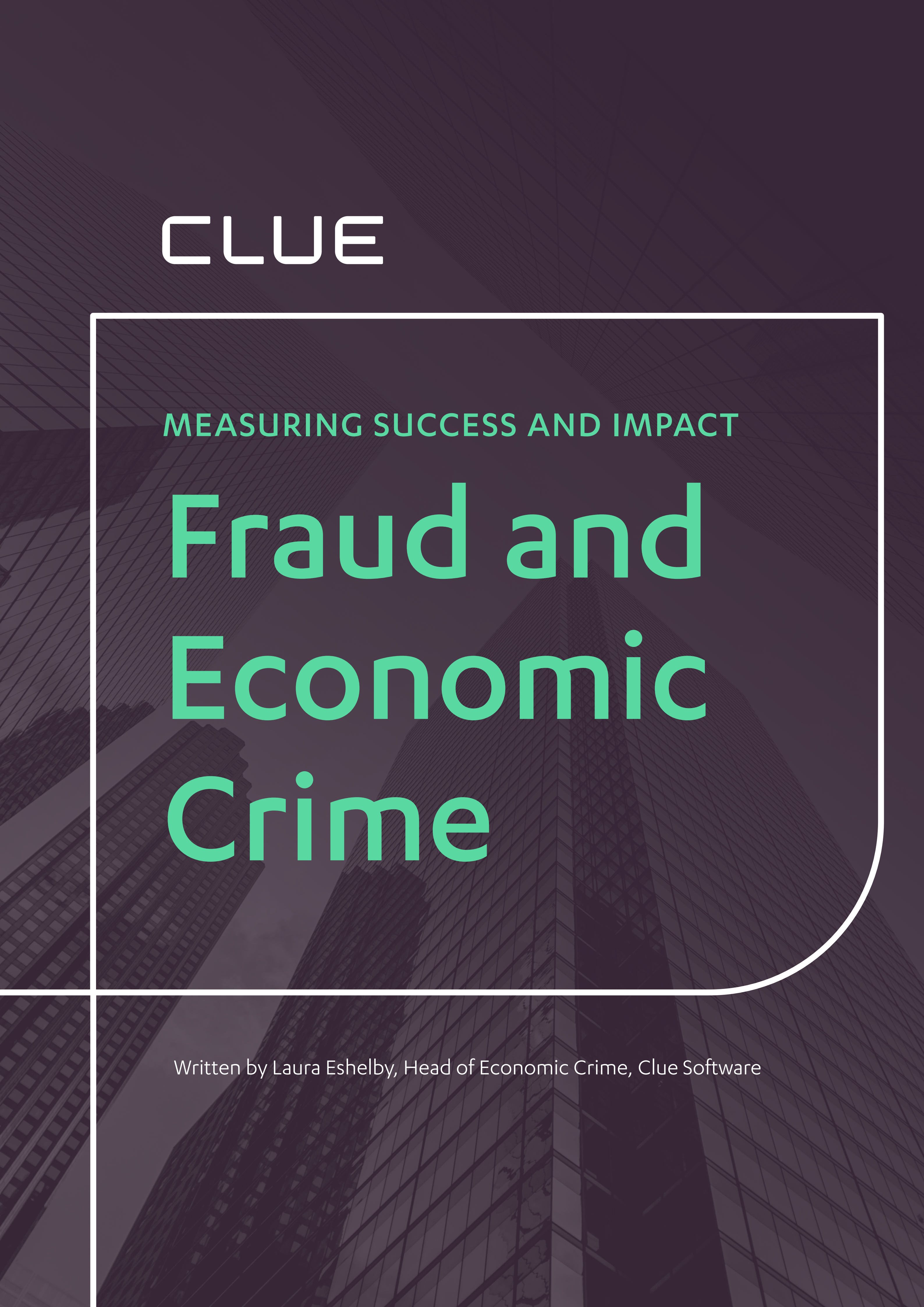


MEASURING SUCCESS AND IMPACT

Fraud and Economic Crime

Written by Laura Eshelby, Head of Economic Crime, Clue Software

Contents

3 Introduction

4 Collective challenges

5 Practical guidance:

- 5 Metrics
- 6 Prevention methodologies
- 7 Deterrence
- 7 Detection
- Recovery

8 Linking intelligence and risk insights

- 9 NHS case study
- 10 MHRA CEU case study

13 Lessons learned reviews

14 Sanctions and penalties

15 Operational efficiency metrics

16 Measuring Success with Clue

18 Conclusions

Introduction

Economic crime, particularly fraud, is the defining crime of our era, impacting all sectors. In the UK, fraud accounts for 39% of all reported crime, with the National Crime Agency estimating that 86% of fraud goes unreported, suggesting we still vastly underestimate its scope.

The challenge is clear: with perceptions of UK corruption rising, demonstrated by a drop in Transparency International's rankings from 8th in 2017 to 18th in 2022, the need for effective tools and resources to combat these crimes has never been greater. However, justifying increased investment in counter-fraud measures can be difficult without solid evidence of outcomes relative to the losses. The Public Sector Fraud Authority estimates annual fraud and error losses of at least £39bn, and UK Finance reports that £570m was lost to payment fraud in just the first half of 2024.

To address these challenges, metrics like Prevention, Detection, and Recovery can help convey the impact of counter-fraud efforts. For example, in the public sector alone, £334m was prevented in fraud-related losses in 2021/22, and in the finance sector, £710m in unauthorised fraud was prevented in 2024.

