2026 Tackling Fraud in the Public Sector

by Laura Eshelby
Head of Economic Crime,
Clue Software

CLUE

Foreword

Your mission is to find, respond to, and reduce the harm caused by fraud, helping to protect and preserve our vital public services.

As we approach the 2026–27 financial year, it's important to reflect on the current operating environment and the evolving counter-fraud landscape across the public sector. This past year has brought significant change, with a new government embedding its priorities and implementing legislative and structural reforms.

This guide examines the scale of the challenge, emerging threats, and the critical areas of focus for leaders in counter-fraud from 2026 onwards.

Success will depend on common themes: strengthening capability, harnessing technology, and aligning risk management with prioritisation and outcomes.

Inside, you'll find insights into these key areas, along with practical signposts to strategies, tools, and guidance that will support your mission - to detect, respond to, and reduce the harm caused by fraud, safeguarding the integrity of our public services.

Scale of the challenge

£219bn

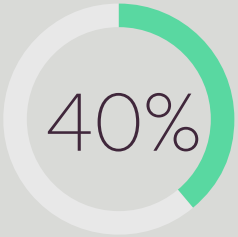
is the estimated cost of fraud UK cross sector

£59bn

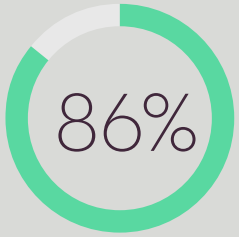
estimated cost of fraud UK public sector

