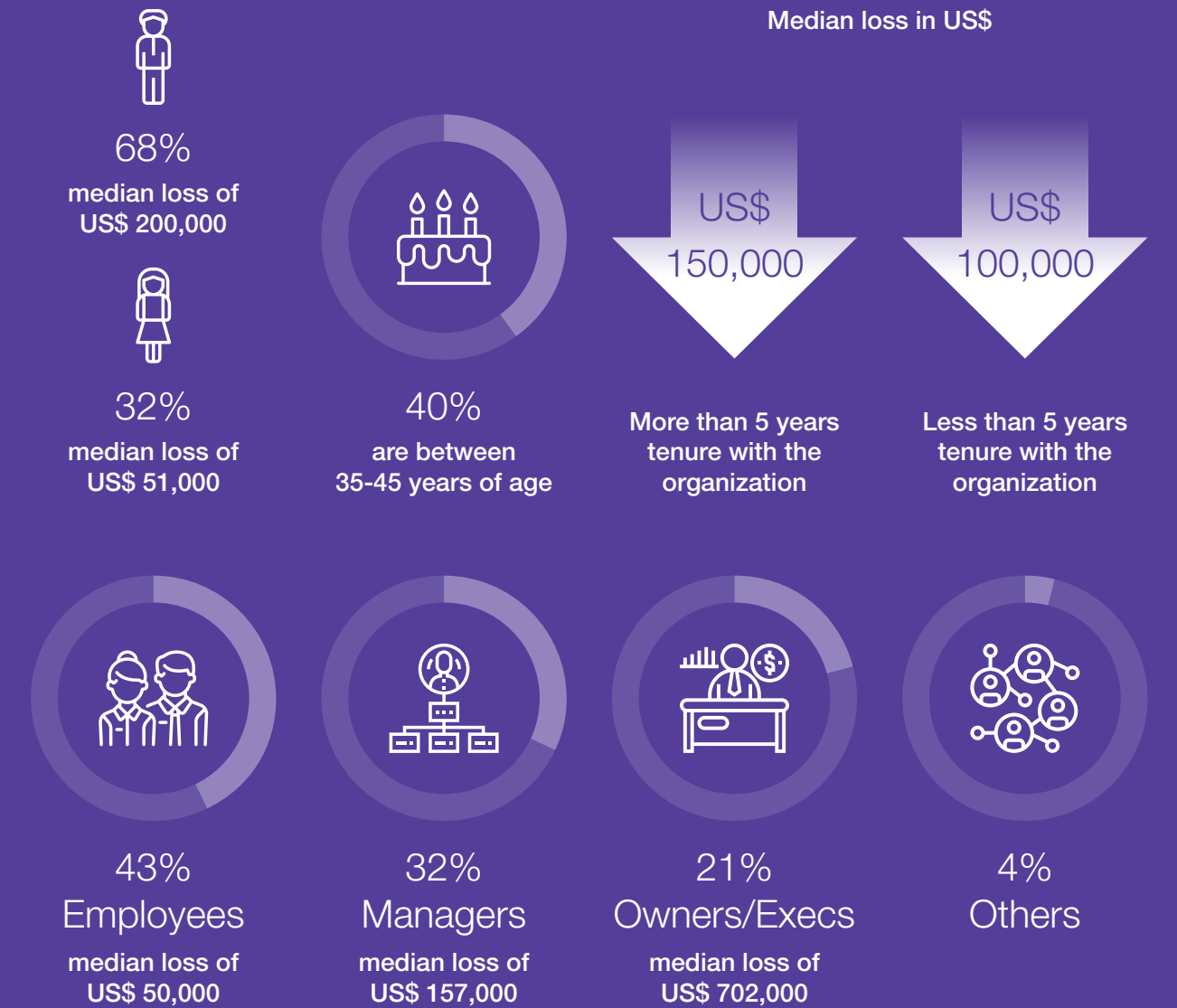
Finally, when addressing whistleblower and tip-offs during training, it is important to stress to learners that employees who witness or suspect fraudulent activities must not engage in or conduct an investigation themselves, and they must make all efforts not to interfere with an investigation.

45 ACFE (2018), Report to the Nations, 2018 Global Study on Occupational Fraud And Abuse - Government Edition, https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rtnn/2018/RTTN-Government-Edition.pdf. [Consulted June 2019]; CFOC (2018), Program Integrity: The Antifraud Playbook.

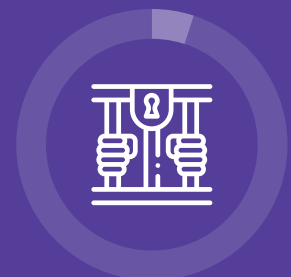
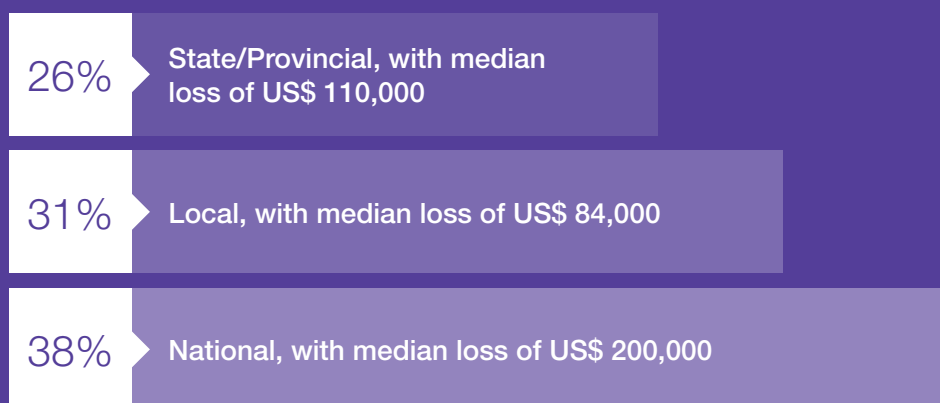
46 Vishal Marria (2018), "How Important are Whistleblowers in detecting crime and fraud?" Forbes <https://www.forbes.com/sites/vishalmarria/2018/11/02/how-important-are-whistleblowers-in-detecting-crime-and-fraud/#1c79f3eb5e09>. [Consulted December 17, 2019]



