ACAMS ENTERPRISE

Best Practice Guide:

Fraud Risk Assessment

Contents

1. Introduction

ACAMS sought to find best practices in conducting fraud risk assessments and held several roundtables and interviews with subject matter experts in banks and non-bank financial institutions.

The industry displays a patchwork approach to fraud risk assessment methodologies. Organizations range from never conducting a fraud risk assessment to treating it as a mere checkbox exercise. More mature organizations have linked fraud risk assessment to their enterprise-wide risk assessment process.

Views among fraud leaders were mixed, with many considering fraud risk assessment an administrative exercise that only told them what they already know. However, pockets of best practices have emerged where organizations, either to mitigate losses or in response to regulatory pressure, have conducted more comprehensive and holistic fraud risk assessments.

In this best practice guide, we examine how to collect data, conduct a fraud risk assessment, and analyze outputs to prioritize key areas of risk for investment. When used effectively, risk assessment can be the biggest and best defense against fraud.

2. The current landscape of fraud risk assessment

2.1 Types of fraud risk assessment and current status

We sought to understand how organizations assess fraud risk for customers and the business. Summarized below are the key processes organizations use to assess fraud risk:

2.1.1. Customer risk assessment (CRA) has an AML focus and is used primarily where there are regulatory requirements to risk assess customers. CRA could assess the risk of the customer committing fraud, such as first-party fraud and application fraud. Often, first-party and application fraud are linked to credit processes. However, organizations can apply the principles for assessing these types of fraud to most financial products.

2.1.2. Product risk assessment involves evaluating the level of risk associated with a financial product, considering factors such as the delivery channel and the jurisdictions involved. For example, cross-border wire transfers are a higher-risk product, as historical data shows us that most fraudulent transactions are cross-border[1]. Fraud leaders referred to agile working practices in change projects, where fraud controls are part of the final set of user stories. If a product or engineering team don't include fraud controls as part of the initial product design but adds them later, there is the danger of additional exposure to fraud.

2.1.3. Enterprise-wide risk assessment is the practice of assessing risks for the organization. It involves identifying various risk types and implementing processes that map risk controls. This is followed by assessing the risk controls for effectiveness and computing residual risks. The organization can then prioritize the residual risks based on how probable and impactful each risk is. This enables the organization to invest adequately and allocate resources appropriately for fraud risk assessment. Regulatory obligations for AML teams to conduct risk assessments vary by jurisdiction.

In this best practice guide, we focus on how to conduct fraud risk assessments considering the risks of external and internal fraud. We seek to prepare organizations for the future fraud landscape by presenting a combination of historical, current, and scenario-based future trends.

1. 2024 Report on Payment Fraud, jointly published by European Banking Authority and European Central Bank. https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud

2.2 Making the business case

The COVID-19 pandemic revealed that bad actors focus their efforts on organizations and institutions that have either direct access to money or products or services with easily transferable monetary value. Financial Institutions, including both banks and non-bank financial institutions, are therefore particularly vulnerable.

However, implementing a comprehensive fraud risk assessment requires careful planning, resources, and management capacity. So, you may have to present a strong business case for undertaking this effort within your organization.

Fraud losses inevitably impact an organization financially but can also have a hugely negative impact in other ways:

- Loss of confidence by shareholders and other stakeholders
- Increased scrutiny by law enforcement and regulatory bodies, with the possibility of fines or criminal action against key individuals
- Internally, loss of trust in the management team, which may increase employee and management turnover
- Other costs, such as legal costs and higher insurance premiums
- Reputational damage in the media and among customers, leading to further loss of confidence, not just in the organization but in the financial system
- Loss of competitive advantage

Reputational damage may be more acute in wholesale banking than in retail banking. This is because any fraud attack on a wholesale bank is likely to be much higher in volume and value than one on a retail bank.

Ultimately, having a solid fraud risk assessment will help an organization to:

- Make effective risk-based decisions for fraud controls, allowing prioritization of effort and resources
- Make an investment case for budget spend
- Provide a stable and comprehensive base that the organization can revisit as new fraud typologies and threats emerge, or products and services change
- Mitigate fraud losses and reduce other associated costs, such as operational, management, and investigatory costs

Establishing a fraud risk assessment is especially urgent because FIs around the world are increasingly reimbursing customers for losses related to authorized push payment (APP) fraud. In the UK, regulations require banks to reimburse for APP fraud losses. Other jurisdictions are considering similar regulations. Many reputable FIs voluntarily reimburse for APP fraud to retain customer trust and loyalty.