4.1m

instances of fraud reported



of all crime reported

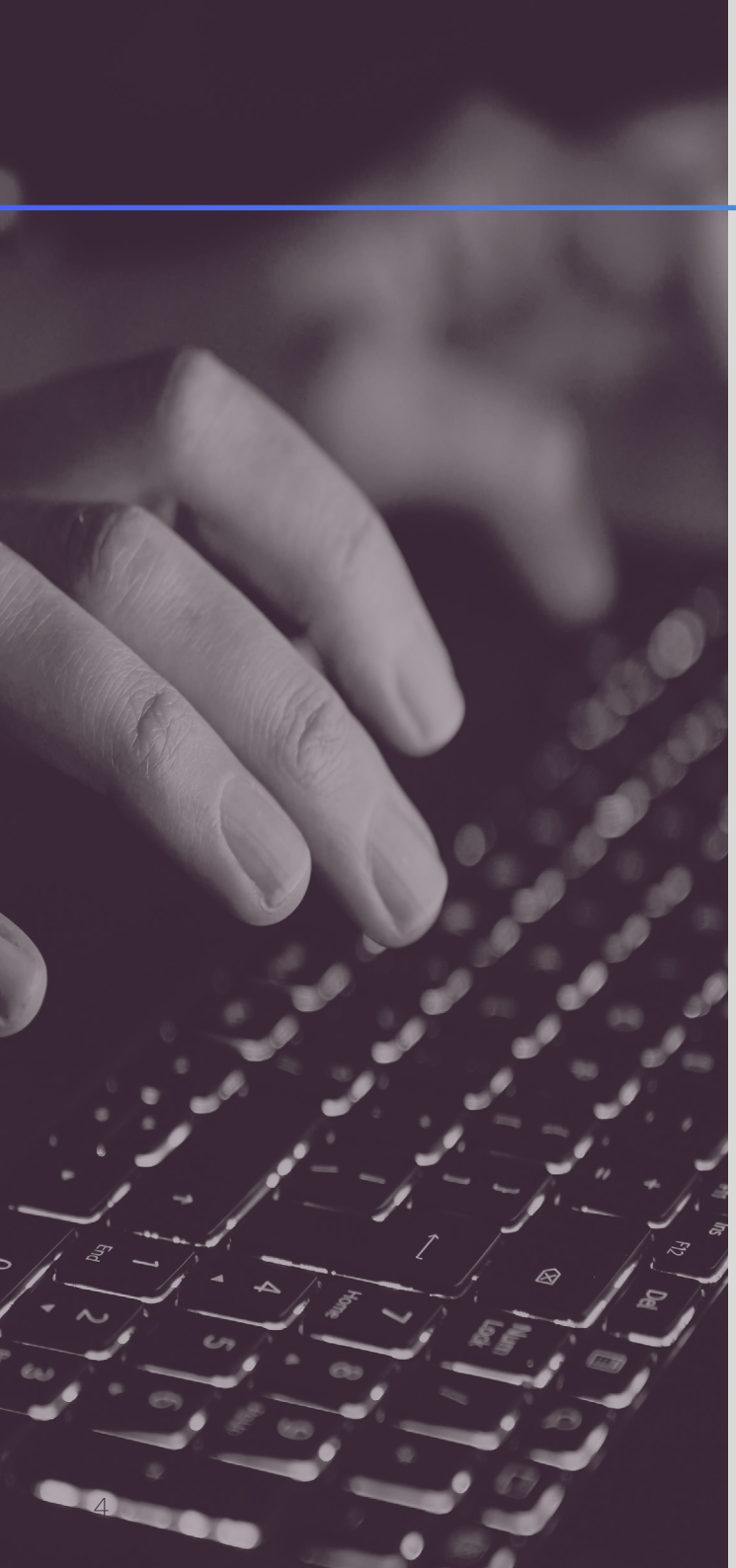


fraud unreported

For those leading counter fraud responses across the public sector, the scale of the challenge remains vast, with fraud now accounting for over 40% of all crime across the UK (ONS). This is likely to be an underestimate, as the NCA has identified that approximately 86% of fraud cases still go unreported across sectors. Several factors may contribute to this; victims may be reluctant to come forward due to fear of personal attack, shame, or reputational damage.

It is critical that organisations make every effort to encourage the reporting of fraud, whether related to insider threats, procurement, or supply chains. A successful approach will combine cultural, contractual, and policy measures, all of which are essential for increasing reporting. This, in turn, enables action to be taken to investigate and recover losses when fraud occurs.

Crucially, it also allows organisations to learn from fraud incidents - informing future business controls, refining processes to prevent further harm, and enhancing overall risk awareness.



Threat landscape

Cyber-enabled

It is estimated that 67% of all fraud committed in the UK is now cyber enabled. These include long-standing frauds, such as mandate, application and phishing (NCA). However, increasingly AI and technology can be used to produce synthetic identities, deepfake images and audio to access government services, benefits, and funding using methods that appear to legitimise applications and bypass biometric controls.

Within the public sector, the increasing reliance on online processes for access to services, customers, and suppliers may leave organisations vulnerable to attack. It's therefore important to understand more about cyber enabled fraud, how perpetrated and controls that can help disrupt it.

Serious and organised

We are seeing an organised element to fraud activity in the UK, with the NCA estimating that 4,500 active organised crime groups are currently operating. This presents an additional challenge for those leading counter fraud operations, as it requires cross-departmental collaboration and close cooperation with law enforcement to mitigate the threat.

A key part of the strategy for tackling organised criminality is the proactive sharing of intelligence, in as close to real-time as possible, enabling those with serious and organised crime capabilities to act, disrupt, and prevent future harm. As we move forward, siloed working has no place in effective counter-fraud management and will only hinder efforts to combat the organised end of fraud threats.

Cross sector

Those operating in the public sector are not alone in the fight against fraud. Unfortunately, all sectors face this challenge, none more so than the financial sector, where both the public and businesses are at risk from a wide range of threats, including identity fraud, romance scams, procurement fraud, and investment-related fraud.

A global survey by SAS estimates that 93% of respondents have been victims of fraud. Fraudsters do not recognise sector boundaries, making it essential to strengthen public-private partnerships and seek new opportunities for collaboration. Initiatives such as intelligence sharing, public private partnerships and technological innovation are key to enhancing both the detection and prevention of fraud, helping to mitigate harm as effectively and early as possible.

Cross border

As we enter the new financial year, we do so in an operating context that is no longer solely domestic. Our fight against fraud increasingly extends into the international sphere, as adversaries operate across multiple jurisdictions, launching remote and large-scale attacks. It is estimated $1 trillion fraud proceeds are laundered globally (GASA).

