GOOD PRACTICE NOTE

Optimizing AML/CFT Risk Management *with* Technology *and* Analytics: A Playbook *for* Financial Institutions *in* Emerging Markets

JUNE 2026

IFC International Finance Corporation
WORLD BANK GROUP

About IFC

IFC — a member of the World Bank Group — is the largest global development institution focused on the private sector in emerging markets. We work in more than 100 countries, using our capital, expertise, and influence to create markets and opportunities in developing countries. In fiscal year 2025, IFC committed a record $71.2 billion to private companies and financial institutions in developing countries, leveraging private sector solutions and mobilizing private capital to create a world free of poverty on a livable planet. For more information, visit www.ifc.org.

GOOD PRACTICE NOTE

Optimizing AML/CFT Risk Management *with* Technology *and* Analytics: A Playbook *for* Financial Institutions *in* Emerging Markets

June 2026

IFC International Finance Corporation
WORLD BANK GROUP

Table of Contents

Acknowledgements vi

Abbreviations of Common Terms vii

Chapter 1: Introduction 2

1.1 Background 2

1.2 How to Navigate the Good Practice Note 3

1.3 Sources, Research Methodology, and Use of Generative AI 5

1.4 Why IFC Published This Good Practice Note 6

1.5 Strategic Benefits of Investing in Technology 9

1.6 Key Challenges Faced in Emerging Markets on Access to and Use of Technology 10

Chapter 2: Leveraging Technology in AML/CFT Risk Management 12

2.1 Opportunities Presented by Technology for AML/CFT 13

2.2 Importance of a Foundational AML/CFT Program 15

2.3 The Evolution of Technology and Use Cases in AML/CFT 15

Chapter 3: Practices for Improving Customer Due Diligence 24

3.1 Capabilities of Technology & Analytics in Addressing Challenges 25

3.2 Foundational Concepts in Customer Due Diligence 26

3.3 Techniques for Optimizing Customer Due Diligence with Technology and Analytics 30

Chapter 4: Practices for Improving Name and Transaction Screening 46

4.1 Capabilities of Technology & Analytics in Addressing Challenges 47

4.2 Foundational Concepts in Name and Transaction Screening 48

4.3 Techniques for Optimizing Name and Transaction Screening with Technology and Analytics 56

Chapter 5: Practices for Improving Suspicious Activity Monitoring 74

5.1 Capabilities of Technology & Analytics in Addressing Challenges 75

5.2 Foundational Concepts in Suspicious Activity Monitoring 76

5.3 Techniques for Optimizing Suspicious Activity Monitoring with Technology and Analytics 81

Chapter 6: Practices for Utilizing Manual Controls 106

6.1 Practices for Utilizing Manual Controls and Low-Tech Tools 107

Chapter 7: Practices for Designing a Technology Selection Strategy and Selecting a Vendor Partner 116

7.1 Key Challenges in Technology Strategy and Selection 117

7.2 Designing an AML/CFT Technology Development and Use Strategy 117

7.3 Designing an AML/CFT Technology Selection and Implementation Strategy 124

7.4 Considerations for Selecting a Vendor Partner 132

Chapter 8: Practices for System Deployment and Maintenance 142
8.1 Key Challenges in System Deployment and Maintenance 143
8.2 Practices for System Deployment 143
8.3 Practices for System Maintenance 146
Chapter 9: Emerging Financial Crime Risk Management Accelerators 150
9.1 Key Trends in the Future of Financial Crime Risk Management 151
Chapter 10: Key Takeaways 158
Appendix A: Glossary of Key Technology Terms 162
Appendix B: Control Maturity Matrix 167
Appendix C: Detection Strategies for Common Typologies 171
References 175

Acknowledgements

This Good Practice Note was prepared under the leadership of Lucas Diez-Suarez, Aisuluu Nasypbek, Chad Carson, Afua Bigirwa, Yahya Camara, and Adonis Brozoza, with contributions from colleagues across the World Bank Group, including Susanne Kavelaar, Robert Heffernan, Faisal Siddiqui, Tom Roth, Kuntay Celik, Fredesvinda Montes, Heena Gupta, Nigel Bartlett, Maristella Aldana, and Lauren Kaley Johnson, and drew on executive support from Taiwo Fayose.

This document would not have been possible without the contributions of numerous industry experts who graciously shared their time, experiences, and insights with the International Finance Corporation (IFC). IFC was fortunate to have had multiple subject matter experts working within technology providers, financial institutions, consulting and advisory firms, public-sector entities, and international organizations contribute time, input, and expertise. IFC would like to thank and recognize Andrés Felipe Cano Cadavid, Yaniree Best, Candice Huggins, Cynthia Shea, Dan Ross, J. Edward Conway, Rick McDonnell, Josée Nadeau, Allan Prochazka, Ryan Wells, Jill DeWitt, Camilla Yellets, Daniel Bisson, Michael Samonas, Kristen Toliver, Rodney Wallace, Ruth Helena Alves da Mota, Abdirahman Muhamud, Mike Moreno, Ece Kugu, Che Sidanius, Zach Johnson, Emma Jackson, Brian Love, Brian Gilman, Evgenia Wetzenstein Ollenschalager, Wolfgang Berner, along with Nikhil Aggarwal, Michael Brien, Dean Chivers, Graham Pampel, Alexander Georgieff, Parth Trivedi, Abhishek Mukherjee, among other contributors.

Finally, IFC and the core project team extend their gratitude and appreciation to the Secretariats of the Wolfsberg Group and Egmont Group of Financial Intelligence Units for their invaluable contributions and to the Secretariat of the Financial Action Task Force (FATF) for its assistance in verifying and updating the references to the FATF's work.

Abbreviations of Common Terms

AFC	Anti-Financial Crime
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
AST	Automated Screening Tool
ATL	Above-the-Line
BO	Beneficial Ownership
BTL	Below-the-Line
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CMS	Case Management System
CRM	Customer Relationship Management
CRR	Customer Risk Rating
DD	Due Diligence
DNFBP	Designated Nonfinancial Businesses and Professions
DLT	Distributed Ledger Technology
EDD	Enhanced Due Diligence
e-KYC	Electronic Know-Your-Customer
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
FT	Financing of Terrorism
GenAI	Generative Artificial Intelligence
ID	Identification Document
IFC	International Finance Corporation
IO	Immediate Outcome
IMF	International Monetary Fund
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KYC	Know Your Customer
MER	Mutual Evaluation Report
ML	Money Laundering
NBFI	Nonbank Financial Institutions
NLP	Natural Language Processing
OCR	Optical Character Recognition
P2P	Peer-to-Peer
PEP	Politically Exposed Person
PF	Proliferation Financing
pKYC	Perpetual KYC
RBA	Risk-Based Approach
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quote
RPA	Robotic Process Automation
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SLA	Service Level Agreement
STR	Suspicious Transaction Report
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UBO	Ultimate Beneficial Owner or Ownership
WBG	World Bank Group

Appendix A, "Glossary of Key Technology Terms" contains additional key technology terms, their definitions, and use cases.

1

Introduction

1.1 Background

Financial institutions (FIs) in emerging markets are on the front lines of the global fight against money laundering (ML) and terrorist financing (TF). Technology and analytics offer unprecedented opportunities to strengthen defenses, improve efficiency, and expand financial inclusion, but without the right strategies, these opportunities are often missed.

The International Finance Corporation (IFC), the private sector arm of the World Bank Group, works to improve living standards by fostering private sector growth in emerging markets. FIs are central to this mission, yet ML/TF risks can limit their participation in the global financial system, reverse development gains, and hinder capital flows.

To help address these risks, IFC previously published ***Good Practice Note: Anti-Money Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks*** (IFC 2019), which describes the essential elements of an anti-money laundering and countering the financing of terrorism (AML/CFT) risk management program aligned with international standards. While the foundational controls described in the prior Good Practice Note remain applicable, technology and analytics have transformed since the original publication, moving from enablers to essential components of modern, risk-based AML/CFT controls.

As such, this Good Practice Note builds on IFC's previous publication and focuses on how emerging market FIs can use technology and analytics to enhance preventive and detective measures. The Good Practice Note draws on, among other sources, IFC's own experiences, insights from an advisory firm, perspectives from FIs and technology providers interviewed by IFC, and a review of published international standards, guidance, and case studies (such as those published by the Financial Action Task Force, or FATF; the Wolfsberg Group; the United Nations Office on Drugs and Corruption (UNODC); and the Egmont Group of Financial Intelligence Units).

This Good Practice Note is primarily intended for use by risk management and compliance professionals as a tool to support strengthening the application of risk-based internal controls, raising awareness of technological capabilities, and guiding the efficient adoption of technology and analytics, among other outcomes. It also serves as a resource for auditors, information technology (IT) specialists, and competent authorities (such as specialists working within supervisory agencies and financial intelligence units, or FIUs).

1.2 How to Navigate the Good Practice Note

This Good Practice Note is designed as a practical, modular resource. Readers can work through it sequentially or focus on the sections most relevant to their needs.

The Good Practice Note will:

- Provide an overview of the foundational elements of an effective AML/CFT program
- Explore opportunities and challenges in using technology for AML/CFT
- Highlight best practices for technology use in customer due diligence (CDD), suspicious activity monitoring, and name and transaction screening
- Offer practices for approaching the selection of technology partners and on implementing systems
- Share examples and case studies from FIs that have undertaken technological transformations
- Examine emerging technologies and accelerators relevant to AML/CFT in emerging markets.

The Good Practice Note will not:

- Recommend specific technology providers
- Offer legal advice on compliance with laws or regulations
- Present one-size-fits-all solutions (best practices should be tailored to each FI's risk profile, operating environment, and overall risk management program).

While the practices within this document are oriented toward FIs, the themes are broadly applicable to other covered entities, including designated nonfinancial businesses and professions (DNFBPs) and virtual asset service providers (VASPs).

Organization of Good Practice Note

Chapters 1–2	Chapters 3–5	Chapters 6–8	Chapters 9–10
Introduction	**Technical Guidelines**	**Special Topics**	**Conclusion**
Objectives, Drivers, and Key Opportunities Presented by Technology	**Use Cases for Technology and Strategies for Optimizing Use across CDD, Screening, and Monitoring**	**Technology and Process Enablement**	**Where Technology & Analytics Are Headed & What Readers Need to Know**

Organization of Good Practice Note

Chapter 1: Introduction	Details the Good Practice Note's objectives, why IFC published the guide, strategic benefits of investing in technology, and key challenges faced in the adoption of technology and analytics
Chapter 2: Leveraging Technology in AML/CFT Risk Management	Details the opportunities presented by technology in AML/CFT, the evolution of technology and its use case within AML/CFT, and an example of the application of artificial intelligence (AI) in AML/CFT
Chapter 3: Practices for Improving Customer Due Diligence	Shares strategies for improving the collection of customer data, verifying customer identities and beneficial owners, conducting ongoing risk profiling, and conducting more efficient ongoing due diligence
Chapter 4: Practices for Improving Name and Transaction Screening	Shares strategies for reducing false positives, improving data quality, improving alert reviews, and strengthening governance as it relates to sanctions, politically exposed persons (PEPs), and adverse media screening
Chapter 5: Practices for Improving Suspicious Activity Monitoring	Shares strategies for improving detection of suspicious activity and reducing false positives, improving the quality of alert reviews and investigations, strengthening program governance, and migrating to machine learning and AI models
Chapter 6: Practices for Utilizing Manual Controls	Shares best practices relating to manual screening and monitoring processes for select FIs with lower inherent risk profiles
Chapter 7: Practices for Designing a Technology Selection Strategy and Selecting a Vendor Partner	Provides a framework and key considerations for defining a technology strategy (and making key decisions such as to build or buy a system) and selecting a vendor partner (when procuring vendor systems)
Chapter 8: Practices for System Deployment and Maintenance	Provides strategies for avoiding common pitfalls when deploying new technology systems and practices for ongoing maintenance of technology systems
Chapter 9: Emerging Financial Crime Risk Management Accelerators	Provides a view on the future state of technology, with a focus on shared services models, public-private partnerships, the convergence with other risk domains (such as cybersecurity and fraud), and emerging use of agentic AI.
Chapter 10: Key Takeaways	Details the primary insights from this Good Practice Note in a summary format.