Beyond financial impact, innovative models, such as those by the UK's Medicines & Healthcare products Regulatory Agency (MHRA) and the NHS, offer frameworks to measure impact on societal, reputational, and human levels. This guide addresses both impact evaluation and operational efficiency, providing sector-agnostic tools and approaches.

Whether you're a practitioner, a leader seeking to demonstrate your team's impact, or aiming to secure further investment, this guide offers insights to support your goals.

Laura Eshelby
Head of Economic Crime,
Clue Software

Collective challenges in demonstrating impact

Given the current operating context in the UK and the scale of economic crime threats, we share a range of collective challenges that, without proactive management, can hinder our ability to clearly demonstrate the impact of our functions and activities.

Outlined below are some key challenges to help set the scene before we consider practical insights, tools, and techniques to address them.

Competing demands

Organisations must often balance competing demands, such as the need to enhance efficiency—producing more, faster, and with fewer resources—while also meeting regulatory, compliance, and functional requirements and maintaining team morale. By leveraging technology, we can achieve efficiency gains, invest in new skills and techniques for team members, and provide enhanced reporting to satisfy stakeholders.
Aligning with high-risk areas

Building on findings from the recent National Audit Office review on government fraud and error, all sectors can benefit from better aligning activities with areas of highest harm or risk. Investing in understanding key risks enables more targeted and effective responses, reducing potential harm. Risk insights can also help inform the business on areas where controls could be strengthened to prevent issues before they arise, reducing the need for resource-intensive investigations and recovery.

In addition, understanding risk helps pinpoint weaknesses in systems that require more resources or investment to improve detection capabilities. Insights from closed investigations are valuable in this part of the counter-fraud journey.

Differentiating stakeholder needs

Reports and insights often need to be tailored to meet the specific needs of stakeholders—whether at the organisational level, where detailed operational efficiency insights may be required, or at the board level, where a broader view is preferred. Boards typically want to see high-level mitigation plans, strengthened controls, and a strategic vision for long-term risk reduction across the organisation.

The board will also want to understand the causal link between activities and their outcomes. To maintain or increase resources, it's crucial to clearly communicate this link to ensure continued support.

Operational management & oversight

Modern fraud and crime management requires insights from individual cases to be applied to overall organisational risk management. However, operational oversight remains essential, with continuous assessment of the quality, speed, and impact of investigative activities. This allows for a clearer view of team effectiveness and helps determine if resource adjustments are necessary based on threat levels.

Technology can support these efforts by providing management information and audit functions, highlighting areas where intervention is needed to enhance processes, such as delays in triage or decision-making. Additionally, tracking operational costs—for example, the cost of responding to certain crime types versus outcomes achieved over time—can support more informed decision-making at the triage and case adoption stages.

Securing staff buy-in for data collection

Gaining and sustaining staff commitment to data entry in case management systems can be challenging, but it's essential for demonstrating impact and tracking decisions, evidence, and steps taken in each case. Showing staff how their input supports future investment, technological enhancements, and improved outcomes can encourage participation. Their contributions also provide valuable threat intelligence, enabling the organisation to better manage risk and achieve its strategic objectives, such as protecting society or ensuring justice. Every pound protected is a pound that goes back into organisational resources and public services.

Current and future measurement capabilities

Measurement capabilities will vary based on organisational maturity and available data. Identifying gaps—such as missing insights on insider threats—can guide the development of intelligence-gathering initiatives. In the absence of comprehensive internal data, industry metrics can serve as a helpful benchmark until a more robust internal evidence base is established.

Practical guidance

Core metrics

Prevention
Preventing harm or loss from occurring, which can include financial loss, now and in the future.

Detection
The identification of harm or loss in your organisation, payment, service or functional area- codified according to legislative, regulatory or compliance need.

Recovery
Recovery of assets, or financial losses that relate to the incident(s) of harm

Prevention methodologies

While investigating harm and recovering losses is essential to demonstrate accountability and deter further incidents, investigations can be costly and time-intensive, particularly with complex cases. It's increasingly important to focus expert resources on the highest-impact cases—those tied to significant harm or loss.

Prevention aims to stop harm from occurring early, at the application or pre-award stage, and it can be applied and measured across a variety of contexts. Below are key benefits, principles, and methodologies for effective prevention, which you can adapt to support your local activities.

Benefits of Prevention

- Harm is prevented in your organisation or society
- Less impact on victims and the public
- Assets and information are secured
- Cost of responding to fraud can be vast
- Building reputation confidence organisationally and sector wide
- Reduce the risk of further and more organised attacks

6 steps to prevent fraud and wider harm

1. **Raise awareness** of fraud and harm types within your organisation, supply chain, and sector.
2. **Increase literacy and education** related to fraud and harm among all stakeholders.
3. **Conduct risk analysis** to understand the threats posed, and communicate findings clearly and regularly across your organisation.
4. **Collaborate with other functions** to test controls and identify system weaknesses.
5. **Utilise data and analytics** to detect various harm types, including third-party data sets.
6. **Implement targeted communication** to inform customers and stakeholders about potential threats and the actions that will be taken if fraud is detected.