Perpetrators of Internal Fraud

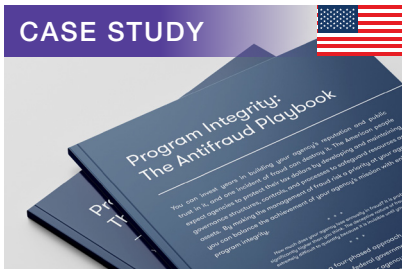


Victims of Internal Fraud



Only 5%
of perpetrators
previously convicted
on fraud-related
charges

CASE STUDY



The United States' Program Integrity: The Antifraud Playbook

In 2018, in the United States (US), the Chief Financial Officers Council and the Department of the Treasury, Bureau of the Fiscal Services introduced the Program Integrity: The Antifraud Playbook, a government-wide approach to fraud risk management. The Playbook provides guidance for public bodies looking to develop counter fraud programs, mature existing counter fraud activities, and prevent fraud, with a main emphasis on fraud risk management. It is framed around successful practices and lessons learned from the federal government and private sector and is in line with relevant guidance in the US Government Accountability Office, legislation and regulations.

What sets the Antifraud Playbook apart is the way it was designed. It is an interactive educational, training and awareness tool, built around 16 “plays” that presents concepts, approaches and strategies to: 1) create a culture; 2) identify and assess fraud risks; 3) prevent and detect fraud; and 4) turn insight into actions.

One of the advantages is that public bodies do not have to implement the Playbook in its entirety or sequentially. The Antifraud Playbook is organized in such a way that each phase builds on the previous one, leading to a robust integrity and counter fraud program. A public body can handpick the information that meets their needs or the maturity level of their counter fraud program. The Antifraud Playbook can therefore be adapted and used differently, depending on the context of a public body.



Impacts of Fraud and Corruption

Fraud and corruption can have serious impacts for government, industries and the public. Public bodies and their leaders should demonstrate their commitment to a counter fraud culture and aim to create and sustain a workforce that upholds the highest standards of integrity. It should be clearly communicated that fraud and corruption are not tolerated within the organization and can give rise to serious consequences.⁴⁷

The following non-exhaustive list highlights some of the consequences of fraud and corruption for countries and the public sector, which may be relevant in the context of a public body. Bear in mind that the mission, priorities and strategic directions, as well as the evolving context of a public body, may require the development of a specific list of impacts, which are more reflective of the public body's environment:

- Decrease a nation's ability to effectively defend its sovereignty and its citizens;
- Loss of revenue and assets;
- Divert money and resources away from the targeted citizens of a public service;
- Increase in expenses, the cost of which is absorbed by the public sector and/or by the community;
- Reduce citizens' level of trust in public bodies; and

- Leave victims with a range of physical, psychological and emotional health problems (e.g., distress, stress, agitation, worry, anger, feeling of violation, anxiety, loss of self-esteem, fear, depression).⁴⁸

The IPSFF Guide to Understanding the Total Impact of Fraud assists public bodies in identifying and measuring the impacts of fraud and/or the cost benefits of counter fraud activity, which can be leveraged to build on the training contents by illustrating the impacts of fraud in the context of a public body.

47 CFOC (2018), Program Integrity: The Antifraud Playbook.

48 IPSFF (2020), Guide to Understanding the Total impact of Fraud; Deloitte (2012), Fraud Risk Management – Providing Insight into Fraud Prevention, Detection and Response, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/Forensic-Proactive-services/in-fa-fm-noexp.pdf>. [Consulted December 17, 2019].

CASE STUDY



Australia's Commonwealth Fraud Prevention Centre

The Commonwealth Fraud Prevention Centre, established as a two-year pilot in July 2019, launched its website in November 2019 to build a strong and proactive national response to countering fraud against Australia. Through collaboration and knowledge sharing with government, non-government and international experts, the Centre aims to provide advice and information on fraud prevention initiatives, as well as legislative and policy changes, to improve and increase the Commonwealth country's counter fraud capability. This includes offering and promoting good practices, tools and resources.

What makes the Commonwealth Fraud Prevention Centre website stand out is the design of its user-friendly architecture, where comprehensive information is written in plain language accessible not only to counter fraud practitioners, but also to a wide range of public officials who may wish to develop or strengthen their knowledge to combat fraud.

Amongst the wealth of information on the site to visit to support the development of pre- and post- counter fraud training aids are: About the Commonwealth Fraud Prevention Centre, Fraud in Australia, and Better Practice for fraud control, which include information on fraud culture, fraud risk assessments, and internal fraud red flags. The Fraud Counter Measures section lists the common types of countermeasures to prevent, detect and respond to fraud, including the dependencies and methods to assess their effectiveness.

The Fraudster Personas section is one of the most interesting parts of the site. The Centre developed personas that include the common, and often coinciding, methods exhibited by fraudsters, as well as the counter measures that could be implemented to minimize their impact. This information could easily be used in conjunction with the red flags of fraud to support the development of training contents or for post training purposes, such as one-pagers, hand-outs or graphics for a public body's internal communications.

Although focused on the legislative and policy framework and the state of fraud in Australia, public bodies around the world can find relevant information and good practices on this well thought-out website, which can be adapted specifically to their context to better fight against fraud.



Evaluating a Counter Fraud and Corruption Awareness Training Program

Evaluation of training is a continuous process that aims to assess the performance and effectiveness of a program and to identify areas for improvements. Repeated monitoring and periodic evaluations are well-known, efficient methods for measuring and sharing insights regarding the effectiveness of a training program and help to identify areas for amelioration.⁴⁹ Evaluating the internal counter fraud and corruption training will:

- Improve the skills of facilitators in their ability to teach and the organization's aptitude for learning in a continuous improvement process;
- Assess impact, effectiveness, results with respect to all employees' level of knowledge, performance and behaviours;
- Identify gaps and opportunities for improvements and/or changes; and
- Improve all aspects of the training program.⁵⁰

The evaluation process should go beyond reviewing outputs and focus on outcomes to be most effective.⁵¹ Instead of focusing on the number of training sessions delivered or the number of employees who attended, public bodies could measure how awareness and understanding of counter fraud and corruption have improved or what changes in behaviour occurred following training. This can be done through targeted cyclical employee surveys following the training.