According to the FT, a survey of 28,000 people showed that forty percent of fraud victims were fully compensated by their bank in the UK, 32% in the US, and 14% in Japan[2].

Reducing fraud losses and maintaining reputation and customer confidence are the key reasons for needing to conduct a fraud risk assessment. Without a holistic approach, risk mitigation is at best a sporadic endeavor and at worst a waste of effort if the top risks are not addressed.

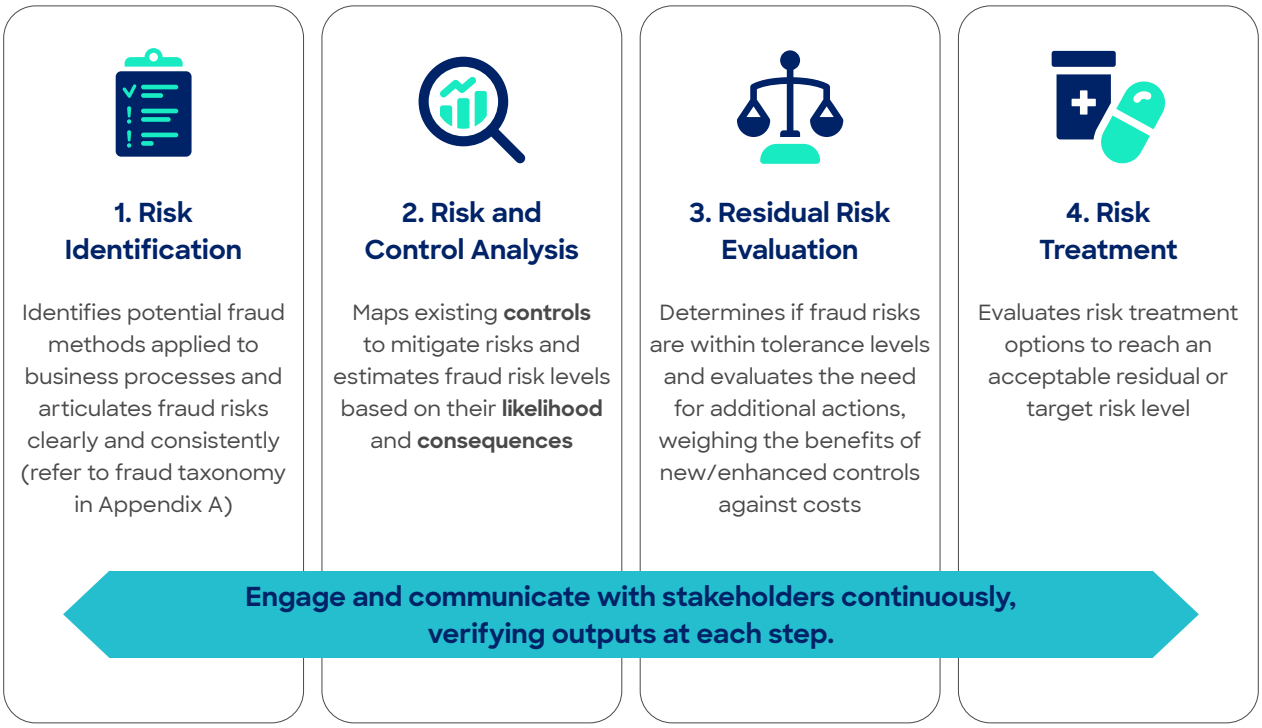
2. UK Banks more likely to pay out fraud compensation than overseas rivals, Financial Times, 28 Sep 2024 https://www.ft.com/content/bbe888ac-8888-40f6-9fb5-d89150025d36

3. A comprehensive methodology

3.1 A step-by-step approach to fraud risk assessment

As the figure below summarizes, a fraud risk assessment can be broken down into four key stages: risk identification, risk and control analysis, residual risk evaluation, and risk treatment.

Figure1: Fraud Risk Assessment - Stages



The table below provides a detailed breakdown of the stages involved in fraud risk management, with steps outlining each stage. Risk identification examines how criminals may exploit business processes, while risk and control analysis assesses the effectiveness of current controls against identified risks. Residual risk evaluation then addresses the risks that remain after applying controls, comparing them to the organization's tolerance levels. Lastly, risk treatment focuses on strategies to reduce residual risks to an acceptable level, promoting a balanced and proactive approach to fraud prevention.