1.3 Sources, Research Methodology, and Use of Generative AI

The development of this Good Practice Note was informed by a combination of IFC's practical experience, industry expertise, and recognized international standards.

Key sources of input include the following:

- **IFC's experience:** Insights derived from IFC's own experiences as a partner to over 800 FIs globally
- **Advisory firm insights:** Insights provided by a consulting firm with experience in technology and analytics in emerging markets
- **Stakeholder perspectives from FIs**: Contributions gathered through targeted interviews with representatives from FIs across the world, including FIs operating in emerging markets and those providing correspondent banking services to FIs in emerging markets
- **Input from technology providers:** Contributions from recognized technology providers (many of whom provided demos of their technology and case studies of their use) and/or existing literature on certain topics
- **Review of international publications:** Existing guidance and reports by international organizations, including those published by the FATF, FATF-Style Regional Bodies (FSRBs), Egmont Group, Wolfsberg Group, the International Monetary Fund (IMF), and the World Bank, among others.

The information presented in this note is primarily sourced from IFC's own experience, unless otherwise specified. Contributors and organizations may not be directly named in order to maintain confidentiality and ensure a provider-neutral perspective.

Finally, in the spirit of promoting the responsible adoption of advanced technology within AML/CFT, IFC used generative AI (or GenAI) when preparing this document. Specifically, GenAI contributed to conducting research, preparing initial draft language, editing and shortening language, and producing tables and graphics. However, any materials generated or edited by GenAI were reviewed by experienced editors and subject matter experts before publication, and the information within this document is the result of the intellectual work of the project team, contributors, and sources mentioned within.

1.4 Why IFC Published This Good Practice Note

IFC's primary objectives in publishing this guide are:

- **To provide FIs with additional resources to counter financial crime, which undermines development outcomes and impedes our mission to raise living standards.** Illicit financial flows fuel human trafficking, drug trafficking, arms trafficking, organ trafficking, extortion, terrorism, corruption, tax evasion, and the proliferation of weapons of mass destruction, among other criminal activities, which run counter to our mission to improve the living standards of society's most vulnerable
- **To assist FIs in implementing and operationalizing risk-based controls to prevent ML, TF, and other types of financial crime.** The FATF, an intergovernmental body established in 1989, establishes global standards for combating ML, TF, and PF. These standards, which include 40 recommendations related to technical compliance and 11 indicators related to overall effectiveness, are intended to establish a common international framework of measures that member countries and jurisdictions should implement to protect the integrity of the global financial system. These standards, which member jurisdictions agree to adhere to, mandate that countries require FIs to "identify, assess and take effective and risk-based action" to mitigate ML, TF, and PF risks by implementing risk-based prevention, detection, and reporting controls (referred to as preventative measures) (FATF 2025c). IFC intends for this Good Practice Note to serve as a resource for FIs to operationalize controls to meet these standards, and, as such, includes multiple references to the FATF's recommendations and supporting interpretative notes
- **To respond to the requests of our partners, assist them in optimizing the use of their resources, and support those operating in lower-capacity environments.** At the time of publishing this Good Practice Note, there was an industry-wide focus on improving the effectiveness and efficiency of the global AML/CFT regime while also improving financial inclusion. In 2021, the FATF highlighted opportunities for technology in a report titled "Opportunities and Challenges of New Technologies for AML/CFT" (FATF 2021a). Later, in 2024 and 2025, respectively, the Wolfsberg Group published two statements on effective monitoring for suspicious activity that encouraged FIs to "move beyond traditional transaction monitoring" and "[establish] a responsible transition framework for innovation in suspicious activity monitoring" (The Wolfsberg Group 2024; The Wolfsberg Group 2025). IFC hopes to complement these efforts (among those of many industry associations, technology providers, government authorities, and international organizations) by providing a technology rubric tailored to FIs operating in emerging markets
- **To underscore the continued and growing supervisory support for adopting advanced analytics and technology as an enabler of risk-based AML/CFT measures alongside the emergence of technology solutions designed for (or adaptable to) emerging market contexts.** In the 2021 report on the "Opportunities and Challenges of New Technologies for AML/CFT," the FATF noted "some supervisors [were] already engaging with the [private] sector to encourage the adoption of new technologies" while citing multiple examples from North America, Europe, and Asia (FATF 2021a). More recently, technology has been viewed as a critical enabler of financial inclusion and verifying customer identity, with the FATF's 2025 Guidance on Financial Inclusion and AML/TF Measures noting "a growing number of countries are adopting innovative, technology-based means to verify customer identity" (FATF 2025a). IFC has also seen growing regulatory support for innovation related to enhancing the effectiveness of suspicious activity monitoring. For example, multiple supervisory agencies, including the Hong Kong Monetary Authority and the Monetary Authority of Singapore) have issued guidance encouraging the use of machine learning, network analytics, and anomaly detection to improve monitoring effectiveness and efficiency (ABS 2024; HKMA 2023; MAS 2018). In addition, the Wolfsberg Group's statements in 2024 and 2025 highlighted the importance of moving "beyond traditional transaction monitoring" while considering fundamental pillars of responsible innovation. The growing support for innovation has

extended to emerging markets, with IFC having seen an emergence of technology offerings available to FIs in emerging markets (with many specifically tailored to the operational environments and/or language needs of certain regions), presenting greater opportunities for FIs in emerging markets to strengthen detection while advancing financial inclusion

- **To assist FIs in maintaining access to the international financial system via correspondent banking relationships.** Correspondent banking facilitates cross-border payments, remittances, and trade, but challenges related to ML/TF have hindered the ability of many banks to maintain relationships with correspondent banks. A WBG study from 2015 found "roughly half the banking authorities and slightly more local/regional banks indicated a decline in [correspondent banking relationships]" with a subsequent IFC study in 2017 finding that over 25 percent of the 300 banks surveyed in 92 countries reported reductions in correspondent banking relationships, with 72 percent reporting "multiple external challenges that reduced their ability to serve customers," citing compliance and correspondent banking-related difficulties (World Bank, 2015, and Stames et al. 2017). However, there have since been significant advancements in the ability of global banks to manage risks associated with correspondent banking. In addition, the FATF issued updated guidance regarding the due diligence measures to be applied by correspondent banks in the context of correspondent banking and other similar relationships (FATF, 2016). There have also been concerted governmental efforts to address the impact of the withdrawal of correspondent relationships, which, combined with the complementary work of international organizations, industry associations, and advancements in respondent bank's AML/CFT programs, among others, have led multiple correspondent banks to begin to offer services to new respondent banks and to new jurisdictions. However, while the situation has improved, many emerging market banks (including some considered systemically important in their own jurisdictions) still lack correspondent banking accounts with global banks, are limited to one (potentially costly) relationship, or have access to correspondent banking services only via a nested relationship. For example, a 2023 report by the Eastern and Southern Africa Anti-Money Laundering Group, which serves as the FSRB for Eastern and Southern Africa, found that 60 percent of member countries were affected by correspondent banking relationship terminations (ESAAMLG 2023)
- **To support the investment climate in the markets served by IFC by reducing a barrier to mobilizing capital.** Perceived or actual weaknesses in an FI's or jurisdiction's regime to combat ML/TF have hindered economic growth, investment, and capital flows. A 2021 IMF study found being included on the FATF's list of jurisdictions under increased monitoring (often referred to as the "grey list") resulted in "a large and statistically significant reduction in capital inflows," which "decline[d] on average by 7.6 percent of GDP" (Kida and Paetzold 2021)[1]
- **To promote financial inclusion and strengthen financial crime detection by guiding FIs on integrating technology and advanced analytics into risk management frameworks**, thereby bringing more transactions into the formal financial system and enhancing the effectiveness of AML/CFT efforts. In its 2025 guidance on financial inclusion, the FATF noted that "the use of technology-based solutions, including data analytics, can help FIs to implement a risk-based approach more effectively, focusing resources on higher-risk situations and avoiding the unnecessary exclusion of low-risk customers." It further underscores that "moving transactions from cash-based, anonymous channels into regulated digital financial services increases transparency and creates an electronic record that can be used to detect and investigate suspicious activity" (FATF 2025a). The Wolfsberg Group agrees, stating in 2022 guidance that "technology can enable an FI to both meet customer expectations on digital engagement and prioritize resources in an effective,

1 That said, FATF notes that the follow-up process, through which jurisdictions work to improve their AML/CFT regimes "help[s] prevent the harm caused by money laundering and terrorist financing in their own country and worldwide" with a February 2026 update noting that 86 of the 114 countries and jurisdictions identified had made the necessary reforms to address their AML/CFT weaknesses and to be removed from the grey list (FATF 2022b, FATF 2026).

risk-based manner" (The Wolfsberg Group 2022). Financial inclusion also enables more individuals and businesses to access financial services—a key tenet of the World Bank Group's mission—and facilitates job growth and creation.

Ultimately, in publishing this Good Practice Note, IFC aims to equip emerging market FIs with practical, technology-driven strategies that strengthen AML/CFT risk management; preserve access to global financial systems; and expand safe, inclusive financial services, thereby safeguarding development gains and enabling sustainable economic growth.

1.5 Strategic Benefits of Investing in Technology

Within the financial services industry, technology is widely recognized as a critical tool for achieving more effective AML/CFT risk management. In its report "*Opportunities and Challenges of New Technologies for AML/CFT*," the FATF found that 85 percent of surveyed stakeholders viewed new technologies as delivering the greatest benefit to AML/CFT, citing increased effectiveness due to greater speed, flexibility, capability, and improved governance (FATF 2021).

At an individual FI level, investing in technology and its supporting processes provides opportunities to:

- **Improve effectiveness at lower cost:** Overreliance on manual processes strains resources, limits risk-based approaches, and increases costs. A 2023 study found that labor accounted for 41 percent of the $85 billion spent annually on financial crime compliance across Europe, the Middle East, and Africa, compared to 31 percent for technology. Strategic technology adoption can reduce manual workloads, improve efficiency, and lower costs over time while strengthening prevention (Forrester Consulting 2023)
- **Reduce customer friction:** Leveraging technology and broader datasets can enable FIs to be "more disciplined and targeted" in their outreach to customers, resulting in minimizing information requests, a better understanding of customers, and ultimately enabling tailored services and a smoother, more personal experience (The Wolfsberg Group 2022)
- **Meet the expectations of correspondent banks and partners:** Investment in technology and analytics can enable FIs to meet the expectations of correspondent banks and other partners. Enhanced data quality, real-time monitoring, and advanced analytics provide transparency, timely reporting, and evidentiary records that counterparties require to manage their own regulatory obligations and risk exposure
- **Support the effectiveness of its jurisdiction's AML/CFT regime:** At the jurisdictional level, an FI's implementation of effective preventive measures strengthens the integrity of a jurisdiction's financial system, supports economic growth, and improves its global standing. However, the FATF, in its 2022 "Report on the State of Effectiveness and Compliance with the FATF Standards," found persistent effectiveness issues pertinent to the private sector. The report found "nearly all (97 percent) of 120 assessed countries have low to moderate effectiveness ratings for preventing money laundering and terrorist financing in the private sector" and stated that "in particular, the non-financial sector performs poorly in terms of risk awareness and applying preventive measures. In general, private sector entities need a change of culture in applying a true risk-based approach to conduct customer due diligence, keep records, and file suspicious transaction reports" (FATF 2022b). The FATF has stated that the fifth round of mutual evaluations, which commenced in 2024, place "a stronger focus on effectiveness outcomes" with the practices of FIs and DNFBPs having an important impact on multiple effectiveness indicators (FATF 2024).