It is also important to collect and analyze data from other reporting mechanisms within the organization (e.g., hotlines, instances of detected fraud, fraud risk assessment, compliance reviews, data analytics, investigations, etc.). This data enables the monitoring of fraud trends. It also provides another avenue for identifying potential internal control gaps or weaknesses in a counter fraud and corruption program, while improving the training.⁵²

To evaluate a counter fraud and corruption awareness training program effectively, the following activities should be considered:

- Establish the scope and frequency of monitoring and evaluation activities to ensure they are comprehensive and cover the different components of the training program;
- Set appropriate measurement criteria for monitoring and evaluation activities;
- Include a mix of ongoing monitoring and separate evaluations of more targeted areas;
- Assess the results of monitoring and evaluation activities against established measurement criteria;
- Mitigate (remedy) deficiencies identified, based on the results of monitoring and evaluation activities; and
- Communicate the results of monitoring and evaluation activities to relevant stakeholders.⁵³

49 CFOC (2018), Program Integrity: The Antifraud Playbook.

50 Kapur (2018), Designing and Implementation of Training Programs in Organizations.

51 Ibid.

52 CFOC (2018), Program Integrity: The Antifraud Playbook.

53 Ibid.

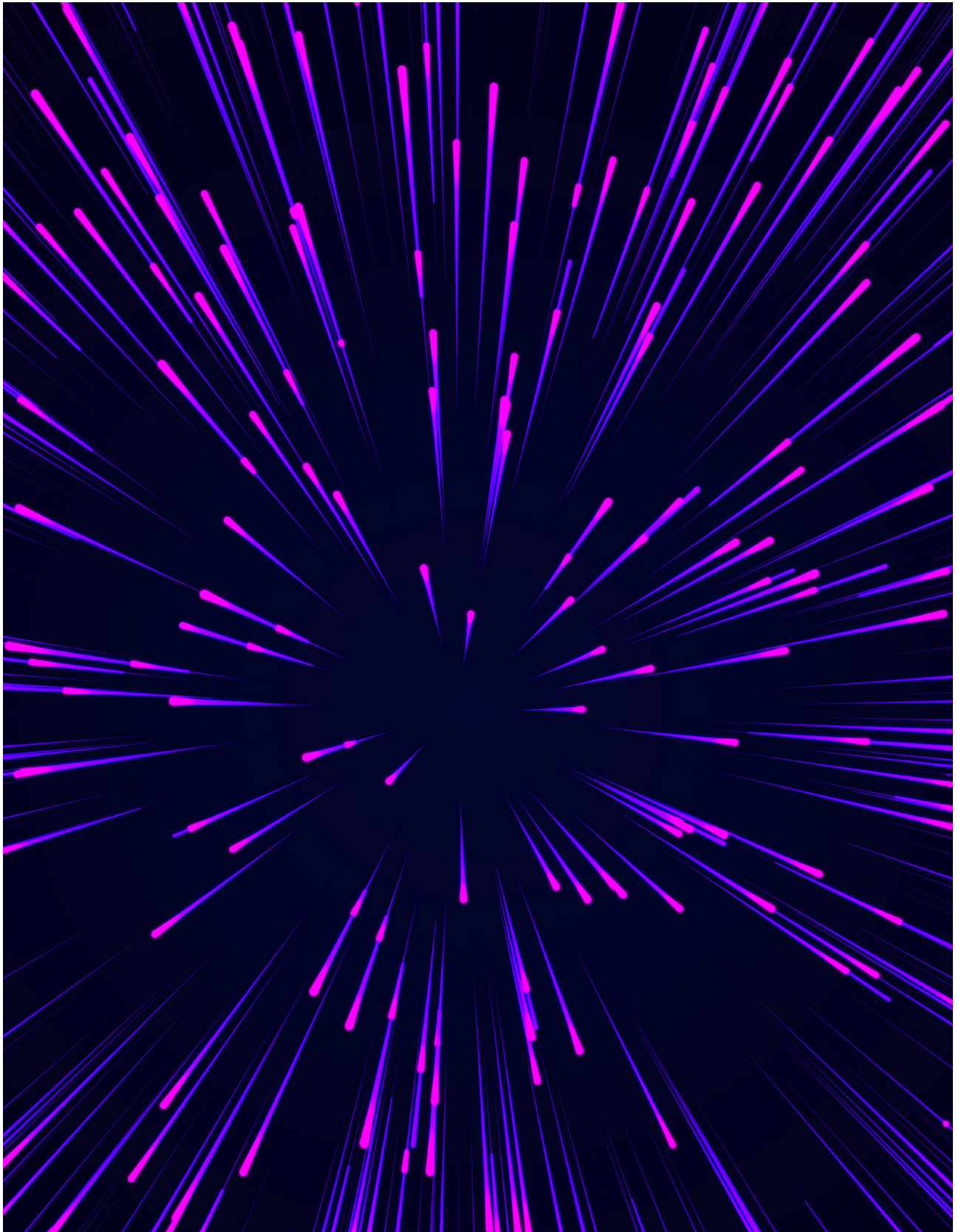
Methods and activities that a public body may consider for assessing its counter fraud and corruption awareness training program include:

- Pre- and post-knowledge tests;
- Post training feedback
- Trainer/facilitator assessment;
- Participant check-in;
- Assessment of completion rates of training;
- Training design review;
- Staff census with questions relating to workplace culture, counter fraud and corruption concepts, principles and behaviours;
- Quantitative and trend analysis of incidences of bullying and harassment, compensation fraud and misconduct; and
- Qualitative review of substantiated fraud and misconduct investigations.⁵⁴

The IPSFF members trust that this Guide to Designing Counter Fraud and Corruption Awareness Training Programs for Public Bodies will support public organizations to strengthen and add value to their respective preventive controls. The hope is that by adapting the various elements presented to their own needs and contexts to design an effective training program, public bodies will strengthen their capacity, as well as that of their employees, to combat incidents of fraud and corruption.

Finally, the IPSFF is considering the development of a more in-depth product focused on the design of an integrated fraud and corruption awareness program, which would focus on the broader scope of such programming to build and expand on this Guide, as a future project.