Risk Identification

Step 1: Collate a fraud taxonomy

A fraud taxonomy documents all historical, current, and potential future fraud scenarios that could impact your organization, focusing on relevant fraud risks:

Historical trends: Past fraud your organization has experienced.

Industry trends: Fraud types seen by similar businesses globally that may affect you.

Regional trends: Fraud typologies affecting other sectors in your region, such as money muling targeting students in the UK or scams aimed at blue-collar workers in the United Arab Emirates.

Scenario planning: Potential future frauds, such as artificial intelligence-based impersonation.

A taxonomy provides a shared language for describing and recording fraud.

Appendix A offers a sample taxonomy development.

Step 2: Engage relevant staff through a survey

Engaging all staff involved with fraud and fraud controls in building the risk assessment ensures the best outcome. By starting with a survey or questionnaire, the following best practices are recommended:

- Involve participants early, explaining the purpose and importance to avoid it being seen as a waste of time.
- Keep stakeholders updated on the process and results. Include frontline staff such as call center operators, branch staff, agents, and relationship managers.
- Use open-ended questions to capture insights that might otherwise be missed.

Step 3: Reconcile survey data with known fraud data

Existing fraud data, KPIs, KRIs, and loss metrics captured will need to be merged with survey results. Focus groups and interviews can help reconcile differences in data points and gain a deeper understanding of survey results.

Step 4: Conduct interviews and verify results

A thorough initial assessment provides a solid baseline, allowing future reviews to focus on business changes and emerging fraud threats. The survey can be followed up with activities to identify additional risks and vulnerabilities such as.

- Interviewing senior executives overseeing functions with inherent fraud risks.
- Independently assessing key processes through documentation reviews and interviews.
- Facilitating workshops with business unit staff being assessed.
- Conducting workshops with fraud experts to brainstorm future fraud schemes.
- Reviewing fraud intelligence, past risk assessments, investigations, or case studies from other sectors.

Risk and Control Analysis

Step 1: Use a risk analysis matrix

Fraud risk analysis involves estimating the likelihood and consequence of each risk, using a risk prioritization matrix to rate risks based on these factors (see Appendix B).

- **Likelihood:** Assesses the probability and frequency of fraud, considering factors such as transaction volume, benefits to the bad actor, and past fraud history
- **Consequence:** Evaluates duration (time until fraud is detected) and impact (severity). Consequences can include financial losses, loss of services, customer experience issues, operational strain, reduced employee morale, reputational damage, and harm to victims

A risk prioritization matrix or heat map helps visualize the relationship between risk probability and impact severity.

Step 2: Identify key controls

After identifying and prioritizing risks, controls are mapped and assessed by asking:

- What controls exist for each risk?
- Are they correctly implemented and functioning as intended?
- Are they adequate to mitigate the identified fraud risk?

Step 3: Confirm control effectiveness

The outputs from the discussions with the business owners should:

- Support discussion outputs with audit results
- Use assurance reviews to validate control effectiveness (design effectiveness and operational effectiveness)
- Reference any existing risk and control self-assessments for confirmation

Step 4: Confirm with business owners

At this point it is useful to:

- Review the risk prioritization matrix with business and process owners
- Confirm control evaluations before proceeding to the next stage

Residual Risk Evaluation

Step 1: Evaluate risks against business appetite and tolerance

- Review the organization's risk appetite and tolerance as defined in its risk management policy
- Evaluate fraud risks against these predefined levels
- Consider the business' nature to determine its specific fraud risk tolerance

Step 2: Consider further actions

For risks above the tolerance threshold, consider options such as:

- Avoiding the risk by stopping the risky activity
- Accepting risks within tolerance by maintaining current controls and monitoring
- Analyzing further with an audit or control "pressure test"
- Treating the risk by adding controls to reduce likelihood or impact

Step 3: Balance costs against benefits

Balance the benefits of new controls against their costs and maintenance efforts.