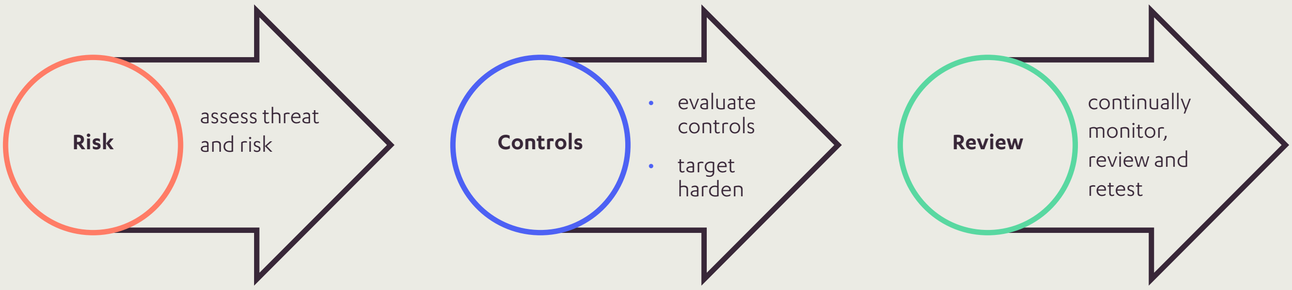


Fig 1- Summary of prevention flow

Prevention methodology

A prevention methodology helps demonstrate the extent of harm prevented before implementing controls or during their design phase. This can involve using either actual or estimated values, depending on the available information and the maturity of the process or programme in question. When actual figures are unavailable, it is often reasonable to rely on proxy values or estimates derived from historical data or broader organisational and sector insights.

Prevention methodologies should be:

- Clearly linked to the intervention or activity
- Evidence-based
- Logical
- Reasonable, Proportionate and
- Data Driven

Prevention can be achieved at different stages of a process lifecycle:

1. At the outset – This occurs pre-application, grant award, payment, or provision of a credit facility. Here, the prevention of loss or value is measured using the actual amount, if known (e.g., if a £1,000 application is stopped, then £1,000 is prevented) or based on estimates (e.g., if the average credit facility offered to new customers is £500, then £500 is prevented).
2. Harm stopped mid-payment/award or contract – When information arises post-payment or award, it can lead to the termination of the account or payment. In this scenario, the total amount may not be declared, but we can increase the actual or estimated remaining value. For example, if a contract valued at £2 million is stopped but £1 million has already been paid out, the value of prevented further harm and loss is £1 million.
3. Harm stopped with no defined period – If information comes to light after payment or award and we cannot determine the specific timescale for which the service or contract would have continued without intervention, we can apply a reasonable and proportionate methodology based on business insights or historical averages. For instance, if I stop a service payment, and payments typically last for an average of three years, it is reasonable to use this as a metric for evaluating the savings.
4. Harm stopped due to ongoing activity – When amendments to controls or behavioural changes lead to prevention, it is essential to establish a baseline before the control change or intervention. We can then measure the percentage reduction in harm identified because of these changes over time.

Deterrence

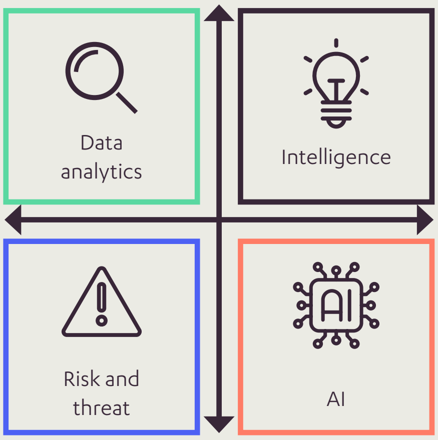
The aim of deterrence controls is to neutralise the criminals' intent. Key controls may include:

- Communicating the consequences of offending
- Providing information on the fraud or other harm response, including detection and monitoring
- Publishing the sanctions and punishment policy
- Highlighting the harm that fraud, crime, and corruption cause to the organisation's mission, such as hindering healthcare provision and impacting vulnerable individuals in society

When considering the impact of deterrence activities, it's essential to tailor your messaging to the audience. For instance, communications will differ when targeting staff compared to suppliers.

Detection

Detection can be approached through core activities tailored to the specific sector you operate in. The key areas of activity are explored below:



- **Data:** Use data analytics, informed by behavioural science, to monitor ongoing activities with the aim of enhancing accuracy and increasing detection rates.
- **Intelligence:** Implement reporting methods such as dedicated hotlines, web forms, and whistleblowing procedures. Some agencies may also utilise human intelligence sources.
- **Risk and Threat Insights:** Regularly assess current and future risks and threats to inform the targeting of thematic reviews and measurement exercises, ultimately enhancing the understanding of the nature and scale of different risks.
- **Use of AI:** Leverage technology to utilise business and risk insights, predicting and highlighting potential patterns or instances of fraud within your systems.