54 “Positive workplace culture” Australian Government, Attorney-General’s Department, <https://www.ag.gov.au/Integrity/counter-fraud/countermeasures/Pages/positive-workplace-culture.aspx>. [Consulted December 17, 2019]; Mo Hamza—Swedish Civil Contingencies Agency (2012), Developing Training Material Guide.; <https://www.msb.se/siteassets/dokument/publikationer/english-publications/training-material-development-guide.pdf>



Annex A

Annex A – Questions to Ask in the Planning Phase

Identifying the Needs

- ? What is the situation at the origin of the need (context, departmental priority, urgency)?
- ? What impacts do we want to have?
- ? What activities and information must be taken into account?

Program Objectives - What does success look like?

- ? What are the goal(s) we want to achieve?
- ? What is the performance goal?
- ? What is the business goal?
- ? How do you see the employees behaving in the future?

Learning Objectives

- ? What knowledge and skills do employees need to have?
- ? What changes do we want to observe?
- ? In order for employees to perform the way they should, what will they need to learn?

Stakeholders to be Involved

- ? Are there any other resources available to assist during design, development and production?
- ? Are there any subject matter experts available to assist during design/development?
- ? Who will review the training deliverables?

Considerations

- ? Are there any similar training programs within the organization?
- ? Are there similar training programs offered by the Public Sector College (or equivalent), or by other public bodies?
- ? What existing training programs are responding (or not) to these needs?
- ? Are there any deadlines for the design and development of the training program?
- ? Are there any restrictions related to employee availability?

Target Audiences

- ? Who are the audiences (learners)? Establish their profile(s).
- ? How many learners are there?
- ? Are the learners located at more than one site? Where?
- ? Do the audiences have the knowledge base to reach the goal(s) of the training?

Delivery Methodology

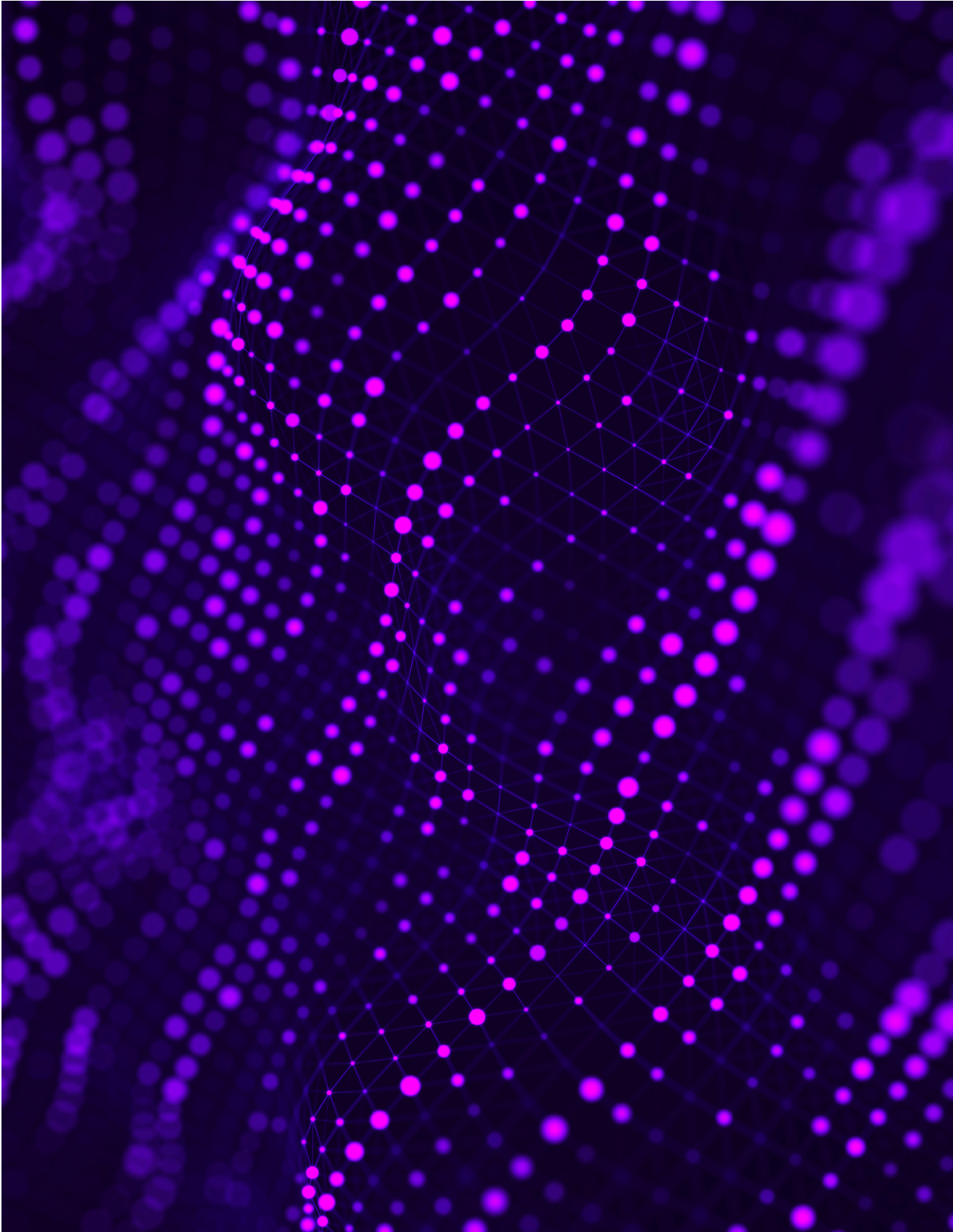
- ? What is the preferred delivery strategy (e-learning, self-directed learning, workplace training, work tools, etc.)?
- ? What is the preferred course length?
- ? What are the constraints?

Indicators

- ? What parameters will need to be used to determine performance?
- ? How will the learning product be evaluated?