At a jurisdiction level, these benefits include, but are not limited to, the following:

- **Improved investment climate:** Effective preventive measures by FIs reduce the risk that domestic banks, payment systems, and businesses are exploited by corrupt actors, criminal organizations, or for terrorism. This, in turn, builds trust with international partners and correspondent banks, which is essential for cross-border trade, capital flows, and investment
- **Access to the international financial system:** Jurisdictional-wide AML/CFT regimes that fail to adhere to international standards can result in a jurisdiction being perceived as high-risk by counterparties and lead to the withdrawal of (or limitations in) correspondent banking relationships, which can in turn undermine trade, remittances, and economic growth
- **Enhanced cooperation in investigating and prosecuting financial crime:** Technology and analytics can improve CDD, record-keeping, and suspicious activity monitoring and reporting, creating a financial trail that investigators can use to detect, disrupt, and prosecute criminal networks. Improved CDD and reporting enhances the ability of authorities to investigate and prosecute illicit actors, which was highlighted as a priority when FATF amended its procedures and methodology for conducting mutual evaluations in 2022 (FATF 2022a).

1.6 Key Challenges Faced in Emerging Markets on Access to and Use of Technology

Although technology and analytics are powerful enablers of ML/TF prevention and detection, FIs face challenges in adopting and using them effectively. While developed market FIs have historically had greater access to advanced solutions, reliance on manual workflows remains common. For example, a 2019 survey found some AML/CFT departments spent up to 90 percent of their time on manual tasks (NICE Actimize 2019, 5). FIs have also faced regulatory penalties and fines related to poor technology selection or implementation having resulted in programmatic failures.

These challenges affect FIs globally, but FIs in emerging markets face additional obstacles, including the following:

- **Limited human capital and technological capacity:** Several recent mutual evaluation reports (MERs) found many domestic banks, nonbank financial institutions (NBFIs),[2] and DNFBPs to face resource, capacity, and technical expertise constraints. This potential gap in resources and skills introduces a risk that, even when advanced technologies are acquired, some FIs may struggle to use them effectively—for example, by failing to properly calibrate monitoring systems or to fully leverage their outputs in conducting alert reviews and investigations
- **Limited customer data availability and quality:** Limitations in the availability and quality of customer data, along with data privacy and protection concerns, also pose challenges. For example, many jurisdictions still lack national identification repositories or identity document (ID) systems (which are needed for customer identity verification) or limit the ability of data to leave the jurisdiction (potentially limiting access to certain options, such as cloud-related services). In addition, many FIs have struggled to keep customer information complete, accurate, and integrated across systems
- **Limited technology offerings and support:** In some settings, the availability of software solutions remains limited or cost prohibitive. Several FIs also reported having limited support in implementing systems and regarding ongoing support (when modifications are required). Finally, even in cases where technology is available and accessible to banks, many systems are not yet accessible to or tailored to the operations of certain NBFIs, such as telecommunications operators that enable peer-to-peer (P2P) transfers
- **High cost of implementation:** High upfront costs can be a significant hurdle for smaller banks and NBFIs, which often operate with limited financial resources and must prioritize immediate operational needs over long-term compliance investments. High costs can introduce challenges for FIs to reach economies of scale (particularly those operating with lower volumes), demonstrating the value of shared utilities
- **Limited quality of supporting infrastructure:** Persistent internet connectivity issues can hinder the operation of sophisticated systems (particularly the ability to perform real-time suspicious activity monitoring and screening). Limited data storage capacity can also hinder compliance with record-keeping requirements. Inadequate infrastructure can not only disrupt operations but also can constrain an FI's ability to invest in solutions widely available in developed markets.

The chapters that follow provide practical strategies, case studies, and tools to help FIs overcome these barriers and fully leverage technology in their AML/CFT programs.

2 This Good Practice Note uses the term NBFIs to consider all FIs that are not licensed banks, such as FIs that originate credit and provide payment services (often referred to as payment service providers or money services businesses).

2

Leveraging Technology in AML/CFT Risk Management

Chapter 2 expands on the foundations set in Chapter 1 by exploring how technology and analytics can strengthen AML/CFT risk management across three core control areas: CDD, name and transaction screening, and suspicious activity monitoring and reporting. As noted, the FATF's "Opportunities and Challenges of New Technologies for AML/CFT" report found that 85 percent of surveyed stakeholders viewed new technologies as delivering the greatest benefit to AML/CFT, citing increased effectiveness due to greater speed, flexibility, capability, and improved governance (FATF 2021). Technology allows several opportunities to strengthen client relationships, as well. For example, the Wolfsberg Group noted advances in technology have "increased substantially the level of transparency between an FI and the customer" and "enhanced an FI's ability to recognize when a customer's risk profile has changed and to update the profile in a timely and effective manner" (The Wolfsberg Group 2022). Chapter 2 defines the opportunities and capabilities of technology in the application of risk-based CDD, name and transaction screening (for the purposes of complying with targeted financial sanctions and identifying PEPs and material adverse media), and monitoring of suspicious activity, before outlining the evolution of use of technology and analytics in AML/CFT controls.

Among other topics, Chapter 2 will address:

- How can technology and analytics enhance CDD, screening, and suspicious activity monitoring?
- What foundational aspects need to be in place to benefit from technology?
- What level of control maturity is needed to benefit from technology?
- How has technology and analytics evolved in recent years?
- How are industry leaders deploying technology and analytics?

2.1 Opportunities Presented by Technology for AML/CFT

2.1.1 Opportunities for Technology in Customer Due Diligence

CDD refers to the collective process of identifying a customer (and verifying their identity), identifying (and taking reasonable measure to verify) their beneficial owners, understanding the purpose and intended nature of the business relationship, and conducting ongoing due diligence on the business relationship and scrutiny of the transactions undertaken.[3,4,5]

The use of technology and analytics can enable FIs to:

- Collect more **accurate, complete, and consistent customer data** during onboarding, faster and with less intensive labor
- More **accurately verify the identity and related data of customers** (at onboarding and during the relationship) (FATF 2020)[6]
- Verify the **identity of a customer using electronic means** (known as electronic know your customer or e-KYC), often leveraging government databases, biometric authentication, and document verification technologies, among others
- More **efficiently analyze and visualize ownership structures** of customers and counterparties
- Better define a **customer's overall risk profile** at onboarding and during the relationship
- **Gain deeper insights** and mitigate risk for higher risk customers through enhanced due diligence (EDD), while also better recognizing **lower-risk situations** and applying proportionate simplified measures that enable financial inclusion
- Enhance internal escalations and approvals through **automated workflows**
- Streamline **ongoing due diligence** and required periodic reviews after onboarding
- Contribute to an **improved customer experience** by reducing friction and information requests; and
- Conduct **more relevant and real-time risk and process monitoring** through generating dashboard reporting.

Chapter 3 describes in further detail opportunities for technology and analytics in CDD and use cases in addressing common challenges.

2.1.2 Opportunities for Technology in Name and Transaction Screening

Name screening and transaction screening refer to the processes utilized to assess the names of relevant individuals (such as customers, employees, and counterparties), legal persons (such as customers, vendors, and merchants, among others) and their beneficial

3 This Good Practice Note considers CDD as defined in FATF Recommendation 10 and the Interpretative Note to Recommendation 10. Refer to Chapter 3 for the full definition at the time of publication.

4 While the terms know-your-customer (KYC) and customer due diligence (CDD) are often used interchangeably, this Good Practice Note considers KYC as the initial process of identifying and verifying a customer's identity at onboarding. CDD is broader and encompasses KYC as well as the ongoing assessment of customer risk, identification and verification of beneficial owners, understanding the nature and purpose of the relationship, and continuous monitoring to ensure customer information remains accurate and up to date. This Good Practice Note considers KYC as a component of CDD, whereas CDD is the full, risk-based process applied throughout the customer life cycle.

5 This Good Practice Note considers "customer" as any natural person or legal person that enters into a financial or business relationship with the FI, which typically occurs through the provision of recurring financial services via an account or occasional financial services that reach a materiality threshold. However, the identity and verification strategies included in this Good Practice Note may be used for individuals and legal entities that carry out occasional transactions with an FI (defined in the FATF's Interpretative Note to Recommendation 10 as those transactions above the applicable designated threshold (of USD/EUR 15,000) or that are payments or value transfers in the circumstances covered by FATF's Interpretative Note to Recommendation 16. Some jurisdictions define these relationships as "nonaccount customers" or "users" and include, for example, walk-in clients and parties to transactions who are not regular customers or account holders (for example, natural persons that receive remittance payments).

6 The guidance references a prior survey that found 26 percent of unbanked individuals in low-income countries cited the lack of official documentation as the primary barrier to account opening.

owners (when applicable, at a minimum in the context of a customer relationship), and transactions (particularly cross-border transactions) against official or other relevant lists. For the purposes of this Good Practice Note, screening is considered inclusive of sanctions screening (for example, official lists of sanctioned individuals, entities, and jurisdictions that are maintained by national or international authorities), PEP screening, watchlist screening (such as against international exclusion lists or other official lists), and adverse media screening (that is, reviewing public sources for negative news indicative of financial crime risk).[7]

The use of technology and analytics can enable FIs to:

- **Detect risks earlier** within CDD and when conducting cross-border payments
- Conduct screening in real time **to reduce the risk of delayed payments** through correspondent banks
- Conduct real time screening **to block or freeze transactions** with sanctioned parties
- Match **customer data more accurately** to identify potential hits and name variations, as well as to limit false positives
- Conduct alias detection **to uncover hidden identities and connections** to broader networks
- Conduct **batch screening** of complete customer datasets on an ongoing basis
- Identify **more relevant adverse media** indicative of financial crime through sentiment analysis
- Conduct screening against multiple lists and **to keep lists updated;** and
- Scale processing **to handle large data volumes** without compromising accuracy.

Chapter 4 describes in further detail opportunities for technology and analytics in name and transaction screening and use cases in addressing common challenges.

2.1.3 Opportunities for Technology in Suspicious Activity Monitoring

Suspicious activity monitoring refers to the manual and automatic processes undertaken by FIs to review customer activity and transactions for indications of unusual or suspicious activity, and, when identified, to analyze and, as necessary, report such activity to relevant authorities in the form of suspicious activity reports (SARs) or suspicious transaction reports (STRs).[8,9]

The use of technology and analytics can enable FIs to:

- **Detect earlier** potentially suspicious customer activity and transactions
- Automate **detection of unusual patterns** to flag suspicious activity (potentially in real time)
- Respond to **threats identified through country national risk assessments** and advisories published by competent authorities
- Improve **the accuracy of detection** to reduce false positives and false negatives
- Improve **the quality of investigations** by integrating internal and external data sources
- Enhance **internal alert reviews and investigations** through automated case managers
- Document **key decisions and report suspicious activity** (when identified); and
- Conduct **more relevant risk and process monitoring** through generating dashboard reporting.

Chapter 5 describes in further detail opportunities for technology and analytics in suspicious activity monitoring and use cases in addressing common challenges.

7 This Good Practice Note considers transaction screening in the context of FATF Recommendation 16 and the Wolfsberg Group's Payment Transparency Standards, and name screening in the context of multiple preventative measures.