Accept a risk outside tolerance if:

- Benefits of the activity outweigh the risk consequences
- Additional treatment costs or timelines negatively impact essential activities

Also:

- Involve senior business owners to assess fraud countermeasures against risk tolerance
- Use a risk management action table (see Appendix B) to guide actions based on fraud risk levels

Risk Treatment

Step 1: Consider options for treatment

Options include:

- Maintaining existing controls
- Enhancing current controls
- Developing new controls and updating processes (see worked example in Appendix C2)

Controls fall into three categories:

- **Detection:** Identify fraud when it occurs
- **Prevention:** Stop fraud before it happens (for example, cybersecurity protocols blocking unfamiliar logins)
- **Response:** Take action after fraud occurs (for example, blocking future card transactions)

Step 2: Determine likelihood or consequences

- Most controls aim to reduce the likelihood of fraud
- Some controls target reducing consequences of fraud

Example: Lowering ATM daily withdrawal limits can reduce financial losses if a bad actor bypasses preventive controls.

Step 3: Score and prioritize residual risk

- Assess the impact and likelihood of residual risks to calculate remaining fraud risk after controls
- Calculate the residual risk score by multiplying the fraud risk's consequence with its likelihood (see risk prioritization matrix in Appendix B)
- Use the residual risk scores to prioritize risks for further action

Step 4: Obtain buy-in from fraud risk owners

- Build new controls or enhance existing controls as needed
- Secure buy-in from fraud risk and control owners for successful implementation
- Ensure timely implementation and testing of these controls with stakeholder support

3.2 Verifying and presenting the output

With the information from the assessment process, you can now draft your fraud risk assessment report. Here are a few key tips:

- **Verify** the report's content with key stakeholders to ensure no critical risks are missed.

- **Keep** the report concise and simple, using charts and diagrams for clarity and ease of understanding.

- **Include** an executive summary that highlights key findings and proposals without jargon, especially if seeking budget approval from senior management.

Once verified, present the report to relevant governance committees such as the board, risk and audit committees, senior management, other staff, internal audit, and specialists (legal, compliance, human resources) for review and action.

3.3 Action plan and checkpoints

Based on the risk assessment, assign each risk in your action plan a **fraud risk owner** responsible for keeping track of and responding to that particular risk. Record which risk belongs to which owner in a **risk register (see Appendix C1)**.

Fraud control owners are accountable for implementing and maintaining the effectiveness of specific controls.

Clearly outline roles and responsibilities (see Appendix C2).

Good practices for maintaining and managing your action plan include:

- Ensure risk plans are accessible and transparent to all stakeholders, allowing easy access to relevant information.

- Conduct regular review meetings to communicate findings and report on progress.

- Offer ongoing training to keep staff informed about the latest trends and fraud typologies.

4. Improving status quo

Opinions differ on how frequently organizations should conduct a risk assessment of this nature. Ultimately, frequency will depend on the nature and growth trajectory of an organization. A stable and mature organization may choose an annual process with quarterly reviews, but a growing organization may need to repeat risk assessment more regularly.

4.1 Consider where you are on the journey

As your business matures and grows in size and complexity, you may need to adapt your approach to risk assessment, moving to a more real-time understanding of your risk profile. You will also need to refine your approach to identify and focus on priority risks. A real-time dashboard that automatically assesses risks and controls might seem futuristic, but some organizations we have spoken to are close to implementing one.

Most established organizations already have some sort of fraud risk assessment in place. If yours does, you can use this best practice guide to improve how you conduct, implement, and culturally embed your fraud risk assessment across the organization.

4.2 Identifying meaningful improvements

The fraud risk assessment framework provides a way to prioritize key actions. However, conducting such an exercise for the first time may feel overwhelming, especially if the process reveals many high-priority actions. With ruthless prioritization, your organization can achieve meaningful improvements in its fraud risk assessment over time. However, if your organization has significantly under-invested in controls, the only way to catch up would be to invest the organization's time, energy, and resources into combating fraud.

Conducting a holistic exercise may reveal synergies across multiple business and operational units and provide opportunities for rationalization and efficiencies. For example, one organization we spoke to realized that one unit had established processes of multi-factor authentication that other units could replicate. The organization went on to centralize fraud operations, having discovered further synergies through the process of risk assessment.

5. The future of fraud risk assessment

5.1 Live Dashboards

Once in place, a solid risk assessment process will provide a platform for identifying, assessing, evaluating, and mitigating against any new fraud risk, whether triggered by new fraud threats or introducing new products and services.

However, as a business grows it will typically deal with an increased volume of data. Manual risk assessments can be difficult to scale up effectively. Automation tools can improve the risk assessment process and reduce reliance on manual reporting.