Contact Person, Organization

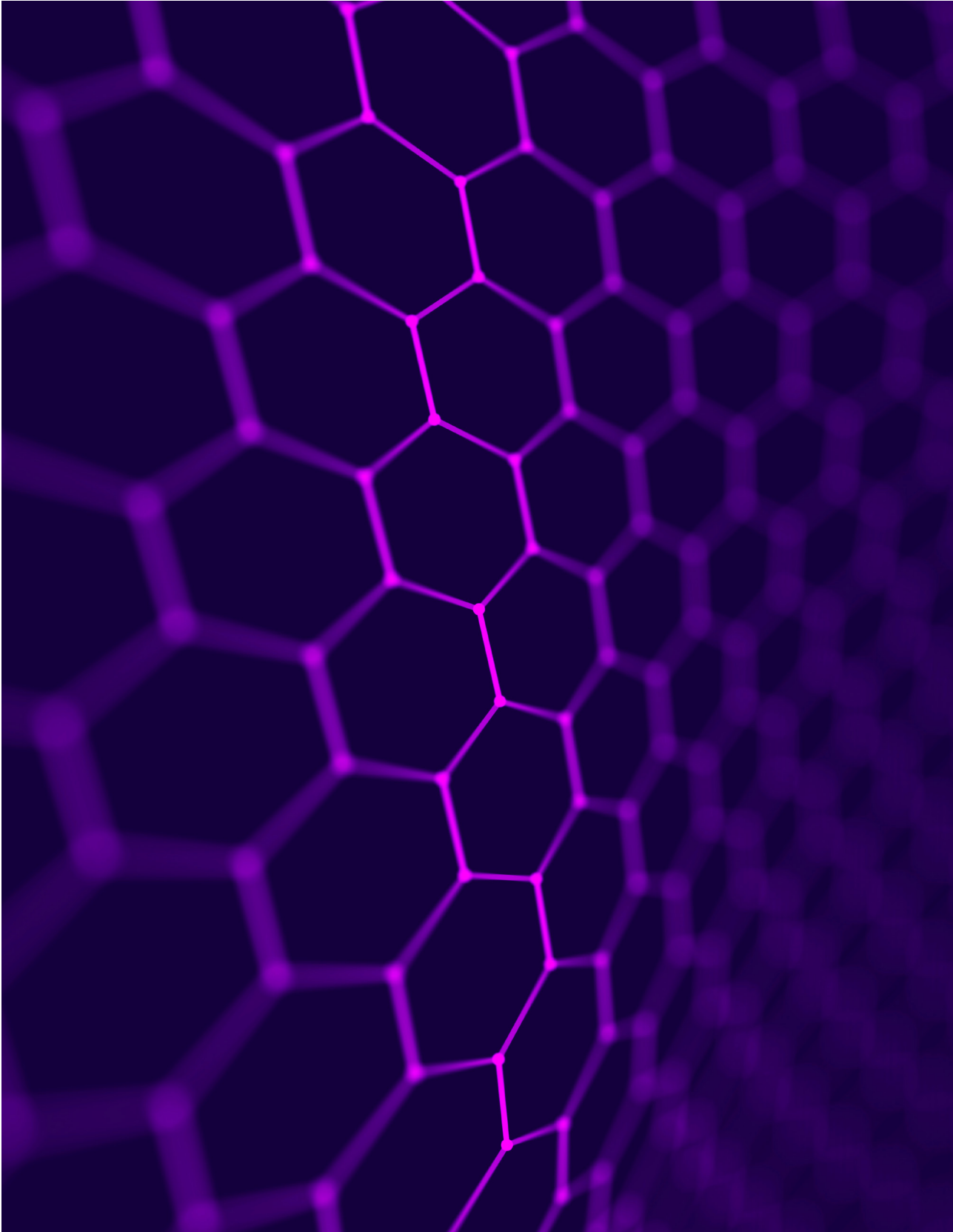
- ? Who is the point of contact for the training?