8 Suspicious activity monitoring forms the underpinning of an FI's ability to meet FATF Recommendation 20 with respect to the reporting of suspicious transactions and supports ongoing monitoring within Recommendation 10. For the purposes of this Good Practice Note, suspicious activity monitoring is the broader, ongoing process of identifying, reviewing, and escalating any customer behavior—transactional or otherwise—that may indicate money laundering, terrorism financing, or other financial crime, whereas transaction monitoring is considered the process of reviewing customer transactions against defined rules, scenarios, and typologies to detect unusual or potentially suspicious activity.

9 Some jurisdictions require reporting on individual transactions (in the form of STRs) whereas others require reporting on suspicious customer activity (which could comprise multiple transactions and other factors). This Good Practice Note does not distinguish between the types of filing. The primary objectives of this Good Practice Note, as it relates to suspicious activity monitoring, are to provide FIs with tactics to enhance the detection of underlying suspicious activity and improve the quality of investigations once potentially suspicious activity is detected.

2.2 Importance of a Foundational AML/CFT Program

Technology supports ML/TF risk management, but its effectiveness depends on an underlying AML/CFT program whose design aligns with an FI's risk profile, regulatory requirements, and international standards.

A sound AML/CFT program includes the following:

- Processes to identify and **conduct due diligence over customers** at onboarding and throughout the customer relationship
- **Internal controls,** including suspicious activity monitoring, processes to identify risks, and name and transaction screening
- **Governance,** including a qualified AML officer supported by sufficient autonomy and technological and human resources
- **Training, communication, and education** for staff, senior management, and the board
- Continuous improvement and ongoing, **independent, testing**
- The embrace of a risk-based approach across all facets of the program, allocating resources in line with identified priorities and applying proportionate measures to areas of lower risk.

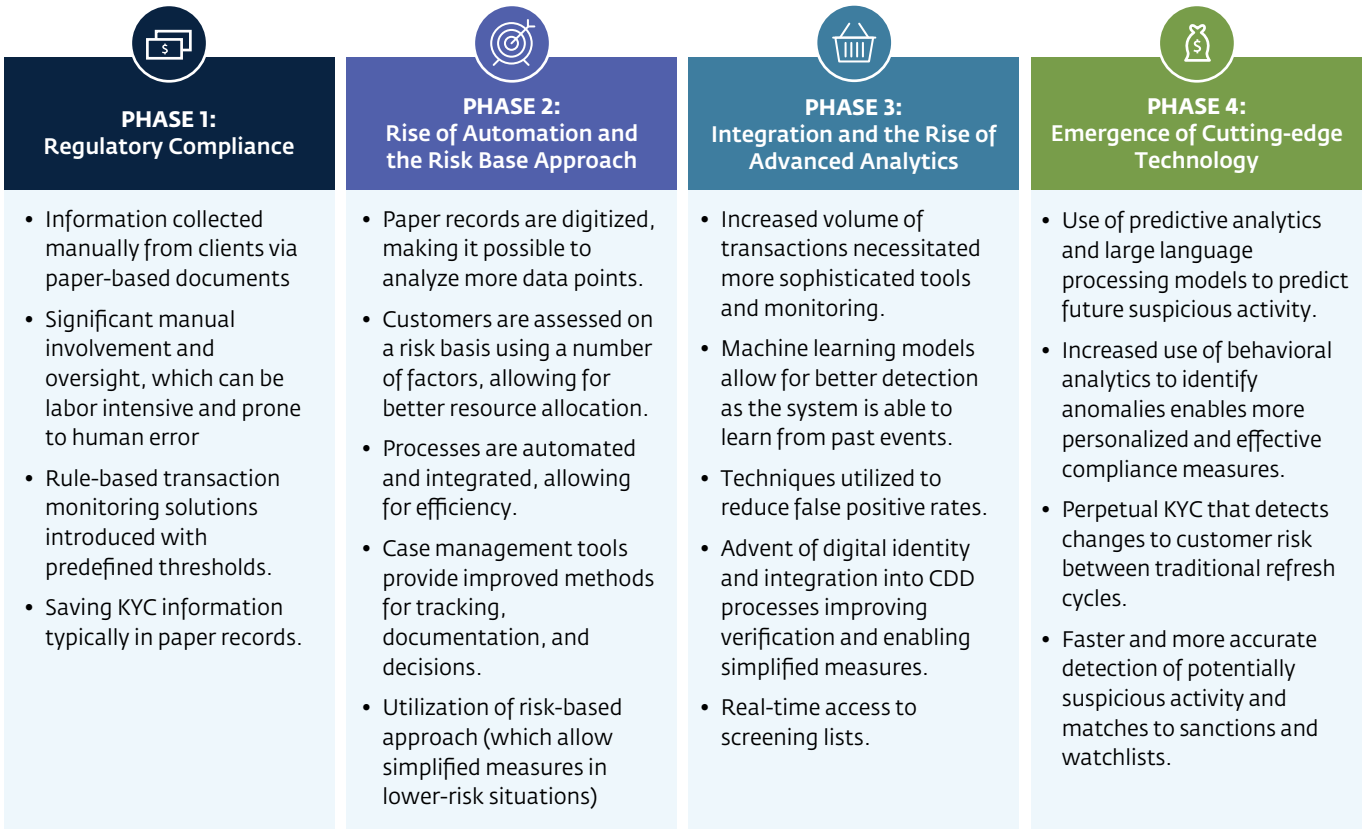
Refer to IFC 2019 Good Practice Note for additional information on the core components of an AML/CFT risk management program.

2.3 The Evolution of Technology and Use Cases in AML/CFT

Technology and analytics have transformed nearly every aspect of AML/CFT programs, with recent advancements enhancing detection, monitoring, reporting, and overall program execution.

Figure 2.1 details the four main stages of technological advancement and the characteristics of each.

FIGURE 2.1 • The Four Main Phases of Technological Advancement in AML/CFT



Source: Original for this publication.

This evolution is not anchored to a specific framework or timeframe; rather, it reflects the industry's response to financial crime risks and the challenges and opportunities associated with new technologies. Table 2.1 outlines and defines several of the main components characterizing each phase, from an initial digitization of customer records to the emergence of agentic AI.

TABLE 2.1 • Evolution of Technology Solutions and Their Role in AML/CFT

Technology Solution and Definition	Use Cases and Benefits in AML/CFT
Phase 1: Regulatory Compliance	
Digital Records Refers to the conversion of data, information, text, images, audio, or other analogue representations into digital form that can be processed by computers (for example, the digitization of onboarding forms and CDD records).	• Digital records provide a comprehensive and accessible repository of customer and transaction data, which facilitates access and analysis of information • Advanced technologies such as AI and machine learning rely on digital data to detect patterns and anomalies

Technology Solution and Definition	Use Cases and Benefits in AML/CFT
Phase 2: Rise of Automation and the Risk-Based Approach	
Automated Screening Tool (AST) Refers to the software system(s) that automate name and transaction screening (replacing manual methods). When ASTs identify matches against included sanctions lists (for example, the U.N. Security Council Consolidated List) and other watch lists, before proceeding further an "alert" is generated for manual review. In cross-border payments, ASTs enable screening of payments prior to processing (reducing the risks of payments being frozen or blocked by intermediary banks).	• ASTs automatically compare customer and transactional data against a wide range of internal and external lists, improving both speed and accuracy • ASTs employ statistical and algorithmic approaches, such as fuzzy matching and risk scoring, to detect potential matches that may be missed through manual processes. • ASTs are typically used during customer onboarding, on an ongoing basis thereafter (typically daily, weekly, or monthly, depending on an FI's risk profile), and prior to processing a cross-border payment
Transaction Monitoring System Refers to the software system(s) that review customer transactions (for example, deposits, withdrawals, transfers, and payments) against predefined rules and behavioral patterns to detect patterns indicative of potentially suspicious activity.	• A transaction monitoring system automatically identifies and generates alerts for potentially suspicious transactions when they meet predefined rules and scenarios. The alerts enable FIs to investigate (and report, if necessary) indications of suspicious activity • Historically, transaction monitoring systems have been based on transactions meeting predefined rules, but recent advancements have embedded machine learning and artificial intelligence techniques into many software solutions
Workflow Management Refers to either the automation of events or processes, allowing tasks—such as steps in customer onboarding—to be routed automatically to the applicable process or control owner.	• Workflow management can enable efficient and consistent task management across multiple teams and departments (for example, automatic PEP escalation for management review and/or approval)
Case Management System (CMS) Refers to software solutions that provide a structured process to manage, investigate, and document alerts from initiation to resolution.	• CMSs serve as centralized repositories for managing alert reviews within a team (as well as enabling oversight to prevent alert backlogs) • CMSs can be used to support the completion of CDD across teams and/or the review of alerts from screening and suspicious activity monitoring • The digital approach simplifies access to relevant records and eliminates the need for physical storage • CMSs can generate audit trails to demonstrate compliance with policies and procedures

Technology Solution and Definition	Use Cases and Benefits in AML/CFT
Phase 3: Integration and Rise of Advanced Analytics	
Digital Identity (or Digital ID) Refers to the software solution(s) designed to identify and verify the identity of natural or legal persons. These systems bind the identity to a digital credential, which, together with other authentication factors, is used to confirm that an individual claiming an identity is, in fact, the identity-proofed individual. At present, Digital ID is typically limited to jurisdictions with centralized national registries and effective verification capabilities or where authoritative sources (such as credit bureaus) exist. Digital IDs also serve as an important control for managing risks of fraud and fictitious customer accounts.	• Digital ID may improve customer access to financial services while ensuring the security and accuracy of customer information through biometric verification (FATF 2020) • Digital ID has the potential to lower compliance costs and reduce the impact of human error in capturing customer information • This approach supports a shift from periodic KYC reviews to a continuous, event-driven process, where customer information is updated continuously • When implemented responsibly, digital ID allows the FI to "pursue new customers without face-to-face interaction—including the underbanked—while focusing resources to address priority financial crime threats" (The Wolfsberg Group 2022)
Biometric Identity Verification (or Biometrics) Refers to the unique physical characteristics that can be used to identify an individual, including physical traits (for example, fingerprints, facial features, iris or retina patterns, or hand geometry) and behavioral traits (for example, voice patterns).	• Biometrics are used during "liveness checks," which confirm that biometric data (for example, a fingerprint or facial features) are being captured from a real, live person at the time of verification (and not from a photo, video, mask, or other spoofing method) • Biometrics enables advanced identity verification in remote customer onboarding and subsequent authentication when initiating a transaction
Electronic Know-Your Customer (e-KYC) Registries Refers to a centralized or federated database maintained by a government agency, regulator, or industry body that stores verified identity information and makes it accessible to authorized FIs through secure APIs or other electronic interfaces. An e-KYC registry acts as a single authoritative source for customer identity verification, allowing participating institutions to retrieve, confirm, and update KYC data without reverifying each customer independently. Registries are often linked to a national ID system, biometric database, or other official records. In emerging markets, e-KYC registries can simplify onboarding for customers who already have a verified digital identity, enabling broader access to financial services.	• Supports real-time and remote verification using secure API connections to national ID or other authoritative sources • Reduces compliance costs by eliminating repetitive KYC processes for customers who move between FIs • Facilitates financial inclusion by enabling quick onboarding for customers with verified identities, even in remote locations • Can be integrated with screening tools to trigger alerts based on changes in customer status (for example, becoming a PEP) • When updated regularly, supports a continuous, event-driven model where identity data stays current with minimal customer intervention