The City of London Police estimate that 70% of detected fraud originates overseas. This highlights the need to strengthen international and cross-border partnerships with our fraud-fighting counterparts - not only within the public sector but also with industry experts and law enforcement agencies. Active intelligence sharing is essential to ensuring a clear understanding of threats, along with a shared commitment to responding collaboratively when required. By working together on targets of mutual interest, we can maximise the efficiency of collective counter fraud resources on a global scale.

The PSFA has identified five strategic objectives to drive counter-fraud efforts across government and deliver better outcomes:

- Support and develop our people.
- Harness data and technology more effectively.
- Embed prevention.
- Drive a targeted, proportionate response against fraudsters.
- Secure cross-system cultural change.

As you review your current approach - or if you are at the point of developing a new strategy - consider using these five areas as key pillars to anchor your efforts.

Operating landscape for counter fraud

The Public Sector Fraud Authority (PSFA) sets the strategy for the Government Counter Fraud Function (GCFF). This aligns with the UK's overarching Counter Fraud Strategy, set by the Home Office (HO), with key priorities including building capability, fostering innovation, and expanding the use of technology to combat fraud.

This overview of the GCFF strategy is designed to support you as leaders in Counter Fraud as you refine your approach for 2026 and beyond. Anchoring your strategy to this publication will be a crucial step in your planning and strategic reviews as you move into 2026/27.

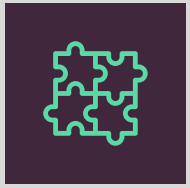
Government Counter Fraud Function strategy

The Government Counter Fraud Function (GCFF) strategy is designed for the whole of government, providing a clear direction for counter-fraud efforts and highlighting how departments can contribute. It also serves as a key resource for those working in fraud, helping to shape priorities and encouraging them to go further.

The GCFF strategy aligns with the key principles of the International Public Sector Fraud Forum (IPSFF) in the fight against fraud:

Fraud will always exist
Some individuals will seek to exploit opportunities for personal gain. Organisations must have robust processes in place to prevent, detect, and respond to fraud and corruption

Finding fraud is a good thing
Fraud cannot be tackled unless it is identified. A shift in perspective is needed so that uncovering fraud is seen as a proactive and positive achievement.



There is no single solution
Combating fraud requires a holistic approach that incorporates detection, prevention, and redress, underpinned by a strong understanding of risk. Collaboration between organisations is essential.

Fraud and corruption are constantly evolving
Both fraud and counter fraud practices change rapidly. Organisations must remain agile and adapt their approach to address emerging threats.

Prevention is the most effective strategy
Preventing fraud through effective counter fraud measures reduces financial loss and reputational damage. It is also far more resource-efficient than relying solely on detection and recovery.

The mission, vision, and statement provide a strong foundation for departmental and local counter-fraud strategies. Taking the mission - "To fight it, you must find it" - as a guiding principle helps set the tone from the top, reinforcing that uncovering fraud is a positive step for many reasons. Investing in robust risk assessment processes enables organisations to identify the highest areas of harm, ensuring that resources and investment are targeted effectively, alongside tactical activity.

Measurement is a key tool in understanding the estimated level of fraud and error in high-risk areas. This is particularly valuable for under-reported areas where little proactive detection work has previously been undertaken.

The PSFA has identified five strategic objectives to drive counter-fraud efforts across government and deliver better outcomes:

- Support and develop our people.
- Harness data and technology more effectively.
- Embed prevention.
- Drive a targeted, proportionate response against fraudsters
- Secure cross-system cultural change.

As you review your current approach - or if you are at the point of developing a new strategy - consider using these five areas as key pillars to anchor your efforts.