One large global bank shared with us that a live dashboard has been built for board committees to review fraud KRIs and KPIs. This dashboard is automated and used by many stakeholders. These KRIs and KPIs can be accompanied by progress updates to provide information on the status of counter-risk initiatives and the changing threat landscape. This will make information more accessible to decision makers, allowing nonspecialists to readily scan crucial data (see an example in Appendix D). A dashboard can summarize the entire risk management landscape, covering:

- Changes in the threat landscape that have implications for the organization

- A summary of recent fraud risk events and what was done about them

- The top fraud risks from the risk assessment process, measured through clearly defined key risk indicators

- A plan of the counter-risk initiatives in place, with relevant accountabilities, implementation status, and actual impact on risk reduction

A well-constructed fraud risk management dashboard reflects the organization's risk appetite and is automatically fed with consistent data as near to real time as possible from across the business. Fact-based prioritization will help focus efforts on fighting those fraud risks that are most serious and likely to occur. Conversely, organizations can loosen or discontinue controls for less threatening, less likely risks to free up resources.

5.2 Breaking up siloes

Fraud risk management can be more effective using a multi-disciplinary team that pools resources from different business areas. Team members typically share business objectives related to specific business or customer outcomes, not necessarily the functional area that matches their expertise.

In the risk context, this might encompass bringing experts from, for example, fraud risk, cyber risk, and money laundering risk areas together to create a holistic approach to risk management. This team could use the same techniques we have discussed to prioritize the overall risks to the business.

6. Conclusion

Fraud risk assessment has traditionally received less attention from enterprise risk assessment largely due to the focus on fraud losses. Unlike the AML sector, which is heavily driven by regulatory compliance, fraud is seen as more closely related to theft and delinquency. However, this perception is changing as jurisdictions such as Australia and the UK adopt different approaches, increasingly prioritizing fraud risk assessments. In the US, regulatory examinations are starting to place more emphasis on fraud risk assessments, indicating a shift in focus within the regulatory landscape.

Regardless of regulatory mandates, fraud risk assessments provide a holistic and structured approach that benefits organizations of all sizes. By systematically identifying, assessing, and mitigating fraud risks, organizations can not only safeguard financial assets but also protect their reputation and maintain stakeholder trust. Integrating fraud risk assessments into an organization's overall risk management framework promotes a proactive approach, addressing potential vulnerabilities before they can be exploited. This approach ensures that fraud risk management aligns with broader enterprise risk management strategies, fostering a culture of risk awareness throughout the organization.

Evolving regulatory interest highlights the importance of fraud risk assessments beyond mere compliance. Organizations that embrace this shift are better positioned to respond to emerging fraud threats, adapt to regulatory changes, and implement more robust risk management practices. Ultimately, a well-executed fraud risk assessment serves as a vital tool in building resilience, allowing organizations to navigate an increasingly complex risk environment with confidence.

7. Appendix A: Fraud taxonomy

Fraud Taxonomy

This fraud taxonomy allows anti-financial crime professionals to classify fraud through four distinct phases of the fraud being committed:

1. WHO initiated the payment?

2. HOW was the fraud executed?

3. WHAT tactic was used?

4. WHERE did the initial compromise or contact take place?

It also allows practitioners to enter a variety of details related to the fraud, its primary typology, the channel through which it was undertaken, and the extent of losses and cases linked to the fraud type.

Please refer to ACAMS Fraud Taxonomy.

8. Appendix B: Risk prioritization matrix

Appendix B1: Risk prioritization matrix

Likelihood	Consequences				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	MEDIUM	HIGH	HIGH	VERY HIGH	VERY HIGH
Likely (4)	MEDIUM	MEDIUM	HIGH	HIGH	VERY HIGH
Possible (3)	LOW	MEDIUM	MEDIUM	HIGH	HIGH
Unlikely (2)	LOW	LOW	MEDIUM	MEDIUM	HIGH
Rare (1)	VERY LOW	LOW	LOW	MEDIUM	MEDIUM

VERY LOW	2
LOW	3-4
MEDIUM	5-6
HIGH	7-8
VERY HIGH	9-10

Appendix B2: Risk matrix key

Risk Level	Level of Action Required
VERY HIGH	The risk is beyond the entity's risk tolerance and appetite. Immediately mitigate or avoid the risk. Provide regular review and reporting of the risk to the senior executive and all relevant stakeholders.
HIGH	Mitigate or avoid the risk, unless the anticipated benefits of the activity outweigh the consequences of the risk. Provide regular review and reporting of the risk to relevant stakeholders and the senior executive at their discretion.
MEDIUM	The risk may be acceptable. Provide regular review and reporting of the risk within the relevant business unit and to affected stakeholders.
LOW	The risk is generally acceptable but must be monitored to make sure that the risk rating does not change.
VERY LOW	The risk is acceptable.