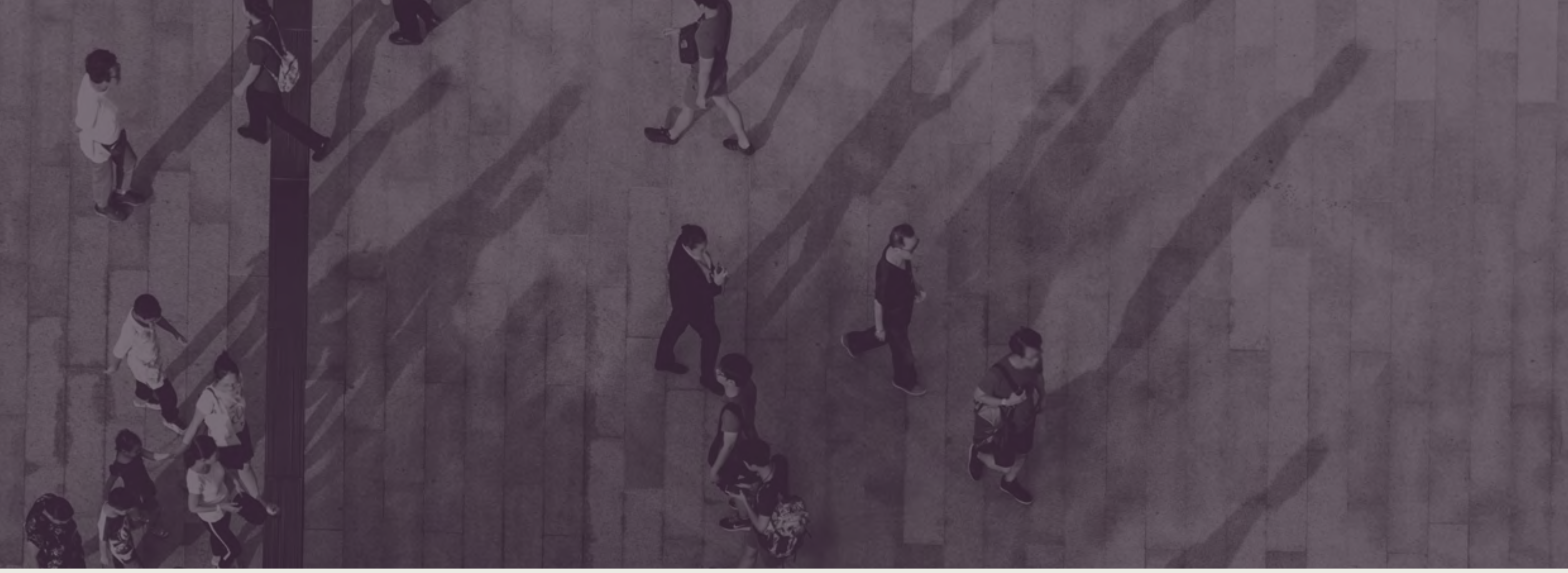
Recovery

Monitoring and recording the recovery of losses caused by fraud, crime, and corruption is crucial. Recovery often experiences delays, sometimes taking years, and the challenge is exacerbated by criminals 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. For example, a different strategy will be required for low-value, high-volume fines compared to complex asset tracing under legislative frameworks like the Proceeds of Crime Act 2002.

Key considerations for recovery action

1. Do we have a recovery strategy and policy in place for civil, regulatory, and criminal recovery activities?
2. Who owns the recovery strategy, and how do we access third-party or external resources when needed for complex asset tracing or court action?
3. Do we have ongoing monitoring of financial recovery in relation to specific cases and activities?
4. Do we have methodologies in place to assess the cost-benefit of taking steps to recover, considering different case types and values?
5. What is the return on investment (ROI) for our unit or activity in relation to assets and funds realised?



Linking investigations to risk insights & strategic intelligence

A Strategic Intelligence Assessment (SIA) provides senior leaders with an overview of the current and long-term issues impacting the fraud landscape. It serves as a foundation for drawing inferences and making recommendations related to measurement, prevention, and future fraud strategy.

An SIA helps define intelligence requirements and supports informed decision-making. It is a living document that should be regularly updated to maintain its relevance. Ongoing information collection and analysis in support of the SIA may include problem profiles, trend analysis, and horizon scanning.

There are six key steps to developing your SIA:

- **Set out clearly information sources used and methods using insights from current/recent intelligence**
- **Produce an overview of current fraud intelligence including sector specific trends and emerging threats**
- **Include analysis of fraud/crime levels based on your intelligence**
- **Include a summary of key recommendations aligned to the issues**
- **Offer prioritisation of the identified issues**
- **Clearly articulate a desired outcome and future state**

Case Study

SIA from the NHS

The SIA provides an estimate of fraud losses and vulnerability across the NHS over the last year. It encompasses intelligence and financial vulnerability estimates based on activity and budget data from the previous year, giving insight into potential threats and vulnerabilities while measuring potential losses due to fraud in the NHS. Additionally, the SIA outlines the current and long-term issues affecting or likely to affect fraud, serving as a basis for drawing inferences and making recommendations regarding prevention, intelligence, enforcement, and future fraud strategy.

Within the SIA, a consistent language has been used to assess probability and uncertainty, with the 'probability yardstick' defining the terminology applied to the range. In using this probability spectrum, the NHSCFA has considered the source, age, and reliability of the information, along with any extenuating factors that contribute to the assessment.

There is no weighting attached to specific factors; instead, a comprehensive approach is taken when assigning probability and uncertainty. The NHSCFA evaluates how financially vulnerable each thematic area is to fraud, bribery, and corruption. To achieve this, the NHSCFA adopts different approaches based on the nuances within each area. The Methods include these areas below , as well as policy, data analytics insights and the use of a baseline vulnerability rate (in the absence of current data a legacy fraud % is applied to calculate this)

Loss measurement exercises

These take the form of an in-depth analysis and measurement of a particular area to provide a statistically robust percentage of how much funding/reimbursement is vulnerable to fraud. This method provides the NHSCFA with the highest confidence.