Fraud, bribery & corruption

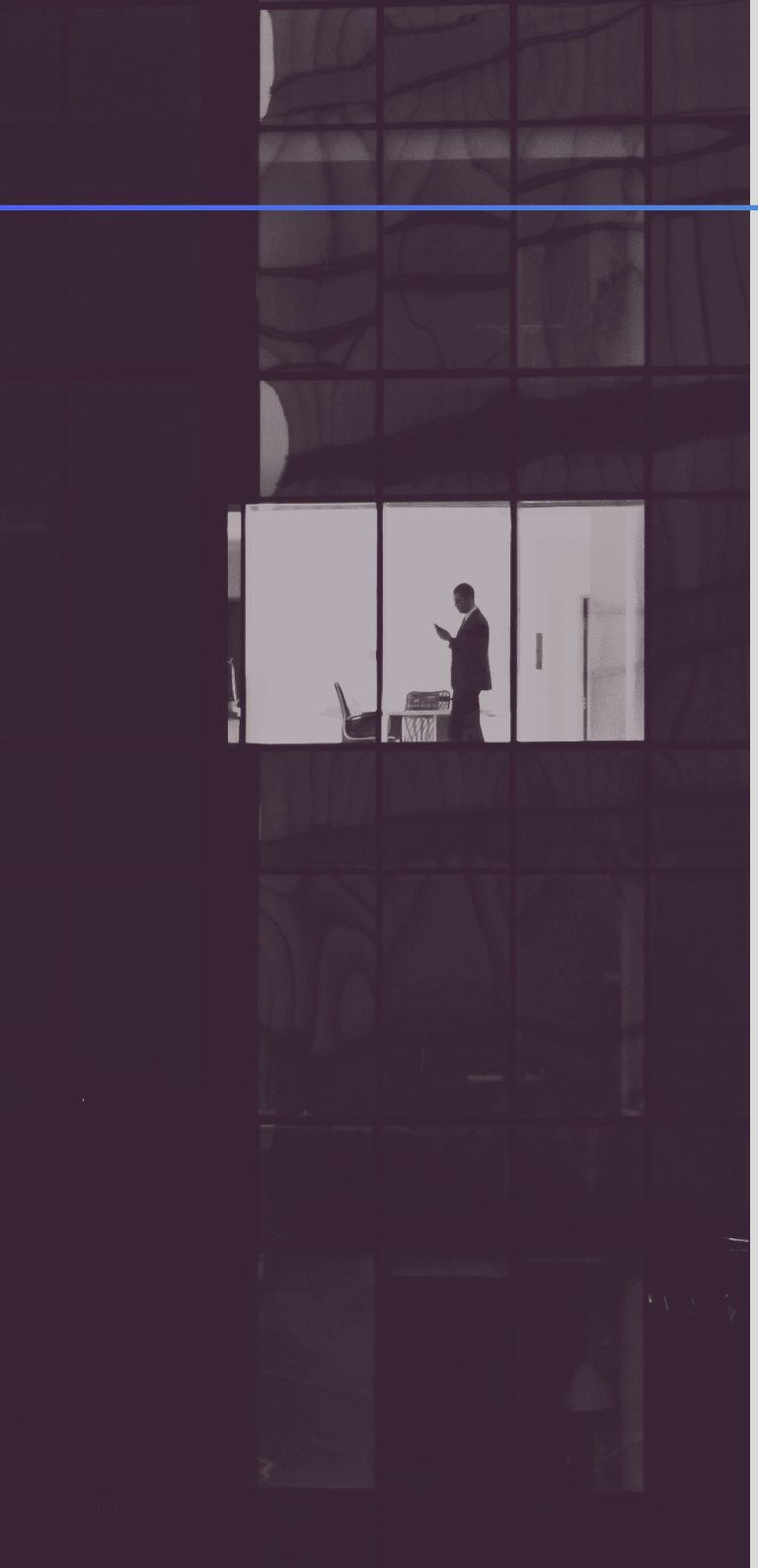
The Function's work covers fraud as well as corruption, bribery, and associated loss from error within and against the public sector. Corruption is often seen as a precursor to bribery and has been defined by HM Government as: "the abuse of entrusted power for private benefit that usually breaches laws, regulations, standards of integrity and/ or standards of professional behaviour."

Build your Counter Fraud capability

Building capability is a key priority, and one that has been growing in maturity since the establishment of a dedicated Counter Fraud Profession in 2018.

The Government Counter Fraud Profession (GCFP) was created to develop a common approach and establish best practice for those working in counter fraud, including within the wider Function. Its goal is to attract, nurture, and retain talent, enhance counter-fraud capabilities, and position counter fraud as a focal point for those entering the public sector.

As well as developing core skills such as investigative, risk, intelligence, leadership - it is also essential to plan activity to build those alongside these in understanding the use of data to detect and respond to threat, and how to harness technology including AI to increase efficiency and prioritise operational activities.