9. Appendix C: Sample Fraud risk register

Appendix C1: Sample Fraud risk register

		Risk Identification			Control Effectiveness								Risk Identification			
		Risk Type	Risk Description	Existing Risk Level (Refer to Risk Prioritization Matrix)	Control Measures	Type of Controls	Controls	Controls Implemented	# Fraud Cases Prevented	Amount of Fraud Loss (After Control Measures)	# of Fraud Cases not Prevented	Result	Risk Owner	Control Owner	Risk Review	Additional Information
		Internal/ External	Provide a description of risk and why it is considered	Very High/ High/ Medium/ Low/Very Low	Yes/No	Prevention/ Detection/ Response	Mitigating controls to reduce the risk	Yes/No	Provide the number of fraud cases prevented based on the controls	$	Provide the number of fraud cases that were not caught by the control	(Eliminate/ Reduce/ Accept)	Title and Department	Title and Department	Weekly/ Monthly/ Annually	
First-Party Fraud	Credit-Related Fraud															
	Goods Lost in Transit															
	Application Fraud															
	Fake Documentation															
	Application Fraud															
	Synthetic Identity															
	[Add other fraud typologies related to your organization's operations.]															
Second-Party Fraud	Money Muling															
	Chargeback Fraud															
	Gift Card Laundering															
	Fake Merchant Fraud															
	[Add other fraud typologies related to your organization's operations.]															
Third-Party Fraud	Account Takeover															
	Identity Theft															
	Authorized Push Payments resulting From Scams															
	Business Email Compromise/Phishing															
	[Add other fraud typologies related to your organization's operations.]															

The Table in Appendix C1 is a sample risk register, which lists the steps and considerations required when you conduct your fraud risk assessment.

This is a template provided by ACAMS. Readers may amend the format and contents based on your organisation's business needs.

Appendix C2: Worked Example

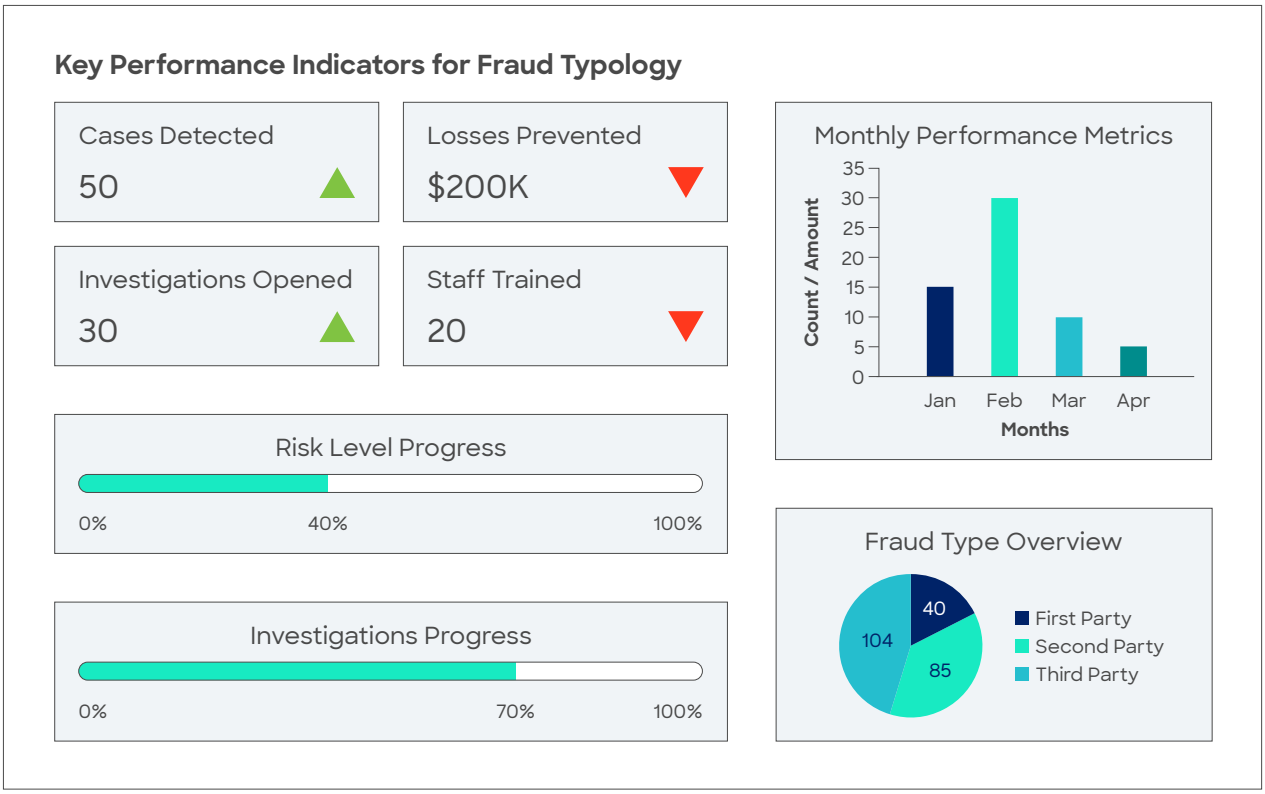
The following is a worked example demonstrating an approach to establishing new controls for an identified high fraud risk.