Annex B

Annex B – Glossary

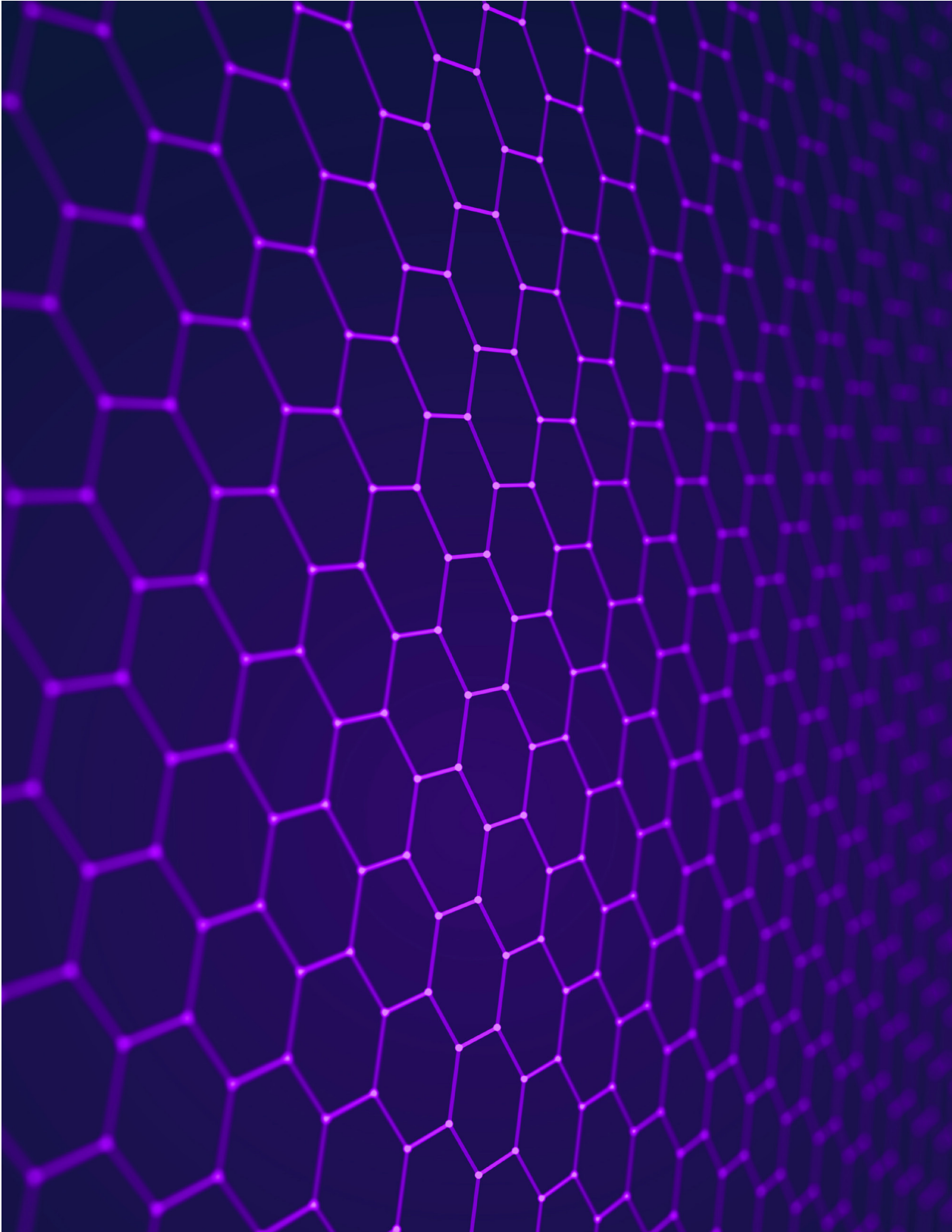
| Term | Definition |
|-----------------------------|---|
| Abuse | Intentional or improper use of public funds, assets and resources. |
| Compliance | Procedures, systems or departments within public bodies that ensure all legal, operational and financial activities are in compliance with current laws, rules, norms, regulations, standards and public expectations. |
| Conflict of Interest | Situation where an individual or the entity for which they work is confronted with choosing between the duties and demands of their position and their own private interests. |
| Disclosure | Provision of information, as required under law or in good faith, regarding the activities of a private individual, public official, company or organization. Information can include a political candidate's assets, a company's financial reports, or a whistleblower's accusations. |
| Ethics | Set of standards for conduct in government, companies and society that guides decisions, choices and actions, based on core values and norms. |
| Integrity | Behaviours and actions consistent with a set of moral or ethical principles and standards, embraced by individuals, as well as institutions, that create a barrier to corruption. |
| Money Laundering | Process of concealing the origin, ownership or destination of illegally or dishonestly obtained money by hiding it within legitimate economic activities to make them appear legal. |
| Oversight | Process of independently monitoring and investigating – internally or externally – the operations and activities of a government agency, company or civil society organization to ensure accountability and efficient use of resources. |
| Transparency | Characteristic of governments, companies, organizations and individuals of demonstrating being open through clear disclosure of information, rules, plans, processes and actions. As a principle, public officials, civil servants, the managers and directors of companies and organizations, and board trustees have a duty to act visibly, predictably and understandably to promote participation and accountability and allow third parties to easily perceive what actions are being performed. |
| Whistleblower | Those who expose information or activities deemed illegal or unethical. |



Annex C

Annex C – Examples of Misconduct

- Unauthorized access, use or modification of information resulting in preferential treatment, disclosure to a third party, or resulting in personal benefit;
- Harassment, including sexual harassment, discrimination and violence in the workplace;
- Theft;
- Provision of misleading information when requesting leave;
- Forgery of medical notes;
- Falsification of travel or other expense claims;
- Fraudulent overtime requests;
- Dishonesty in staffing processes;
- Accepting or solicitation of a bribe;
- Withholding or suppression of a complaint or report against another employee;
- Utilization of another employee's access to retrieve information for personal gain (query non-authorized information-database checks on associates, family members etc.);
- Modification, destruction, or manipulation of information residing on an IT system for illegal purposes; and
- Excessive personal utilization of work computer and other electronic media (e.g., cell phone, tablets, etc.).



Annex D

Annex D – Examples of Fraud Controls

The following provides some examples of preventive, detective and responsive fraud controls that public bodies may consider including and/or discussing in the context of their respective training program:

Preventive Controls

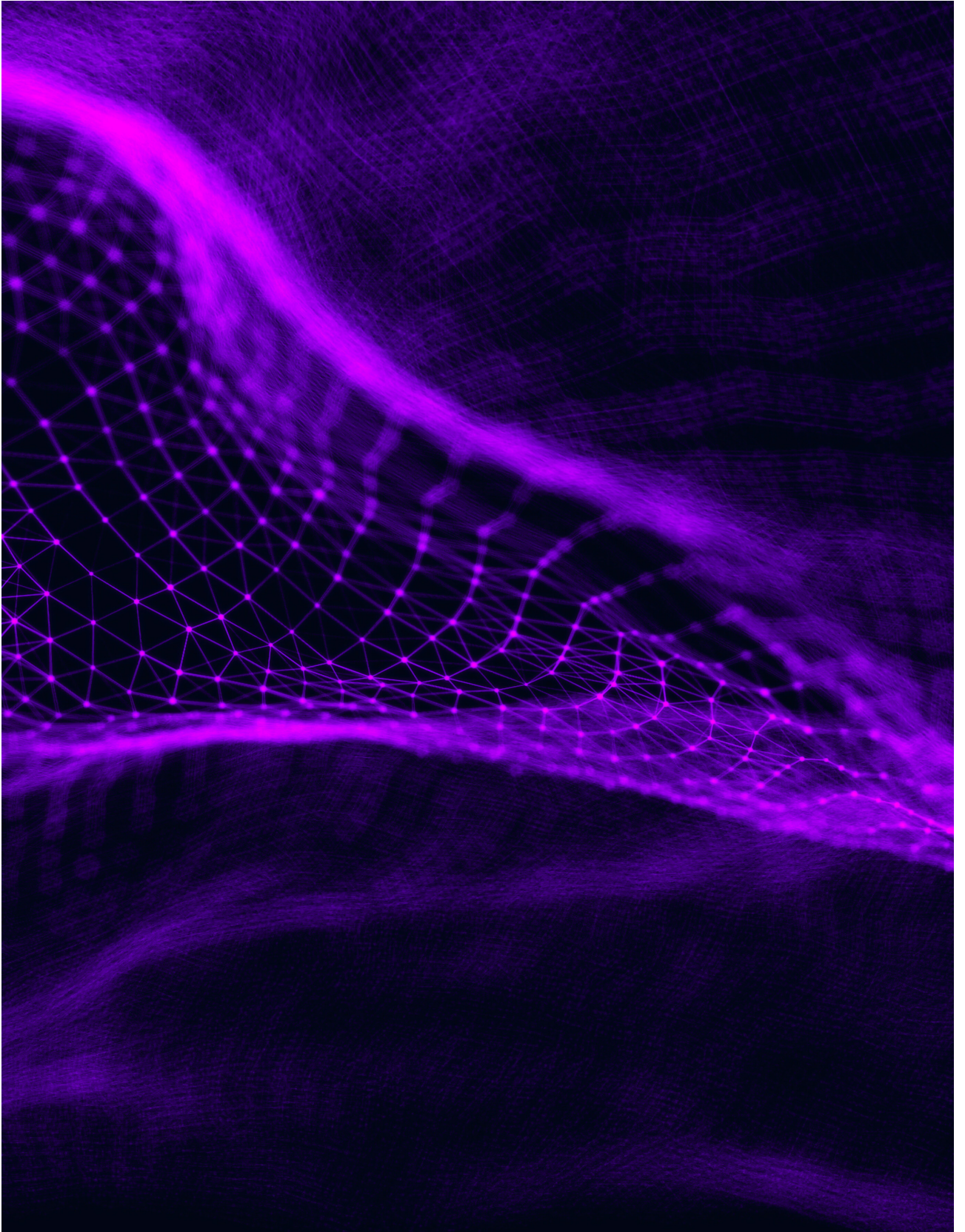
- Counter fraud and corruption training and awareness;
- Code of conduct, legislation and policy;
- Governance, accountability and oversight;
- Segregation of duties applied throughout the organization;
- Self-disclosure and reporting mechanisms;
- Internal escalation procedures;
- Sensitive information controls;
- Proactive data analysis (e.g., advanced analytics, predictive analytics);
- System or physical access controls; and
- Employee and third-party due diligence.