Monitor recovery of loss

Monitoring and recording the recovery of losses caused by harm is crucial. Recovery often experiences delays, sometimes taking years, and the challenge is exacerbated by bad actors operating across jurisdictions and employing digital methods, making asset tracing increasingly difficult. Therefore, it's important to establish a clear cost-benefit strategy for recovery, weighing the costs of pursuit against the potential realisable value.

Your organisation's approach to recovery may involve an in-house unit, a shared service, or outsourcing to a third party. The model selected will depend on the value and complexity of the debt.

Harness data and technology

In recent years, the use of technology has become a cornerstone of any quality counter fraud response, and it is right that it remains a key feature in any strategy moving into 2026/7.

There are several ways to plan and prepare for the use of technology, including AI tools that are becoming more widely available across the public sector:

- **Data audit** - Understanding the scale, types, and quality of data held within your organisation is crucial for the successful implementation of technology and software to support your operational processes.
- **Skills audit** - Conducting a skills audit is essential to ensure you have the right individuals capable of leading and managing the use of data. It also helps to provide quality advice on the right technology at the right time.
- **Business problem analysis** – Taking the time for thorough business problem analysis. This process helps you to fully understand your key issues, pain points, and process bottlenecks related to fighting fraud, enabling you to direct the right tools and techniques at the right areas, and at the right time. It also plays a key role in building a successful business case for investment, should it be required to progress.
- **Regular monitoring** - Developing a regular monitoring process is essential to stress-test the technology deployed, ensuring it is effectively addressing the business and process problems identified. This should be an ongoing process that informs future operational refinements and technological investments.

Any new strategy for Counter Fraud should include a focus on how technology can be harnessed to support efficiency efforts with operational activity and consider strategic alignment to the key principles of the national strategy regarding AI.

Embed prevention

At the heart of fraud prevention is the drive to stop fraud or loss upstream and use the insights gained from detected fraud to inform system changes, preventing ongoing, future, and systemic fraudulent abuse.

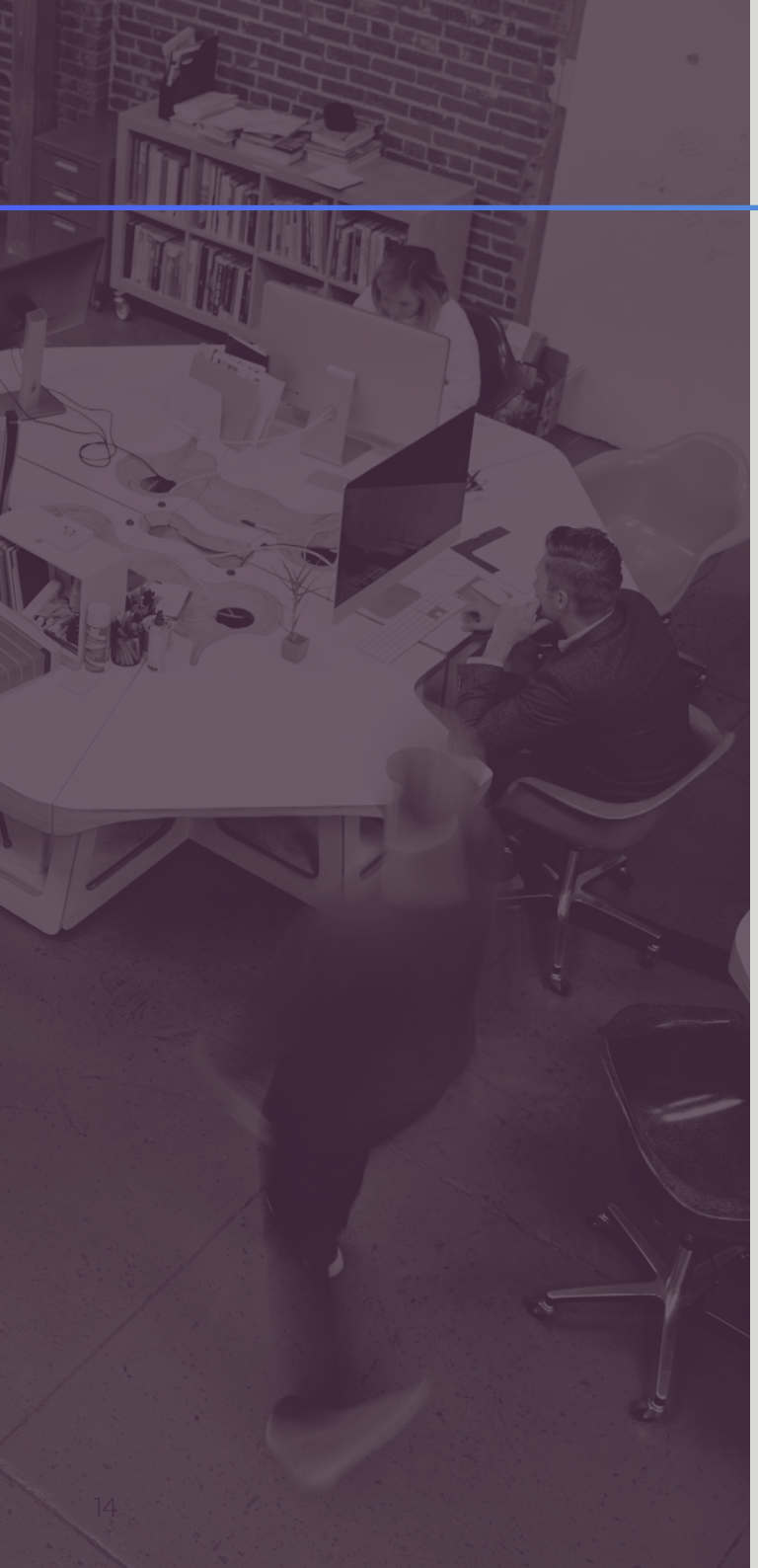
Raising awareness of what fraud is, how it manifests, what to do if it is spotted, and the sanctions that will be applied, are all key activities for leadership within your organisation. Increasing understanding across all stakeholders is therefore key.