Identified Risk	Criminal opens an account using a synthetic identity (ID).
Existing Controls	• Checks against false ID database • Shared intelligence with other organizations • Document verification to confirm that the identification provided by the customer is authentic
Risk Score	7 = High: The possibility of this happening is likely, based on historic data, and may increase with the advent of artificial intelligence. The consequences could be severe if the volume of incidents increases.
Control Proposals	Prevention: • Introduce multi-factor authentication by requiring multiple forms of verification, such as a one-time passcode sent to the customer's mobile device • Use knowledge-based authentication to verify a customer's identity by asking specific questions that only the customer would know
Risk Owner	Head of Business
Control Owner	Head of fraud operations
Timescale	Complete implementation by end of December next year
Residual Risk Score	4 = low: Number of incidents and losses reduced

Fraud risk owners are responsible for keeping track of and responding to that particular risk. Usually these are senior business leaders.

Fraud control owners are accountable for implementing and maintaining the effectiveness of specific controls. So, while there is one fraud risk owner, there may be several different controls against that risk owned by different parts of the business, such as information technology, legal, and fraud operations.

10. Appendix D: Sample fraud risk assessment dashboard



Authors and Contributors

Authors

Shilpa Arora, Head of AFC Products and Solutions, ACAMS

Joby Carpenter, Global Subject Matter Expert, Crypto and Illicit Finance

Florence Hui, Senior Manager, AFC Products and Solutions, ACAMS

Madiha Kanwal, Fraud Subject Matter Expert, ACAMS

Katy Worobec, Director, Azymus Consilium Fraud Consultancy

ACAMS would like to thank the following key contributors to this guide:

Jonathan Arras, Senior Director, Fraud Product, Visa

Freddy Arthur, EMEA Fraud Strategy Leader, Nice Actimize

Mauriceo Castanheiro, Head of Product Strategy, Fraud Solutions, Verafin

Sally Felton, Director, Fraud Risk Management, BDO UK LLP

Edward Gilson, Senior Fraud Specialist, Vanguard

Kamlesh Harry, Director – Fraud Risk, Payment & Digital, Standard Chartered

Damian Hixson, Partnership Manager, CIFAS

Anthony Hope, Group Head of AML, CTF and Fraud Risk, National Australia Bank

Levent Kutluca, Head of Fraud, HSBC Asia Pacific

Katherine Odendaal, Director, Financial Crime, Fraud & Investigative Services, Guidehouse

Raymond Olsen, SVP, Director of Enterprise Fraud Management, Wintrust Financial Corporation

Vishnu Palaniappan, Director, Global Wholesale Fraud, HSBC

Dr. Durgesh Pandey, Partner, DKMS & Associates

Nisreen Sabri, Head Fraud Management – EMEA & Global Private Banking, HSBC Middle East

Anthony Shao, Partner (Fraud Detection and Investigation), Ernst & Young

Tobias van Kesteren, FCC Officer External Fraud/Business Change Manager, Rabobank

Kalyani Vasan, Partner, Strategy, Risk and Transactions, Forensic & Financial Crime, Deloitte