Comparative loss assessments

Where the NHSCFA has not directly measured, we are reliant on vulnerability percentages derived from partners or stakeholders. These may not be 100% comparable, therefore, the NHSCFA has the least confidence in them.

Case Study

Regulator: MHRA Criminal Enforcement Unit (CEU)

The CEU measures its effectiveness in tackling the illegal trade in medicines through a tailored methodology that assesses the cumulative impact of completed Threat Reduction Interventions (TRIs).

A Threat Reduction Intervention occurs when an identified criminal threat is determined to have been removed or reduced as a result of CEU-led, supported, or coordinated action. Here, a threat is defined as the product of an individual's or group's means, motivation, and opportunity to offend. Each TRI is designed to address one or more of these factors, with the single strategic aim of preventing future offending or reducing its likelihood. This may involve dismantling criminal networks, denying financial incentives, or reducing victim vulnerability.

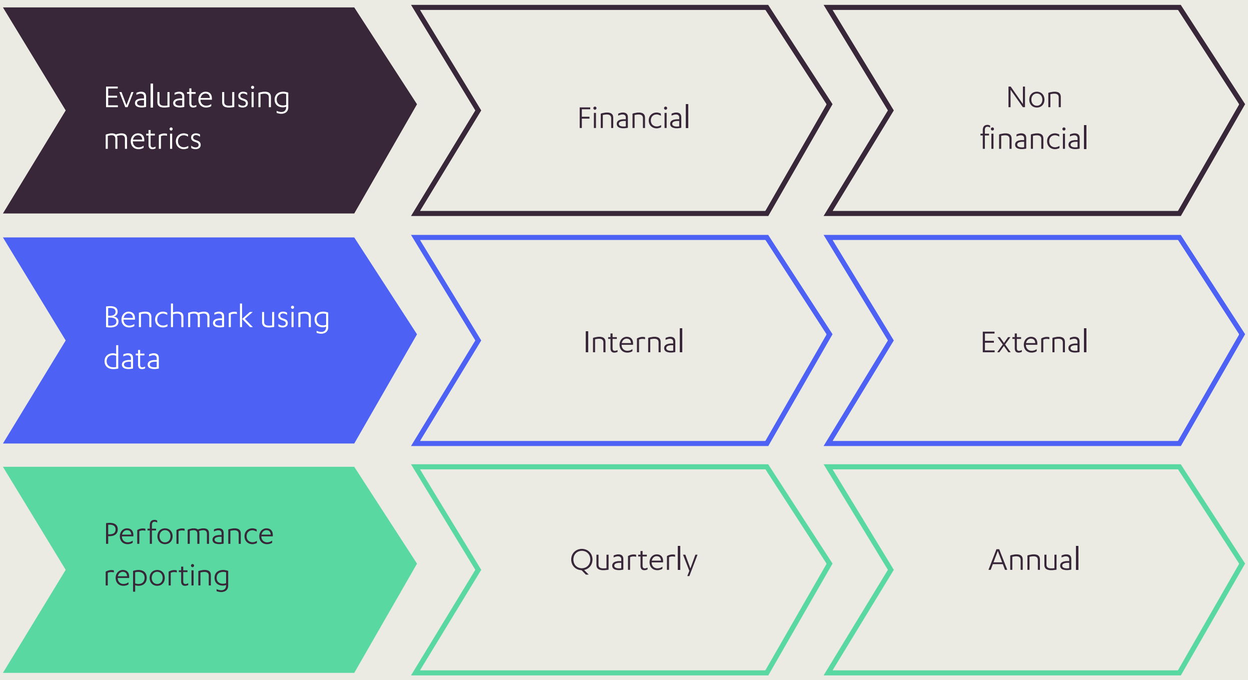
TRIs often involve preventative or disruptive activities rather than focusing solely on criminal justice outcomes. Over time, sustained and innovative TRIs targeting different behavioural drivers can significantly reduce the overall level of criminal threat.

The impact of threat reduction may arise from multiple interconnected TRIs, occurring either concurrently or sequentially. For instance, in a typical operation, the arrest of a suspect, the seizure of illicit goods, the imposition of a custodial sentence, and the confiscation of financial assets are each considered individual TRIs.

The CEU uses professional judgement and intelligence to classify each completed TRI into one of three categories—minor, moderate, or major—based on its positive effect on the threat and the anticipated duration of the impact. To ensure consistency and rigour, these preliminary assessments are reviewed by an independently chaired moderating panel.

Each TRI is then assigned a nominal numerical value linked to its category, producing an aggregate Threat Reduction Score. For clarity and alignment with operational cycles, the CEU reports this score quarterly, using a rolling twelve-month period to present its Threat Reduction Index.

Impact and metrics- including beyond financial



Evaluate using metrics | Financial | Non financial

Benchmark using data | Internal | External

Performance reporting | Quarterly | Annual

Setting metrics to demonstrate and measure success is challenging, whether you are part of a new or more mature function. The first hurdle is reflecting on what constitutes a meaningful measure of success in your specific context and how it aligns with your overall organisational aims.

This may include metrics such as the financial value of losses prevented, the value of detected fraud, and the recovery of funds or assets. When actual figures are available, they should be used; however, if they are not known, estimates of losses with appropriate explanations may be reasonable.

If you operate in a regulatory sector, consider whether your success is defined by both preventative and reactive interventions. Are you monitoring professional sanctions issued, as well as financial metrics to demonstrate value?