Alongside raising awareness, maintaining effective fraud risk management is crucial, and using insights from closed investigations to inform control evaluation and testing. This is strengthened as a process with regular threat analysis and horizon scanning in your organisation and beyond.

Drive a targeted, proportionate response

This element of the Functional strategy serves as a call to arms for stronger collaboration in the collective fight against fraud in the public sector. While there will always be a need for enforcement responses - such as investigation, recovery of losses, and criminal prosecutions - the strategy also advocates for a broader use of the sanctions toolbox. This includes the consideration of civil penalties and potentially joint enforcement actions that may incorporate professional disqualification and/or regulatory sanctions.

This parallel approach to sanctions can help deter fraudsters from future activity and send a clear message to those considering criminality, particularly in relation to spending schemes, policy areas, and professions.



Secure cross-system cultural change

The final aspect of the Functional strategy emphasises the ongoing need to increase recognition and understanding of the value of counter fraud work. This includes both improving the articulation of outcomes and impact upwards, including at Board level, and fostering closer collaboration with non-fraud professionals, such as those in finance, audit, and HR.

Together, these wider stakeholders can help support the aims and objectives of those fighting fraud and amplify the importance of speaking up if fraudulent activity is suspected or spotted.

A good early action in Q1 2026 will be to map your key stakeholders and consider how you can engage them on your strategy and annual action plan, how can they support its success, and how and when will you brief upwards to ensure the impact of your counter fraud efforts are acknowledged.

3 key steps to develop your counter fraud strategy for 2026 onwards:

STEP 1

Preparation

- Use risk insights to inform your strategy - using your fraud/corruption/harm risk register
- Analyse and define the current (tactical) and future (strategic) challenges faced
- Horizon-scan and assess the wider environment you operate in
- Evaluate and prioritise operational, business, financial and strategic challenges and issues
- Define and re-define your existing counter-fraud maturity

STEP 2

Development

- Develop the strategy by defining the scope and time frame
- Consult with stakeholders internally and externally
- Use SWOT analysis to help inform your thinking
- Design optimal future state
- Agree and present key activity
- Analyse resource investments needed
- Develop a responsibilities matrix

STEP 3

Monitor and promote

- Confirm how progress will be monitored
- Obtain sign-off from a board-level leader
- Engage wider business stakeholders and suppliers in developing the bid
- Build a strong narrative based on strategy, risks and opportunities
- Provide clear evidence of the issues, proposed strategy, risks, and opportunities
- Communicate and track delivery through the strategy's lifecycle with an action plan
- Promote the strategy internally and externally

What will 2030 bring?