Technology Solution and Definition	Use Cases and Benefits in AML/CFT
Artificial Intelligence (AI) Refers to a machine-based solution capable of making predictions, recommendations, or decisions that influence real or virtual environments, based on human-defined objectives while operating under varying levels of autonomy and human oversight. The primary goal of AI is to automate aspects of analysis, reducing human labor for routine tasks and uncovering insights that may not be readily accessible to humans. Currently, machine learning is the most familiar and widely developed form of AI within AML/CFT, but other forms of AI (including GenAI and agentic AI, as described in Phase 4) quickly emerging.	• AI enables advanced anomaly detection capabilities in support of suspicious activity monitoring. For example, AI can analyze vast amounts of transaction data to identify patterns and behaviors that deviate from the norm (indicating potentially suspicious activity) • AI provides an opportunity to improve detection, reduce reliance on manual processes, and improve the speed and accuracy of investigative efforts • GenAI can support initial research, drafting and editing internal reports, or even drafting SAR and STR narratives
Machine Learning Refers to a subset of AI that trains computer systems to learn from data, identify patterns, and make decisions with minimal human intervention. Machine learning involves developing algorithms to solve problems automatically through experience and evolving pattern recognition, often with limited (known as supervised) or no (known as unsupervised) direct human involvement.	• Within screening and suspicious activity monitoring, machine learning can analyze the results of previous investigations and false positives and learn to identify potential alerts that can be closed automatically, without human intervention • Machine learning can recognize patterns such as those leading to SARs or STRs or customer exits, and prioritize higher-risk alerts, including the ability to respond more rapidly to identified national priorities (The Wolfsberg Group 2025) • Machine learning techniques can be further automated, as described under agentic AI
Natural Language Processing (NLP) Refers to a subset of AI that enables computers to understand, interpret, and manipulate human language. NLP enhances the analysis of unstructured data, such as text from emails, social media, and news articles, enabling FIs to extract meaningful insights from large volumes of text data, helping to detect indicators and connections that may indicate illicit activities.	• NLP can be used in adverse media screening to identify more relevant results and reduce false positives by not flagging certain matches unnecessarily • In these scenarios, NLP can perform sentiment analysis and identify positive or negative context within media sources. For example, in the sentence, "The CEO of ABC Company was removed by the board; however, John Smith, who has sufficient experience, has replaced him," NLP can determine John Smith is portrayed positively
Robotic Process Automation (RPA) Refers to a productivity tool that enables users to configure scripts, often referred to as "bots," to automate certain actions (such as gathering customer and transaction data in the context of alert reviews). Bots can mimic or emulate selected tasks within broader processes (such as manipulating data, transferring data between applications, or triggering responses). RPA utilizes a combination of user interface interaction and descriptor technologies (for example, systems that capture standardized descriptive data) to perform these tasks. Scripts can operate across multiple software solutions, overlaying and automating processes.	• RPA can automate investigative or other documentary manual processes, ultimately decreasing the workload on staff responsible for investigating and resolving alerts. For example, RPA can gather information from a customer's CDD file, transaction activity, and publicly available sources to support an analyst's review of a suspicious activity monitoring alert • This approach not only enables human investigators to focus their time on high-impact analysis but also to help reduce false positives

Technology Solution and Definition	Use Cases and Benefits in AML/CFT
Phase 4: Emergence of Cutting-Edge Technology	
Distributed Ledger Technology (DLT or Blockchain) Refers to a protocol that enables simultaneous access, validation, and updating of an immutable ledger (a digital record) distributed across multiple computers. DLT typically operates across multiple entities or locations, creating a distributed digital database. DLT is not yet widely adopted in AML/CFT programs.	• DLT could create a secure, immutable record that allows customer information to remain updated and to prevent it from being altered • By providing a digital record accessible only to authorized parties, DLT can reduce the risk of data manipulation and fraud (providing enhanced security) and enable more efficient payment processing
Agentic AI Refers to software programs designed to independently make decisions and take actions to achieve specific goals. Agentic AI possesses a high degree of autonomy and decision-making capability, enabling it to perform tasks with limited human intervention. This type of AI forms the foundation for building intelligent applications.	• Agentic AI has the potential to impact many AML/CFT controls. Among others, agentic AI has been used to conduct initial alert reviews and draft SARs or STRs for submission • In CDD, by incorporating contextual factors, Agentic AI can perform more dynamic customer risk rating • In transaction monitoring, agentic AI can detect anomalies by identifying previously flagged suspicious behaviors and applying the same investigative logic to current transactions. This approach differs from traditional rule-based threshold methods, offering greater adaptability and intelligence

Source: Original for this publication.

Later, Chapters 3–5 provide additional use cases as well as examples of this technology used by FIs (including in emerging markets) across each phase. Chapters 7 and 8 provide best practices for deploying technology solutions, with Chapter 9 highlighting the direction of today's cutting-edge technology.

2.3.1 Example of Today's Technology Capabilities

As an example of the leading edge of technology and analytics, some FIs have been able to realize significant gains in detecting more suspicious activity and reducing false positives. The following case study details the efforts of a global bank interviewed by IFC that ultimately led to a two- to fourfold increase in the identification of suspicious activity, while reducing alerts by 60 percent.

CASE STUDY • A Global Bank's Journey to Identifying up to Four Times More Suspicious Activity While Reducing Alerts by 60 Percent

PROBLEM: The bank wanted to improve its transaction monitoring processes as compliance professionals felt that its current detection methods were slow and inefficient, relying on broad customer segments and manual investigations. The bank wanted to implement a solution that was faster, more efficient, and more effective. The suggested approach was partnering with a cloud service provider to develop an AI-based monitoring system, but there were concerns relating to data privacy and model explainability.

SOLUTION: The solution was designed to run in the cloud and to utilize a vendor partner's AI for risk detection, with models trained and validated on the bank's production data. The bank leveraged its expertise in financial crime compliance to refine these models. As part of the solution, security concerns were addressed as the bank ensured all information was encrypted within its cloud environment both in transit and at rest. The bank prioritized model governance to ensure risk score explainability. The project employed DevOps principles (of continuous integration and delivery to shorten the development lifecycle) and agile methodologies to enhance software development, marking the bank's initial agile-at-scale venture. This approach supports rapid experimentation for strategic investment.

OUTCOME: The solution processes data within days, significantly faster than the previous 30-day system. The bank's monthly analysis of 8 billion transactions across 63 million accounts now takes just a few days. The solution has uncovered suspicious behaviors and new typologies, such as misuse of business loans, without specific models. Its ability to detect broader network activity has enhanced insights for compliance analysts, improving the conversion rate of suspicious transaction alerts reported to authorities with more detailed information.

Source: An FI interviewed by IFC

3

Practices for Improving Customer Due Diligence

Chapter 3 builds on prior chapters by further defining opportunities for technology and analytics, as well as best practices for leveraging them, within CDD. CDD is a foundational component of an FI's AML/CFT program, yet many FIs continue to face challenges such as manual customer outreach, data limitations, and issues with system connectivity, which has led to process inefficiencies, inconsistent risk assessments, increased costs, and increased risk of breaching regulatory requirements. However, there are multiple opportunities to leverage advanced analytics and technology to enhance CDD practices, which can improve onboarding, data quality, verification measures, risk rating methodologies, and ongoing due diligence, among other controls.

Among other topics, Chapter 3 will address the following:

- What are the main challenges in conducting CDD?
- What are the main process steps in conducting CDD?
- What are the capabilities of technology and software solutions available?
- What are some strategies and technology use cases to better collect customer information?
- How can technology enable more accurate verification of the identity of customers?
- How can technology enable more accurate verification of ultimate beneficial owners (UBOs)?[10]
- How can technology enable FIs to more accurately verify the address and location of customers?
- How can analytics enable FIs to assess customer risk continuously?
- What are the practices for conducting efficient ongoing due diligence (or periodic reviews)?
- What is perpetual KYC (or pKYC) and how are FIs integrating it?

10 Using the definition from the FATF Glossary, the term "beneficial owner" refers to the "natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person." The Good Practice Note refers primarily to UBOs in the context of taking measures to identify and verify the identity of the natural persons that ultimately own or control a legal person or legal arrangement.

3.1 Capabilities of Technology & Analytics in Addressing Challenges

FIs of all sizes and maturity levels face challenges in conducting effective CDD. These include:

1. **Manual and fragmented data collection and analysis:** Reliance on paper-based processes, fragmented data sources, and the absence of workflow automation can introduce operational complexity, cause delays, and result in inconsistent data quality. In addition, utilizing multiple external sources can be cost prohibitive for many FIs.
2. **Weaknesses in verification and authentication methods:** In many jurisdictions, there are limitations in an FI's ability to leverage authoritative sources for verifying customer identity and beneficial ownership information and for identifying lists of sanctioned individuals or PEPs. As a result, FIs may have vulnerabilities in their CDD processes and increased exposure to individuals or entities subject to sanctions, among others.
3. **Weaknesses in UBO identification processes:** Complex ownership structures and poor or fragmented data transparency can hinder accurate identification and verification of beneficial owners (particularly when involving shell companies, other nominee arrangements, and/or jurisdictions with limited beneficial ownership data availability).
4. **Static customer risk ratings:** Outdated customer risk ratings may not reflect changes in customer behavior or external risk factors, resulting in missed escalations, ineffective monitoring, and failure to detect emerging risks. Actual customer behavior may also indicate that a customer's current risk profile presents a lower risk than when initially assessed. Maintaining accurate and dynamic risk ratings requires continuous monitoring and integration of new information, which is frequently absent in static or periodic CDD approaches.
5. **Workload in conducting ongoing due diligence:** Periodic refreshes (which includes updating customer information on set intervals after initial onboarding) can require significant human resources and coordination among multiple business areas, introduce customer friction, and may fail to address emerging risks as they occur, all while leading to potential audit and regulatory findings if customer information cannot remain up to date.
6. **Misalignment of internal incentives:** Tension between sales priorities (for example, high growth targets, speed in onboarding customers, the need to minimize friction in customer experience, and associated customer churn) and risk management practices (including thorough CDD and EDD, if necessary), can lead to inconsistent application of controls and pressure to bypass processes, which can impact an FI's profitability and resources.
7. **Staff expertise and capacity:** FI staff, particularly those in operational or client-facing roles, with limited knowledge of corporate structures, understanding of beneficial ownership, ability to identify red flags, and/or limited familiarity with authentication and research tools, can present a vulnerability in the effectiveness of CDD.

Collectively, these challenges can result in a fragmented customer experience, as siloed processes cause repeated information requests, delays, and inconsistent communication. In some cases, they may also result in multiple profiles for the same customer across the FI, affecting customer satisfaction and potentially driving them to competitors.

However, there are software solutions and techniques that FIs can use to strengthen CDD. For example, some available solutions can combine automated identity verification, risk scoring, and continuous monitoring within a single platform. These features can also feed into related solutions that can assess enterprise-wide risks. Many solutions offer features like electronic ID checks, beneficial ownership mapping, and sanctions screening, which can be integrated with real-time transaction monitoring and dynamic customer risk rating updates. In addition, advanced analytics and workflow automation tools exist that can streamline customer onboarding and periodic reviews while retaining documentation for audit purposes.

3.2 Foundational Concepts in Customer Due Diligence

Before highlighting techniques to overcome these challenges, this Good Practice Note first provides foundational information on CDD. While this section provides useful background information that can benefit experienced professionals, readers familiar with these concepts and that are focused primarily on strategies to overcome challenges may proceed directly to Section 3.3, "Techniques for Optimizing Customer Due Diligence."