More mature organisations may track the cost of the fraud response, including investigative expenses, the use of tools, and third-party services for detecting and recovering losses. This cost may be accounted for and offset against the net recovery value realised.

Benchmarking can also provide valuable insights. How can you learn from other regulatory or membership bodies regarding their approaches to measuring success? In terms of financial outcomes, focus on the recovery of money or assets, as well as funds preserved when considering prevention.

Regarding reporting frequency, organisational performance cycles may dictate this, but best practices typically involve at least quarterly reporting. Year-on-year comparisons can help establish targets to aim for and demonstrate growth over time.

Regarding reporting frequency, organisational performance cycles may dictate this, but best practices typically involve at least quarterly reporting. Year-on-year comparisons can help establish targets to aim for and demonstrate growth over time.

Non-financial metrics

The way an organisation responds to harm—whether related to fraud, corruption, or safeguarding—can significantly impact its market reputation, and for public sector organisations, their global standing. This impact is often evaluated using perception indices or surveys, such as those conducted by Transparency International, which are recognised worldwide.

Reducing threat or harm- This can be achieved by evaluating and modifying controls or systems in response to identified vulnerabilities, as well as assessing the cost savings resulting from these actions.

For example, implementing a system control change, such as enhanced identity verification, can lead to a reduction in specific threat types and associated losses over time.

Reputational – This can be measured using internal or external surveys.

For example, such assessments are particularly useful in areas with less reporting or evidence, such as corruption.

Human impact - Harm often results in a lack of or reduction in services provided to the most vulnerable members of society. Estimating or evaluating the cost of preserved services or protected assets can be powerful, depending on your operating context.

For example, the preservation or recovery of social housing or care services.

Environmental - The measures taken may lead to the protection of our environment, including water, land, and food resources.

For example, preventing illegal water contamination and environmental crime protects the health of local and national communities.

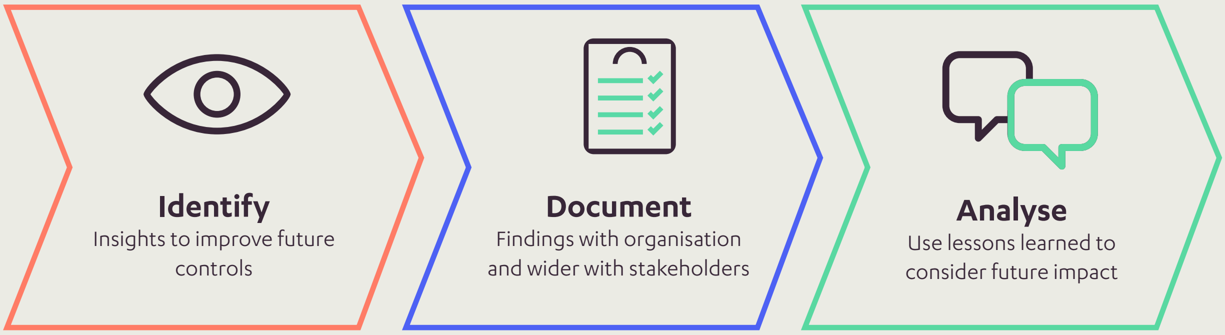
Security – There is a causal link between various types of economic crime. Preventing fraud can help to avert further harm and disrupt more serious organised crime, such as preventing fraudulent gains from being used to fund terrorism.

Lessons learned reviews

Utilising lessons learned is crucial when evaluating prevention or deterrence controls. Insights can be derived from various sources, including:

- Intelligence reports
- Suppliers or third parties
- Audit reports
- Thematic or measurement exercises
- Data analytics
- Investigation reports

The lessons learned process includes the following steps:



Identify
Insights to improve future controls

Document
Findings with organisation and wider with stakeholders

Analyse
Use lessons learned to consider future impact

Sanctions and penalties

It is essential for organisations to have a clear policy outlining how they will address fraud and crime, as this will inform metrics and management information related to their response.
For some organisations, established sanctions and policies will align with sector regulations, particularly for those operating within a regulatory framework. Others may require a tailored strategy that aligns with the available legislative framework and can address a variety of threats and crime types. In certain cases, it may be necessary to seek new powers to impose desired penalties, such as civil fines.

A sanctions and penalties (S&P) policy should include the following features:

- The decision-making process for each penalty, including authority levels.
- The appeal process for each penalty.
- The applicable legislative framework.
- The procedure for referring cases to third parties for further action, including protocols.
- The debt recovery process and other recovery actions.
- Aggravating and mitigating factors to consider.
- Communication methods and frequency of updates.
- A cost-benefit evaluation of taking action.
- A table outlining aggravating and mitigating factors for establishing your S&P policy is provided below:

Aggravating	**Mitigating**
Abuse of power or position of trust	Vulnerability of suspect
Preplanning of offence	Health issues
Organised activity/scale	Disproportionate impact sanction may have in relation to offence
Repeat offending	Voluntary disclosure or early disclosure
Victim impact	Voluntary repair or repayment

Further reading on frameworks and guides for UK:

lawsociety.org.uk/topics/anti-money-laundering/sanctions-guide

cps.gov.uk/legal-guidance/fraud-act-2006

cps.gov.uk/legal-guidance/money-laundering-offences

Operational efficiency (OE) metrics

We have explored various metrics, both financial and non-financial, to capture the impact of fraud and other investigation and intelligence activities. Additionally, we've considered the broader effects of these activities beyond addressing individual incidents, including the relationship between risk and alignment with strategic objectives.