Detective Controls

- Quality assurance checks;
- Automatic notification of high-risk activities and transactions;
- Auditing and monitoring;
- Hotline, whistleblower, anonymous tip-offs;
- Activity, exception and/or incident reporting;
- Retrospective data analysis; and
- Fraud detection program.

Responsive Controls

- Incident response plan;
- Internal investigation, enforcement and accountability protocols;
- Penalties for fraud and noncompliance;
- Recovery and debt management;
- Document and evidence storage; and
- Audit logging.



Annex E

Annex E – Selecting the Training Delivery Methods, Techniques and Developing Exercises

Regardless of the size of an organization, training is more effective when delivered in real-time (i.e., live and in-person) to a small group. However, it may not be possible, if learners are spread-out across different locations or due to the number of learners to train.

In these instances, a combination of approaches might be more appropriate. The method used should:

- Connect the contents with the audiences; and
- Be in accordance with the needs and requirements of both the learners and the organization.⁵⁵

Review the methods and techniques available within the organization and assess which exercises will benefit the learning objectives, while considering the learners' styles and types. To help public bodies, the following provides a range of training delivery methods and techniques that can be adopted, as well as examples of content that can be incorporated for each of them:

- **E-Learning:** One of the most common methods for training employees, e-learning should be a foundational learning piece. It facilitates quick dissemination of information and facts, while providing an opportunity to present the core, proper attitudes and expected behaviours that learners can assimilate at their own pace,

without having to change location. E-learning requires appropriate technology and supporting tools and resources.

E-Learning solutions could be adapted and offered as refreshers or targeted training, as they can be shorter, easier to change (content), allow for just-in-time delivery and are adaptable to the specificity of the audience.

- *E-Learning fits well for targeted training on a specific topic or yearly refresher, following mandatory training;*
- *It may also be worth considering for senior management, middle-managers and supervisors, as specific micro-training.*
- **Lecture:** Lectures present an opportunity to provide verbal explanations and disseminate key counter fraud and corruption concepts, information and facts. This method is effective when facilitating a larger group. Topics could include:
 - *What is internal fraud?*
 - *What is corruption?*
 - *What are the types of internal fraud potentially at higher risk of occurring within the organization (program, service)?*
 - *Why, when, where and how does internal fraud or corruption happen (generally speaking, government-wide, organization-wide, and/or program, service specific)?*

⁵⁵ ACFE (2019), Developing an Integrated Anti-Fraud, Compliance, and Ethics Program; Kapur (2018), Designing and Implementation of Training Programs in Organizations; Rupert Layland (2012) "Behavioural Economics," Training Journal, <https://www.trainingjournal.com/articles/feature/behavioural-economics>. [Consulted June 2019].



- **Discussion:** In order to stimulate and engage learners, the use of discussion is very effective. It may also be used to consolidate other types of learning and as a reinforcement tool following training, such as reminders for managers to encourage dialogue, share experiences, stimulate interests and thoughts, as well as generate solutions. Topics for discussion may include:
 - *Who perpetrates fraud?*
 - *What to do if you witness suspected fraudulent activities?*
 - *How to report fraud?*
 - *How are employees protected in the event they come forward?*
- **Case Study:** Carefully prepared case studies can be an effective way to focus learners on key issues. They can facilitate and enhance engagement and learning by generating solutions, changing attitudes and sharing experiences. Case studies may include those illustrating:
 - *How to identify fraud (common financial, transactional and behavioural red flags);*
 - *How internal fraud is prevented within the organization;*
 - *How internal fraud is detected within the organization;*
 - *How internal fraud is addressed within the organization;*
 - *What the consequences are for fraudulent or corrupt acts.*
- **Group Exercise:** The use of group exercises can facilitate engagement and benefit team building by increasing collaboration, generally resulting in improved productivity. Group exercises may include those which demonstrate:
 - *How fraud and corruption hurt the organization;*
 - *How fraud and corruption hurt employees;*
 - *How fraud and corruption harm citizens;*
 - *How fraud and corruption harm vulnerable people;*
 - *How fraud and corruption harm systems (policing, court and legal aid, welfare, hospitals, public services delivery, etc.);*
 - *How fraud and corruption hurt industries; and*
 - *What could we do, as a team/program, to help reduce these risks and vulnerabilities?*
- **Role-Play:** Including interactive exercises, such as role-play, is an excellent technique to practice the concepts, skills and behaviors, promote learning and retain the materials taught. It makes the training more interesting and memorable. Learners that have practiced counter fraud skills and behaviors in a simulated environment are more likely to use them effectively in their day-to-day work:⁵⁶
 - *Specific examples of past fraud and corruption cases and schemes could be used as a basis for the role-play script.*