3.2.1 Defining Customer Due Diligence

Per FATF Recommendation 10, and the corresponding Interpretative Note to Recommendation 10, CDD refers to the collective process of identifying a customer (and verifying their identity), identifying (and taking reasonable measures to verify) their beneficial owners, understanding the purpose and intended nature of the business relationship, and conducting ongoing due diligence on the business relationship and scrutiny of the transactions undertaken.[11]

CDD is also foundational to downstream processes such as name screening, transaction screening, and suspicious activity monitoring and reporting, with Recommendation 10 also linking to several other recommendations and immediate outcomes.

In 2025 guidance, the FATF encouraged FIs and countries to consider "the implementation of CDD measures that are proportionate to the relative risks of a product" to "significantly increase access and the use of financial services" (FATF 2025a). The guidance highlights multiple Simplified Due Diligence (or "SDD") measures enabled via technology and analytics, described further in Chapter 3.3.2.1.

FATF's Recommendation on Customer Due Diligence

FATF's Recommendation 10 outlines the following measures for CDD (FATF 2025c):

- Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the FI is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include FIs understanding the ownership and control structure of the customer
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds

11 As noted in Chapter 2, while the terms KYC and CDD are often used interchangeably, this Good Practice Note considers KYC as the initial process of identifying and verifying a *customer's* identity at onboarding. CDD is broader and encompasses KYC as well as the ongoing assessment of customer risk, identification and verification of beneficial owners, understanding the nature and purpose of the relationship, and continuous monitoring to ensure customer information remains accurate and up to date. This Good Practice Note considers KYC as a component of CDD, whereas CDD is the full, risk-based process applied throughout the customer life cycle.

3.2.2 Key Process Steps within CDD

Table 3.1 outlines the key stages of CDD, underlining main components and considerations for each stage.

TABLE 3.1 • Stages within CDD and Key Process Steps

#	Stage	Key Process Steps and Considerations[12]
1	**Customer Identification and Information**	• For natural persons, collect basic identifying information to properly establish the customer's identity. The requirements may vary by jurisdiction, but typically include the customer's legal name (first and last name), date of birth, residential address, and an official identification number or other unique identifier[13] • For legal persons and arrangements, collect basic identifying information to properly establish the customer's identity. The requirements may vary by jurisdiction, but typically include the name of the legal person or arrangement, registered or commercial address, principal place of business (if different from the registered address), an official identification or registration number, information on the legal form and governance structure (for example, the memorandum and articles of association of a company), and the names of directors, senior management, and persons authorized to act on behalf of the legal person or arrangement • Determine if other information should be collected based on local requirements and while considering a risk-based approach. For individuals, this may include occupation, source of income, and gender, among others, which may be required by the jurisdiction's regulatory or legal requirements and/or assist in customer risk rating. For legal persons, this may include the legal person's registration date and jurisdiction of registration, authorized signatories, and industry. In determining whether any additional information should be collected, FIs are required to apply a risk-based approach (and consider whether information is pertinent to assessing and mitigating risks and/or managing legal, regulatory, or contractual obligations)

2	**Customer Identity Verification**	• Implement measures to confirm that the information is accurate and authentic using reliable and independent sources
		• Define methods for acceptable documentary verification (that is, utilizing documents provided by a customer) and/or nondocumentary verification (for example, third-party sources)
		• Define acceptable sources for an official identity, which may include one or more of the following:[14]
		  ○ For natural persons and UBOs:
		  ❖ Domestic government-issued IDs (for example, national ID, voter ID, driver's license)[15]
		  ❖ Foreign government-issued IDs (for example, a passport)

12 The stages and steps outlined in this table are based both on the FATF's Recommendation 10 and Interpretative Note to Recommendation 10 and common industry practices for completing CDD. Local requirements may vary and may require additional or different procedures. Readers are encouraged to consult applicable local laws and regulations as this table is not intended to be an exhaustive list of all possible steps.

13 As noted in FATF's 2020 Guidance on Digital Identity, examples of official Identification numbers may include, but are not limited to: a taxpayer identification number, driver's license number, passport number, number from a voter registration card, social security number, and refugee Identity documents.

14 For additional insights, refer also to FATF 2020.

15 The term "ID" or "IDs" refers to a government-issued document or officially recognized credential used to verify the identity of an individual or legal person. For individuals, this may include passports, national identity cards, driver's licenses, or other forms of photographic identification. For legal entities, this may include certificates of incorporation, registration documents, or business licenses issued by relevant authorities. In most cases, a government-issued ID is required, but, in certain cases, an FI can identify a customer without a government-issued ID and instead apply "simplified measures." An example of simplified measures enabling account opening without a government-issued ID is included later in this chapter.

#	Stage	Key Process Steps and Considerations[12]
		❖ Cross-referencing information with official government databases and registries (for example, electronic know-your-customer or e-KYC registries) ❖ Cross-referencing information to private databases (for example, credit bureaus). o For Legal Persons and Arrangements ❖ Proof of existence (for example, a certificate of incorporation, a certificate of good standing, a partnership agreement, a trust deed, or other documentation from a reliable and independent source confirming the name, form and current status of the customer) • Define alternate verification measures for lower-risk instances. Per the FATF's 2025 Guidance on Financial Inclusion, an FI's identification program may consider alternative data points and verification measures that, subject to local requirements, could be applied in lower-risk instances[16]
3	**Identification and Verification of UBOs (for Legal Persons and Arrangements)**	• Establish a definition of UBOs using a threshold based on the legal requirements within the jurisdiction and any additional risk-based controls (with a minimum of 25 percent ownership or lower thresholds in certain higher-risk scenarios, such as 10 percent, and any additional individuals exercising control over the legal person) • Establish a definition of UBOs for legal arrangements. For example, the definition should also include the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control • Establish methods to identify UBOs (which, for example, could include asking the customer for a list of UBOs and/or accessing official registries, among other sources.) • Implement reasonable measures to verify the identity of the UBOs, such as: o Obtaining a signed certification from the customer regarding its UBOs o Obtaining corporate documentation (for example, articles of incorporation, shareholders registries, or directors exercising significant influence or control) listing the legal person's UBOs o Gathering the name, date-of-birth, residential address, and an identification number for identified UBOs o Cross referencing information to other independent and reliable sources, such as a beneficial ownership registry, a companies registry, public databases, or third-party provided sources
4	**Customer Risk Rating (also known as Customer Risk Profiling)**	• Obtain information on the purpose and intended nature of the customer relationship • Assess the risk presented by the customer at onboarding, considering, among others: o Customer type (for example, individual vs. legal person) o Customer industry or occupation (that is, if operating in higher-risk industries and income sources) o Geographic location (that is, if operating in a higher-risk area or jurisdiction) o Products and services (that is, if utilizing higher-risk products) o Anticipated transaction value and volume • Assign a measurable risk rating (for example, high, medium, or low) using qualitative and quantitative data, which may then trigger additional due diligence

16 This list comes from paragraph 154 of the FATF's 2025 Guidance on Financial Inclusion. The Guidance includes a non-exhaustive list of examples of alternative data points and verification measures that, subject to local requirements, could be applied in lower-risk instances to enable financial inclusion for individuals without a formal identity document (FATF 2025a).

#	Stage	Key Process Steps and Considerations[12]

5	**Enhanced Due Diligence (EDD)**	• Obtain additional information for customers presenting heightened risk or meeting one of several predefined categories. EDD may include, among others:
		  ○ Completing adverse media screening (in addition to PEP and sanctions screening)
		  ○ Obtaining and verifying information on source of funds or wealth
		  ○ Completing a site visit for certain legal person customers
		  ○ Understanding the legal person's AML/CFT controls (if applicable)
		  ○ Obtaining information specific to the customer type (for example, if a PEP, information about the PEP's current or former role and ability to direct government funds)
		  ○ Obtaining independent references from third parties who may have knowledge about the customer
		• Obtain additional approvals (as required) before onboarding the customer
		• Conduct enhanced monitoring (throughout the customer relationship)

6	**Ongoing Due Diligence (known also as Periodic Refresh or Perpetual KYC)**	• Implement measures to ensure that customer information remains current, customer identity is verified, and that the FI maintains a continuous understanding of the customer relationship. In most jurisdictions, this is achieved through a periodic review process, with the frequency of updates determined by the customer's risk rating (typically annually for higher-risk customers). However, many FIs are now utilizing a combination of perpetual KYC and trigger-event-based approaches to updating customer information • Evaluate if transactions are aligned with the customer's profile (as a method to identify the person on whose behalf a transaction may be conducted)

Source: Original for this publication, with information sourced from FATF 2025a, 2025c, BCBS 2014.

There are also times where simplified due diligence (also known as simplified measures or SDD) may be permissible. According to the FATF, "where the risks of money laundering or terrorist financing are lower, financial institutions should be allowed and encouraged to implement simplified CDD measures." These include allowing FIs to verify the identity of the customer after establishing a business relationship (for example, if account transactions arise above a defined threshold) and not collecting specific information related to the nature of purpose and intended nature of the relationship, but rather inferring the purpose and nature from the type of transactions or business relationship established (FATF 2025c). Chapter 3.3.2.1, "Using Technology and Transaction Limits to Apply Simplified Measures and Promote Financial Inclusion," provides further information.

3.2.3 Comparing Manual vs. Automated CDD

Manual CDD processes rely on paper forms, physical document checks, and human review to collect, verify, and assess customer information. While they can offer flexibility and allow for nuanced judgment in complex cases, manual approaches are time-consuming, prone to human error and misconduct, and often result in inconsistent data quality, delays, and higher operational costs. Automated CDD processes leverage technology such as digital onboarding platforms, biometric verification, data integration tools, and workflow automation to streamline data collection, improve accuracy, and enable real-time risk assessment. Automation supports scalability, consistency, and faster decision-making, but requires reliable internal and external data sources, robust governance, and appropriate system tuning to avoid excessive false positives or missed risks. In practice, many FIs adopt a hybrid approach, using automation for routine tasks and manual review for high-risk or complex cases.

3.3 Techniques for Optimizing Customer Due Diligence with Technology and Analytics

As previously noted, FIs face many challenges in conducting CDD, including, but not limited to, the quality and completeness of customer data; the ability to identify and verify the identity of customers; maintaining an accurate risk rating of customers; and in completing ongoing due diligence.

The following sections offer strategies, best practices, and considerations for the following topics:

3.3.1 Strategies for Improving the Collection of Customer Data

Achieving consistent and updated customer data remains a challenge for FIs globally, particularly those with multiple business lines, as disparate data structures and inconsistent processes can hinder customer identification and risk rating. Manual processing and poor data management represent several barriers to improvement, with many FIs still onboarding corporate customers through manual workflows. While centralizing customer information in a single data lake offers benefits, it is not the only way technology can enhance CDD. Automation, secure storage, metadata tagging, and digital forms can streamline data collection, improve accuracy, and reduce costs without full centralization.[17] Consistent, high-quality data at onboarding is critical as poor input leads to poor output, and foundational technologies not only strengthen routine data capture but also support the more complex task of identifying and verifying UBOs.

Table 3.2 outlines several data collection technologies and considerations for their use.

17 The term "data lake" refers to a centralized repository for storing structured and unstructured data at scale. Within AML/CFT, a data lake can be used to aggregate and standardize customer, transaction, and external data, from multiple sources, to be applied for one or more purposes (such as customer risk rating). The term "metadata" refers to information that describes and provides context about other data, such as its source, creation date, author, format, or classification. Within AML/CFT, metadata supports data integrity, auditability, and efficient retrieval by recording details about when, how, and by whom customer information was collected or updated. Refer to Appendix A, "Glossary of Key Technology Terms," for additional information.