There are fundamental aspects that can be evaluated concurrently to monitor and demonstrate the operational effectiveness of your unit. These factors will vary based on the size, complexity, and maturity of your unit, as well as the requirements of your senior leadership team.

These metrics should be reported quarterly and annually. As your operational effectiveness matures, you may choose to adjust your key performance indicators (KPIs) and metrics over time. Demonstrating growth and improvement is a key aspect of OE metrics.

Example of OE Metrics to Capture:

- Investigation Open Date
- Estimated Value of Loss/Asset at Stake
- Length of Time Investigation Remains Open
- Quality Assurance Reviews and Results
- File Reviews and Actions
- Date Closed
- Referred to Third Party
- Compliance Rates/Information
- Backlog Data (e.g., age of oldest open case, review dates)
- Cost of Each Investigation

Total unit volumes and averages for all metrics can be reported on dashboards, weekly and monthly for team levels, and quarterly for upward reporting. These metrics should be developed on a case-by-case basis, by team member, and then collectively as a unit.

The metrics for investigation should be measured alongside outcomes, including:

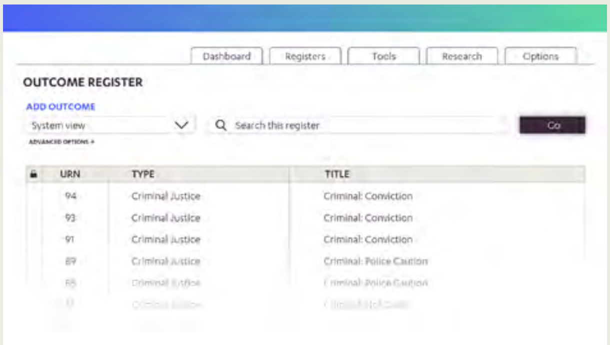
- Civil Outcomes: e.g., penalties, fines, letters before action
- Criminal Outcomes: e.g., prosecution, caution, other sanctions
- Financial Prevention: estimated or actual
- Financial Recovery: actual
- Assets/Money Frozen
- Realisable Assets or Funds
- Professional Strike-Offs/Disqualifications

It's helpful for each case to understand the value of the loss (actual when known) versus the realisable amounts. This can guide the appropriate course of action for recovery or, in some cases, lead to a write-off if the cost of pursuing recovery outweighs the potential impact.

Measuring Success with Clue

In Clue, the Outcome Register enables you to record and analyse the results of investigations, actions taken, and decisions made, helping you measure the impact and success of your investigative or intelligence work.

While all registers in Clue are customisable, the Outcome Register is uniquely designed to define outcomes aligned with your team's or organisation's mission. By linking records from various registers - such as incidents, information, and materials gathered during investigations - to an outcome record, it allows you to demonstrate key achievements such as financial recoveries, civil or criminal sanctions, prosecutions, and other resolutions. This provides valuable insights into the overall effectiveness of your efforts, both current and evolving.



URN	TYPE	TITLE
94	Criminal Justice	Criminal: Conviction
93	Criminal Justice	Criminal: Conviction
91	Criminal Justice	Criminal: Conviction
89	Criminal Justice	Criminal: Police Caution
88	Criminal Justice	Criminal: Police Caution
[illegible]	[illegible]	[illegible]

How does the Outcome Register support measuring success?

The Outcome Register helps you define and track key success metrics in the following ways:

Capturing actions and decisions

- Able to record tasks undertaken to final case outcomes - such as no further action, warnings, guilty findings, fines, or education initiative providing a clear summary of investigative results.
- Monitoring decisions from the decision register at each stage of the investigation to identify patterns between decision making and successful resolutions.

Measuring operational efficiency

- Linking the outcomes to Incident records, task records etc. to track how quickly and effectively cases are resolved.
- Using time-based metrics from customised child lists, such as the duration of investigations or time to first action, to measure efficiency

Evaluating impact

- Capturing and analysing outcomes, including and not exclusive to monies recovered, losses prevented, or fines issued, number of disruptions to help demonstrate value of using the system.
- Tracking outcomes across multiple cases to display cumulative savings and recoveries.

Supporting compliance and accountability

- Maintaining detailed records of outcomes, ensures legislative and regulatory standards compliance.
- Using the Outcome Register to demonstrate accountability by linking decisions from the decisions register. To evidence oversight and checkpoints are being captured with integrity.

Demonstrating continuous improvement

- Aggregating outcome data using views, dashboards, charting to identify trends, such as recurring fraud patterns or other high-risk areas to enable more proactive measures.
- Using analytic tools and reporting capabilities to refine processes, ensuring better results over time.

Facilitating reporting for stakeholders

- Produce reports that clearly demonstrate investigative success to leadership, regulators, or external stakeholders.
- Highlighting metrics such as fine totals, conviction rates, financial recoveries, and overall case resolution rates, in alignment with business objectives.

Seamless interactions with other Registers and reporting

Incident Register: The Outcome records can be easily linked directly to incident records, creating a clear chain of accountability from initial reporting to final resolution.

Information Register: Incoming information from webforms or self-generated can be triaged and assessed ensuring only cases that met a threshold progress to investigation and recording the outcomes for better tracking.

Material and Statement Registers: Correlate decisions and outcomes with the evidence obtained during investigations, ensures transparency and vigour of effort.