- **Brainstorming:** Brainstorming is a recognized method to stimulate creative thinking and may be particularly effective for generating innovative solutions to address specific fraud-related issues. Preparation to steer the discussion and limit the scope of intervention, as well as good facilitator skills, would be required to make the brainstorming exercise effective. It also requires active participation of the attendees. Brainstorming exercises may include questions or topics around:
 - *What are the internal fraud and corruption vulnerabilities (weaknesses or gaps) in your own program?*
 - *What are the internal fraud and corruption risks (potential loss, damage or destruction) in your own program?*
 - *What could be the solutions, controls and mitigation strategies to reduce the vulnerabilities and risks in your own program?*

Train the Trainer

Providing the correct type and level of training to employees is important for a counter fraud and corruption awareness training program’s success. Trainers have an important role to play and success will depend on their skills and aptitude as facilitators. Using a “Train the Trainer” method and employing staff trainers to teach employees is an effective training technique to ensure that facilitators are appropriately prepared to deliver training.

With this approach, it is important to equip facilitators with the knowledge, skills and confidence needed to instruct others by providing them with effective training and preparation prior to launching the training program. Train the trainer gives instructors the opportunity to:

- Receive helpful advice and guidance from experienced counter fraud specialists;
- Develop their own style and improve delivery techniques and communication skills; and
- Understand how to deliver the training in a positive and constructive environment.⁵⁷

Train the trainer exercises generally include:

- Background information, goals and objectives, target audiences of the counter fraud and corruption training program;
- Basis of the curriculum (why the program was developed);
- Directions on how to use the curriculum (e.g., explanation of the contents):
 - *Course planning forms and checklists;*
 - *Materials, equipment, and facility specifications;*
 - *Unit or module overviews with key messages;*
 - *Scope and sequence guidelines, (e.g., sample course outline or agenda with timeframe); and*
- Resources to support the contents (e.g., website, tools and guideline, etc.).⁵⁸

57 Kapur (2018), *Designing and Implementation of Training Programs in Organizations*. Skills Converged (2016), *Train the Trainer, the Art of Training Delivery*. South Carolina: Create space Independent Publishing Platform; Eleanor O’Carroll (2012), *Train the Trainer: Unlock your potential as a professional trainer*. Dublin: Gill Books.

58 Hamza, Mo—Swedish Civil Contingencies Agency (2012), *Developing Training Material Guide* <https://www.msb.se/siteassets/dokument/publikationer/english-publications/training-material-development-guide.pdf>.



Pre- and Post- Training Aids

The development of pre-training aids and supports should be judiciously considered to promote and build awareness around the training program and to prepare employees before learning takes place. They can serve to create positive anticipation around attending the program. Examples of pre-training aids and supports for trainees may include:

- Teasers, invitations and reminders;
- Presentations;
- Structured pre-training assessments;
- Case studies;
- Simulation exercises;
- Hand-outs; and
- Promotional campaigns.⁵⁹

Retention of learning is key for a successful training program. In order to align the learning outcomes with the organization's objectives, incorporating a series of post-training aids and tools stimulates and strengthens the learned concepts and helps to ensure better retention and applicability of the learning.⁶⁰

The level of management closest to the employee usually has the greatest influence on them. Creating discussion points for managers to encourage dialogue in team meetings can provide greater resonance than training alone. By keeping an "if you look after your people, your people will look after your customers" type of approach⁶¹, it gives managers real-world tools to sustain what has been learned.

Some ideas of post-training materials to assist employees include:

- User guides;
- One-pagers on specific topics;
- Checklists and charts;
- Games;
- Intranet pages and hyperlinks to relevant website;
- Posters;TV/computer screens and pop-pop-ups.










59 Uma Pricilda Jaidev & Susan Chirayath (2012) "Pre-Training, During-Training and Post-Training Activities as Predictors of Transfer of Training" IUP Journal of Management Research; Hyderabad Vol. 11, Iss. 4: 54-70.

60 Ibid.

61 Rupert Layland (2012) "Behavioural Economics," Training Journal.

Acknowledgement

International Public Sector Fraud Forum Sub-Working Group Members (in alphabetical order):

| | | |
|-------------------|---|---------------------------------------|
| Lead: |  | Jeremy Sales , Canada |
| Co-Chairs: |  | Patrick Dessureault , Canada |
| |  | Scott Gaines , United States |
| Members: |  | Paul Barton , United Kingdom |
| |  | Lexi Howard , Australia |
| |  | Rob Malcomson , United Kingdom |
| |  | Marie-France Martel , Canada |
| |  | Laura Munsie , Australia |
| |  | Paul O'Neil , New Zealand |

Thank you!

We wish to thank the IPSFF Members who provided comments on the various, evolving iterations of the Guide (in alphabetical order): Johana Ayers, USA; Mark Cheeseman, UK; Laura Eshelby, UK; Jennifer Evans, AUS; Lexi Howard, AUS; Lucinda King, UK; Andrew Lawrence, AUS; Allison Lerner, USA; Rob Malcomson, UK; Christopher McDermott, AUS; Paul O'Neil, NZ; Jennifer Robinson, CAN; Wendy Saschenbrecker-Tang, CAN; Rebecca Shea, USA; and Andrew Walter, AUS.

A special thank you to the Special Contributors (in alphabetical order): Hamid Andishan, CAN; Alan Azar, CAN; Kimberley Batte, CAN; Andrew Lawrence, AUS; and Teresa Martin, CAN.

We also want to express our gratitude to the Canadian Representatives for their on-going support in reviewing and providing feedback on the contents (in alphabetical order): Martin Dufault, Kenneth Ko, [Benoit Labelle](#), Kathrine Leafloor, Aude Lortie, Kathleen Navas, Louis-Philippe Rouillard, William Sanderson, Karen Schwarz, Chris Thomas, Jonathan Wright and David Zorzo.

Writer: Marie-France Martel, CAN

Publisher: International Public Sector Fraud Forum, Cabinet's Office, UK, 2020