Since the last iteration of this publication, I have reflected and believe it's still true that the last few years for those operating in the public sector to tackle fraud have been extraordinary. The impact of COVID-19, the resulting economic downturn, a governmental change and various subsequent and ongoing global conflicts have significantly increased the challenges for leaders in this space.

Since 2020, there has been increased scrutiny regarding how fraud activity is being managed, the introduction of targets for public sector organisations and various legislative changes.

The way fraud is tackled is also shifting, with a growing focus on upstream preventative measures, alongside the continued need to maintain the skillset and resources necessary for an effective enforcement response. A new government administration in 2024 accelerated the focus on the use of technology and AI, particularly to increase efficiency in countering fraud.

With this in mind, let's look ahead and consider what operating in the Counter Fraud Function might look like in 2030. Here are some thoughts to consider when revisiting your current or future strategy:

Technology by default

Technology will be a core component of every counter-fraud provision across the public sector, including AI, to enhance operational efficiency. This will cover areas such as intelligence ingestion, evidence analysis, and the use of data collection and evidence for sanctions and disposal.

Capability and development

Capability and development will focus on blended skills beyond just investigation. Counter-fraud practitioners will need skills in risk management, data analytics, and investigative techniques. We will move away from siloed, single-discipline approaches to counter-fraud.

Risk management

Risk management will remain the core focus of successful counter-fraud work, with regular and high-quality risk assessments informing the targeting and resource management of counter-fraud operations.

Recognition of the role of counter fraud professionals

The role of counter-fraud professionals will be increasingly recognised by senior leadership, board-level executives, and other professionals. It will be better understood and celebrated for the significant impact it has on the overall health and protection of vital public services.

Collaboration across departments and beyond

Collaboration between departments, arm's length bodies, and external partners will continue to strengthen, with public-private partnerships providing quick access to innovative tools and techniques that can be deployed rapidly across the public sector.

The scale and threat of fraud are likely to increase rather than decrease in the next five years. Fraud is already being perpetrated across jurisdictional boundaries, at pace, and through cyber-enabled methods.

The time is now to consider how we can work across functions, with our digital, cyber and security colleagues to ensure we are leveraging legislative and policy initiatives to maximise resilience to all threats - not just fraud.

While we do not yet know the methods that will be used to perpetrate fraud in 2030, we can be sure that criminals will seek to exploit emerging technology and target future funding schemes and services. Being proactive in understanding the emerging landscape from 2026 onwards will be key to staying ahead of the threat.

How Clue Software can help

Clue Software works with many stakeholders across sectors and jurisdictions. All of these stakeholders, like us, share a common mission and purpose: to protect society and reduce harm. Our intelligence, investigation and risk management application is supported by AI, and enables professionals like you to:

Strengthen your investigative processes – leading to better detection, mitigation, and prosecution of wrongdoing.

Enhance your understanding of risk – allowing you to link intelligence to identified risks and use learning outcomes from investigations to inform and continually update your fraud risk management cycle.

Clearly articulate success – through tangible metrics, such as case outcomes, disruptions through contract stoppages, financial recoveries, and other efficiency gains.

Justify investment – to internal and external stakeholders, supporting further investment and making the best use of the software capabilities.

Access a powerful community – through our dedicated networking and events platform, Connect, you can talk directly with fellow fraud fighters across the public sector and beyond, as well as have access to regular sector updates, Threat Insight Group, toolkits, podcasts, and webinars.

Working with so many experts in their fields allows us to gain unique insights into how each of them is leading the development of best practices, innovating in the processes and techniques they deploy to detect, prevent, and reduce harm, and how they are all focused on building capability to secure success for years to come.

We have a proven track record of over 40 years in helping leaders manage counter fraud, crime, corruption, and safeguarding activities. If you want direct assistance in shaping your requirements, exploring the art of the possible for your operational activities, and planning effectively for business planning from 2026 onwards, contact me at:
laura.eshelby@cluesoftware.com