Views and Dashboards: Outcomes can be illustrated using the search and querying functionality within Clue and for more analysis external analytics tools can be used.

Complex Reporting: Using Clue's analytics connector to integrate into Power BI/full analytics suite or use the API to integrate with your data warehouse and other tools.

Benefits for your organisation

By balancing the outputs of a combination of registers, your organisation can:

- 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 good use of the software capabilities.
- Strengthen your investigative processes leading to better detection, mitigation, and prosecution of wrongdoing.

Conclusions and the total cost of responding to fraud or harm

The metrics and processes explored above have focused on the loss to the organisation or the value of the harm, but they do not fully account for the total costs involved in identifying and responding to that harm. To provide a more comprehensive insight into the incurred costs, we should also consider:

- Suspending and Replacing Staff or Suppliers
- Using Third-Party Agents to Recover Debts
- Professional Costs/Disbursements (e.g., legal fees)
- System Reviews and Control Changes

These costs are in addition to the less tangible impacts, such as reputation, trust, and market effects in certain industries.
With the various frameworks and evaluation options we have explored, there will be factors that determine what is appropriate for your organisation now and what may be suitable for future use. For instance, if you have a high volume of referrals in a specific area, such as fraud, you may wish to focus on enhancing prevention outcomes rather than solely increasing detection levels. Conversely, if you have very low detection rates in known harm areas (as defined by risk and intelligence assessments), you may want to prioritise activities that drive up detection levels.

There is no one-size-fits-all approach for demonstrating the impact and success of your activities within your organisation. However, this guide may provide insights into the possibilities for tailoring and enhancing your approach as needed.

Further reading and information

Public Sector departmental fraud and error, PSFA, Cabinet Office
assets.publishing.service.gov.uk/media/65f45beeaf6a0d001a90d4fd/Cross-Government_Fraud_Landscape_Report_2021-2022.pdf

National Audit office report on fraud and corruption against government
www.nao.org.uk/reports/tackling-fraud-and-corruption-against-government

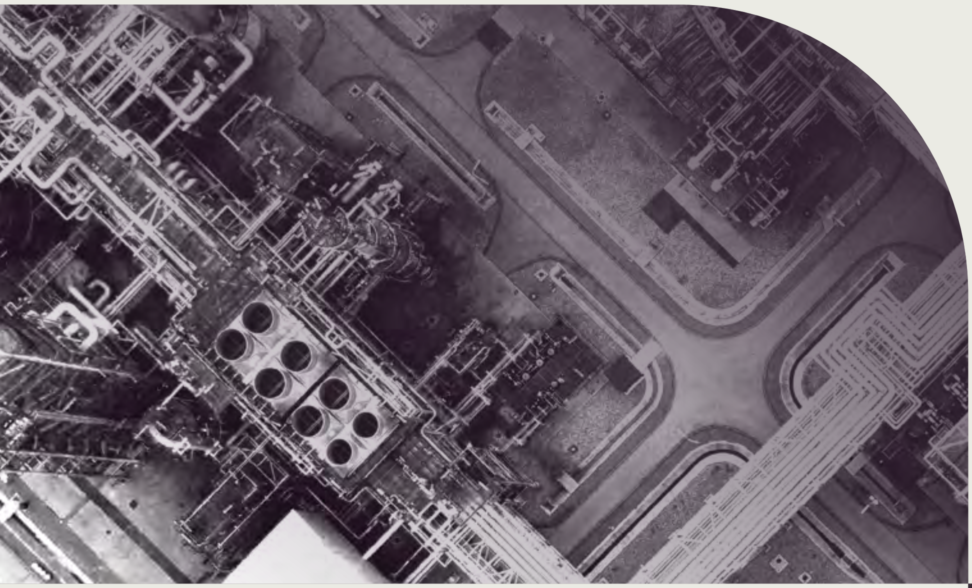
National audit office risk assessment of money laundering/terrorist finance
www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

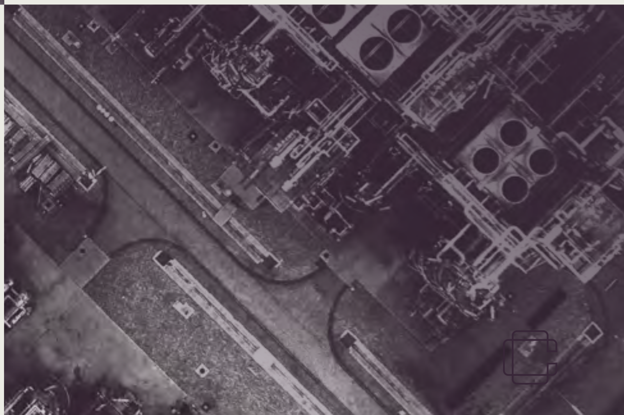
UKF half year report on financial sector and harm including fraud
www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2024

CIFAS fraudscape- industry wide insights on reports of fraud and economic crime
www.fraudscape.co.uk

FCA enforcement data- how the regulator demonstrates impact
www.fca.org.uk/data/fca-enforcement-data-2023-24

NHS SIA 2023
cfa.nhs.uk/about-nhscfa/corporate-publications/SIA-23/SIA-2023





Want to discuss how Clue can better support you in measuring and demonstrating and the impact of your intelligence and investigations?

Contact your customer success manager to get started.

CLUE

Clue House, Petherton Road, Hengrove, Bristol, BS14 9BZ, UK.
Company Number 01715616
Company registered in England & Wales.