TABLE 3.2 • Technology and Use Cases in Data Collection

Technology Solution and Definition	Best Practices for Use
Data Collection	
Automated Forms Refers to the use of a digital form during onboarding where customers input required information (for example, name and date-of-birth) and provide additional requested data (for example, occupation and source of wealth). These forms remain important for collecting high-quality digital data from a customer, with many FIs embedding data intake through a direct customer-facing digital portal.	• Enable structured data capture by using digital forms, drop-down lists, check boxes, and conditional logic to ensure consistent, high-quality input and avoid free-text variability • Streamline, integrate, and automate data capture by pre-populating fields from existing records, extracting shared customer data across business units, and applying auto-formatting to maintain accuracy • Capture the full legal person name (and/or a unique identifier number) and alternate names (so-called "doing business as" or "aliases") to enable systems to avoid creating multiple profiles • Limit drop-down options and structure industry or subindustry selection for clarity and precision • Embed quality controls by applying field validation (for example, flagging incomplete or inconsistent entries) • Establish a documented firm-wide data structure that defines accuracy and completeness expectations
Mobile Devices Refers to the use of smartphones to scan and directly upload customer documentation, improving data collection and reducing delays associated with manual submission.	• Use mobile applications or secure web front ends integrated with core systems to capture customer information efficiently • In regions with less smartphone penetration, consider using unstructured supplementary service data, which allows exchange of text messages with a customer using less sophisticated mobile devices, to collect onboarding data at low cost
Optical Character Recognition (OCR) Refers to the uploading or real-time capture of documents and the extraction of structured information from these documents into text. This text can then be used to prepopulate forms or to validate information previously captured.	• Use OCR to minimize clerical errors during data entry, which can reduce the risk of missed or inaccurate matches in screening errors (particularly in non-Latin alphabets or transliterations) • Configure systems to automatically identify documents that do not match predefined templates. Route to an analyst for manual review • Embed quality controls by applying field validation (for example, flagging incomplete or inconsistent entries)

Technology Solution and Definition	Best Practices for Use
Commercial Databases Refers to external data sources offered by specialized vendors containing information on PEPs, sanctions lists, adverse media, watchlists, and corporate registries. Integrating commercial databases into CDD processes can enable automated screening for high-risk individuals and entities, support EDD, and help validate customer-provided information.	• Consider third-party databases to identify and verify UBOs and for later screening for PEPs, sanctions, and adverse media • Consider third-party sources (such as KYC utilities or repositories) for gathering information about an FI's counterparties (such as the, Wolfsberg Questionnaire), particularly if establishing a commercial but not account relationship
Data Storage	
Document Storage Refers to the retention of gathered documents (whether digital or physical) in secure environments with access controls defined by user roles, with an additional advantage of creating secure backup copies to ensure data continuity.	• Centralize storage and avoid storing documents in email or local drives, or in one physical location without a backup copy. Use defined processes and naming conventions to ensure consistent loading and retrieval • Apply metadata or tracking to record modifications, timestamps, and expiry dates • Maintain data in environments where investigators or regulators can readily access required information • Align storage practices with requirements on recordkeeping and securely dispose of records after expiration
Customer Relationship Management System (CRM) Refers to the software platform(s) used to collect, organize, and manage customer information, including contact details, account profiles, onboarding records, and communication history, throughout the customer life cycle.	• Centralize customer data and communications in a single platform, avoiding fragmented records in emails or folders • Apply consistent data entry standards, user roles, and access controls (aligned with a firm-wide data dictionary) to safeguard information and support privacy • Integrate with screening and other workflow tools for CDD, ongoing monitoring, and escalation of alerts
Data Verification or Integrity	
Biometrics Refers to the automated recognition of individuals based on their biological and behavioral characteristics. Biometric data may include voice, fingerprints, facial features, and retinal patterns. Biometrics enables liveness testing and presentation attack detection, thereby improving the verification of individuals providing information, particularly in non-face-to-face onboarding scenarios.[18]	• Consider risks of deepfakes (synthetic media products in which AI is used to realistically manipulate or fabricate a natural person's appearance, voice, or actions) • Match biometric data (for example, facial recognition) against uploaded documents or trusted external databases for e-KYC onboarding • Encrypt biometric information and transmit it securely after capture • Incorporate liveness detection to confirm a live presence (for example, blinking, head movement)

18 Per the World Bank Group's report "Identification for Development: Digital ID and Financial Inclusion" (2019, 56), biometric verification can help expand financial access while mitigating fraudulent account opening and can be effective even in contexts with low literacy, provided privacy safeguards are observed. Similarly, the FATF's 2025 Guidance on Financial Inclusion highlights multiple examples of utilizing biometric data as a mechanism for non-face-to-face customer identification and verification that enables, in some cases, the application of simplified CDD standards (FATF 2025a). The FATF encouraged the application of simplified CDD standards in Interpretative Note to Recommendation 10, which states "there are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk the country or by the financial institution, the country should allow and encourage its financial institutions to apply simplified CDD measures."

Technology Solution and Definition	Best Practices for Use
Metadata Tags Refers to information that describes and provides context about other data, such as its source, creation date, author, format, or classification. Metadata supports data integrity, auditability, and efficient retrieval by recording details about when, how, and by whom customer information was collected or updated.	• Use a clear folder structure to group documents by onboarding stage or category when metadata tagging is not possible • In mature environments, include source details such as device ID or SIM information to confirm data origin
Authoritative Database Verification Refers to validation of customer identity and information against trusted external sources, such as e-KYC registries, national identity databases, passport records, tax authority files, credit bureaus, or telecom SIM registrations. Database verification supplements customer-submitted documents by confirming information against official records.	• Connect to e-KYC registries via secure APIs to retrieve preverified identity profiles, where available • In countries without registries, triangulate multiple authoritative sources (for example, credit bureau, voter registry, and utility bill database) to confirm identity • Document verification results and source references for auditing purposes
Federated Identity Cross-Checks[19] Refers to verifying customer identity using credentials issued by other trusted entities, such as banks, telecoms, insurance companies, or social welfare agencies—especially where no centralized registry exists. This approach relies on interoperability agreements or digital ID frameworks to share verified identity records.	• Establish agreements with sector partners to enable identity verification based on prior KYC records • Ensure privacy rules and consent management are in place before exchanging identity data • Use federated checks to supplement document-based verification, reducing onboarding friction for underserved customers
Document Authentication Technology Refers to automated methods for assessing authenticity of identity documents—such as checking machine-readable zones, embedded barcodes, holograms, watermarks, and issuing authority details—to detect forgery or manipulation.	• Configure systems to detect mismatches issuing authority codes or template inconsistencies • Integrate with OCR to validate document content against intended template • Route suspect documents to manual review using defined escalation procedures
Geolocation and IP Verification Refers to using device- or network-based location information to confirm the geographic consistency of a customer's declared location during onboarding or when conducting transactions. This can help identify anomalies indicating possible identity misuse or fraud.	• Match declared address to device-related location data, (for example, GPS coordinates or IP location) to verify geographic consistency or detect anomalies (while abiding by data privacy or protection rules) • Flag divergences for manual review, particularly for high-risk jurisdictions or sectors • Use location data as an additional risk-rating factor and in monitoring

Source: Original for this publication.

19 In a federated model, multiple independent parties agree to rely on each other's identity proofing and authentication results, supporting CDD when embedded in a trusted digital identity framework with appropriate governance.

3.3.2 Strategies for Verifying and Authenticating Customer Identity and Information

Verifying that customer information is accurate and up to date is a core element of CDD. FIs have traditionally relied on manually reviewing official identity documents, but this process can be slow, prone to errors, and vulnerable to counterfeiting techniques utilized by illicit actors. Digital methods, including digital identity solutions, APIs to centralized registries, address verification, as well as the use of other nondocumentary methods, have been utilized by FIs to enhance identity verification methods and streamline processes. The adoption of digital ID programs varies widely globally, yet its potential is significant. One study estimated that scaling digital onboarding could add 3–13 percent to GDP in some countries by 2030 (UNECA 2024). However, effective use of digital IDs requires identity proofing, deduplication, and secure authentication aligned with an FI's digital maturity.

Table 3.3 outlines several verification technologies and considerations for their use.

TABLE 3.3 • Technology and Use Cases in Verifying Information

Technology Solution and Definition	Key Considerations
Digital Identity Solutions Refers to electronic methods to authenticate and verify the customer during onboarding and throughout the customer life cycle. These solutions can use multiple approaches, such as multifactor authentication, biometric verification, and OCR.	• Choose single, two-factor, or three-factor authentication and select biometric modalities (for example, fingerprint, facial recognition, or iris scan) suited to the onboarding process and available technology • Decide whether processing occurs on the customer's device, the FI's platform, or via a hybrid model, and validate biometrics against government documentation or alternative trusted sources • Pair biometrics with OCR for document checks; adopt multimodal methods combining documentation, biometrics, and third-party validation; and incorporate active or passive liveness detection • Maintain tamper-proof audit logs, bind user credentials to the onboarding device, and require binding upon device change or suspected compromise • Establish mechanisms to validate the integrity, accuracy, and completeness of data from third parties (for example, if an FI outsources aspects of customer onboarding)
Application Programming Interfaces (APIs)[20] Refers to sets of rules and protocols that allow software systems to communicate and exchange data securely. In the context of AML/CFT, APIs are often used to connect an FI's internal systems to external databases and registries for real-time customer verification, information updates, and validation of nondocumentary evidence (for example, government registries and credit bureaus).	• Use APIs to connect with centralized registries, considering the maturity of national infrastructure[21] • Ensure API compatibility with existing systems such as CRMs or transaction monitoring systems • Align APIs with strong authorization and authentication technologies to prevent misuse • Maintain detailed audit logs to verify that all API access and data changes are completed, authorized, and reviewable

20 An API acts as a messenger, enabling communication between two systems. APIs facilitate integration by structuring messages in a consistent format. For example, a sanctions screening tool with an available API will require specific information, such as name, surname, date of birth, and gender, to be sent in the request. The screening system processes this data and returns a structured result to the source system, which is configured to interpret the response. This approach allows disparate systems to connect and exchange information efficiently, as both the sending and receiving systems understand the format of the messages and responses.

21 Examples include Uganda's National Identification and Registration Authority and Nigeria's Bank Verification Number system which enable FIs to perform real-time, API-driven ID verification.

Technology Solution and Definition	Key Considerations
Technology-Enabled Nondocumentary Evidence[22] Refers to methods used to verify a customer without relying solely on physical identity documents. These include direct customer contact, credit bureau or consumer reporting agency checks, public database searches, accessing information in KYC utilities, mobile phone data, and digital footprint analysis (for example, geolocation and social media presence).	• Determine and document the minimum number and type of independent sources needed to verify identity, including documentary and nondocumentary methods • Combine nondocumentary data sources (for example, utility records, telecom data, and geolocation) with AI and machine learning tools to cross-check identity attributes, detect anomalies, and improve match accuracy • Ensure systems can handle onboarding outside normal business hours and across multiple channels, provided customers have access to a suitable device • Consider alternative measures for verification (including, for example, those detailed in the FATF's 2025 Guidance for Financial Inclusion) (FATF 2025a)

Source: Original for this publication.

In addition, many FIs utilize (and screen) a customer's provided e-mail address against internal and third-party databases to identify indications of fraud and illicit activity.

3.3.2.1 Using Technology and Transaction Limits to Apply Simplified Measures and Promote Financial Inclusion

The use of technology in enhancing identity verification can also enable FIs to adopt SDD in lower-risk scenarios. In several jurisdictions—where permitted by local law and regulation—FIs have adopted SDD while adding other controls, such as transaction limits, to minimize risk exposure while promoting financial inclusion. Starting in 2021, the FATF examined the unintended consequences of misapplication of FATF Standards including those on financial inclusion. This led to several revisions (in February 2025) to the FATF recommendations to not only allow but also to "encourage simplified measures in lower risk scenarios" (FATF 2025b). Some private sector actors have found that "with the appropriate controls in place, non-face-to-face customer engagement may be a standard, or even lower-risk engagement channel and can serve as a powerful enabler for financial inclusion" (The Wolfsberg Group 2022, 3). The FATF also acknowledged this by revising the Interpretative Note of Recommendation 10, clarifying that higher risks are present only in non-face-to-face business relationships or transactions "where appropriate risk mitigation measures have not been implemented," emphasizing the responsibility of FIs to implement risk-based controls that consider inherent risks and the capabilities of technology (FATF 2025c). The adjacent case study highlights an approach adopted in Mexico and the corresponding practices adopted by the financial services industry.

22 Previous verification methods highlighted opportunities to use reliable sources to confirm provided information. However, in some regions, centralized and reliable data sources may not be available, or the documentation provided may not be trustworthy. While verification against centralized registries is considered a form of nondocumentary verification since no physical document is presented, this section focuses on the use of technology to support other forms of nondocumentary evidence and outlines good practices for implementing such solutions.

CASE STUDY • Mexico's Tiered Account Framework for Simplified Measures

In 2011, Mexico amended its AML/CFT regulations to introduce four levels of account relationships with progressively stricter CDD requirements and higher transaction limits.

These account types include:

- LEVEL 1 (N1): Requires only full name and date of birth for basic, nontransactional accounts
- LEVEL 2 (N2): Requires additional address and an ID for accounts with limited transactions
- LEVEL 3 (N3): Requires additional address verification, phone, and email for higher transaction volumes
- LEVEL 4 (N4): Requires full CDD for standard accounts with no limits

These types align with a corresponding limit on the total value in the account (of approximately the equivalent of $750 for N1, $3000 for N2, $10,000 for N3, and no limits for N4). As a result, Mexico's banks adjusted onboarding processes to match each tier's requirements. N1 and N2 accounts could be opened with simplified documentation, often remotely, while N3 and N4 required full verification, including beneficial ownership checks for legal persons. As a control, Mexican banks-imposed limits on the volume of transactions permitted in certain accounts unless an increasing level of due diligence would be conducted.

Source: Faz, 2013, and an FI interviewed by IFC.

3.3.2.2 Methods for Verifying Customer Location (or Geolocation)

Verifying customer location serves as an important control since individuals may attempt to open or later access accounts from higher-risk or sanctioned jurisdictions. FIs can leverage several technologies to facilitate address and location verification. For example, telecommunication systems play a role in collecting and verifying address information, especially in regions with underdeveloped postal systems or high rates of urban migration. These tools can be particularly valuable in digital onboarding environments, where face-to-face verification is limited or absent.

Table 3.4 provides an overview of location verification technologies and key considerations for use.

TABLE 3.4 • Technology and Use Cases in Geolocation

Technology Solution and Definition	Best Practices for Use and Key Considerations
SIM Registration and Geolocation Refers to the integration of an FI's systems with telecom subscriber records and device geolocation, which is useful for address and location validation.	• Use subscriber ID, device location, and telecom records to confirm address • Combine with biometric or telecom data to strengthen onboarding accuracy • Apply geofencing to block or flag activity from sanctioned jurisdictions • Ensure compliance with telecom regulations and data privacy laws
Mobile KYC and AML Tools Refers to tools that analyze telecom databases and device data for address triangulation, device consistency, and fraud detection.	• Cross-validate location using GPS, cell tower, and IP data • Apply geotagging for address verification and transaction compliance • Flag anomalies such as multiple accounts per device or sudden shifts in usage • Embed checks in both onboarding and ongoing monitoring

Technology Solution and Definition	Best Practices for Use and Key Considerations
Advanced Analytics Refers to advanced analytics applied to device, network, and transaction logs to detect anomalies.	• Identify improbable behaviors (for example, rapid logins from multiple jurisdictions) • Integrate multiple verification modalities (for example, GPS, IP, or subscriber data) • Monitor for anomalies (for example, location mismatches or repeated login attempts from high-risk regions or jurisdictions)

Source: Original for this publication.

3.3.3 Strategies for Identifying and Verifying Beneficial Owners of Legal Persons

Criminals often use complex and opaque ownership structures to conceal their activities, making it difficult for FIs and law enforcement to identify the individuals who ultimately control legal persons. While FATF Recommendation 24 (and the corresponding Interpretative Note to Recommendation 24) encourages the creation of beneficial ownership registries (or alternative mechanisms "on the basis of risk, context, and materiality"), global implementation remains uneven, and registry data can be difficult to access or validate (FATF 2022a). To identify beneficial owners of legal persons, many FIs still rely on manual records, face high costs to integrate data, and struggle to link entities. However, there are several use cases for technology and analytics to enable faster, more accurate identification of ownership and mapping of complex relationships.

Table 3.5 provides an overview of technology that can assist in verifying the UBOs of legal persons and key considerations for use.

TABLE 3.5 • Technology and Key Considerations for Identifying and Verifying UBOs

Technology Solution and Definition	Best Practices for Use
Automated Forms and Excel-Based Mapping Refers to the use of spreadsheets to build relationship trees based on available data, with each row capturing a single relationship between a source (parent) and a target (child). Pivot tables can then be used to display the layers of relationships between various parents and children.	• Consider including additional attributes, such as relationship types (for example, PEPs), to provide investigators with enhanced visualization and context • If using Excel-based solutions, consider formulas to identify relationships, including ownership percentages • Color coding and conditional formatting can be used to highlight specific relationship types, such as ownership above a certain threshold or connections to PEPs
Integration with Government-Backed and Commercial Registries Refers to connecting to official registries, commercial databases, or open-source data to cross-check declared ownership information against authoritative records.	• Identify relevant national registries and commercial aggregators and access them (such as via APIs or bulk downloads) • Normalize registry information into a consistent format, resolve entities against internal records, and tag with source • Schedule regular data refreshes to detect ownership changes and trigger alerts for potential changes to risk rating

Technology Solution and Definition	Best Practices for Use
Advanced Entity Resolution and Network Analytics Refers to the use of graph databases and link analysis to map relationships between legal persons, shareholders, and directors across jurisdictions, revealing hidden ownership structures.	• Match and merge duplicate or variant entries across registries and data sources to create a single, accurate profile of each legal person or individual • Use graph or network analysis to visualize multilayered relationships and trace indirect or hidden control to the true UBO • Identify links to sanctioned parties, PEPs, or adverse media subjects within ownership networks

Source: Original for this publication.

3.3.4 Strategies for Applying a Dynamic Customer Risk Rating

Across the financial services industry, practices for risk rating customers have evolved from a static, one-time assessment at onboarding to a rating that changes over time.[23] This practice, known as "dynamic customer risk rating," is due largely to technology that allows FIs to analyze customer data and transactions as they occur. Many FIs use automated systems to segment customers by geography, product, and transaction type, drawing on both internal and external data that reassigns customer risk ratings on an ongoing or periodic (for example, monthly) basis. More advanced FIs use machine learning for dynamic risk ratings, peer group analysis, and real-time anomaly detection. Many FIs have found that in shifting to a risk-rating approach that places greater emphasis on behavior, customers often exhibit less risky activity than initially anticipated at onboarding, leading to lower risk scores over time and better aligning due diligence measures to actual risk.

Table 3.6 defines five stages of control maturity for ongoing customer risk rating.[24]

TABLE 3.6 • Control Maturity of Ongoing Risk Rating

Basic	Fragmented	Managed	Integrated	Agile
Customer risk ratings are not updated after initial onboarding.	Customer risk ratings are updated periodically but based on static data factors, so the risk remains constant after the periodic review.	Customer risk rating occurs after the periodic reviews, with EDD triggered if new high-risk factors are identified.	Customer risk ratings are updated as factors are updated or when new information (for example, transaction activity) results in a change to the customer's risk profile; typically updated at least monthly.	Customer risk rating is perpetual (updated daily, weekly, or twice-per month), with the customer record continually updated to reflect the latest risk profile, based on internal and external factors.

Source: Original for this publication.

23 Customer risk rating (also referred to as customer risk profiling) is the process by which an FI assesses the level of ML/TF or other financial crime risk posed by a customer after evaluating several factors (for example, the customer's geographic location or products used) to assign a risk rating (for example, low, medium, or high). Ratings guide the depth of due diligence at onboarding and the depth and frequency of ongoing monitoring during the customer relationship.

24 Refer to Appendix B, "Control Maturity Matrix" for additional information on control maturity.

The ability to move to ongoing customer risk rating first relies on a foundational methodology for assigning a risk profile. Table 3.7 provides information on the components that comprise a typical customer risk rating methodology and key considerations for FIs.

TABLE 3.7 • Typical Components of a Customer Risk Rating Methodology

Key Component	Key Considerations
Risk Factors (also known as Variables) Refers to the attributes gathered through CDD that can be used to assess risk factors related to customers, products and services, channels, and geographies, such as geographic profile, peer group (for example, PEPs), industry segmentation, entity type, expected or actual transaction types and geographies, results of adverse media screening, and any investigations or SAR or STR filings. For example, a risk rating methodology may consider customer type, geography, product, delivery channel, and expected activity.	• Common risk factors include customer type (for example, individual vs. legal person), geography, industry or sector, products or services used, delivery channel, or expected transactional behavior • Ongoing risk rating typically considers actual transactional behavior and presence of SARs or STRs • Multiple variables may be needed to assess one factor. For example, geography risk may need to consider residence and location of transactions • The rating for risk factors or variables relies on underlying risk rating methodologies (for example, a risk rating assigned to individual products, occupation, or industry) • Methodologies typically involve an "automatic high risk" overlay (such as for PEPs), but FIs may apply segmentation within (for example, high-risk vs. low-risk PEPs), with tiered due diligence or monitoring requirements
Scales Refers to the measures to translate qualitative and quantitative information into a consistent risk rating or classification. Scales are a numerical value, typically 1–3, 1–5, or 0–100), with lower scores generally reflecting lower risk. For example, a risk rating methodology may assign a qualitative rating of Low, Medium, High, or Very High, assigning a numerical value of 1, 2, 3, or 4, respectively.	• Use transparent scoring scales (numeric, categorical, or hybrid) that are applied consistently across all customers • Required information may be unavailable or not captured. Default values are often used in these cases, typically defaulting to higher scores as a precaution • Document how scores are assigned and weighted to support auditability and regulatory review
Weights Refers to the measures to highlight the relative importance or influence assigned to each risk factor when calculating a customer's overall risk rating. For example, a risk rating methodology may assign a weight of 30 percent to customer type, 20 percent to geography, 10 percent to delivery channel, and 40 percent to transactional activity.	• Assign higher weights to factors that pose the greatest ML/TF risk, such as geography or PEP status, and review regularly to ensure they reflect current threats • Base weight assignments on historical case data, industry typologies, and emerging risk trends • Periodically run sample customer profiles through the methodology to confirm that weighted scores produce realistic and consistent risk rating
Aggregation Method Refers to the overall aggregation of the inputs to result in an overall risk rating. For example, a risk rating methodology may assign a risk rating of "high" if the sum of the scores for each risk factor (calculated by multiplying the scales by the weights) reaches a total of 70 or weighted average of 3.5 or greater (on a four-point scale)	• Document aggregation formulas and thresholds clearly to ensure transparency • Use methods that prevent dilution of high-risk factors (e.g., maximum-risk overrides where appropriate) • Validate and test aggregated scores regularly against known risk cases and typologies

Source: Original for this publication.

Technology and analytics provide an opportunity to move beyond assigning a risk rating at the onset of a relationship or only during periodic reviews. Table 3.8 highlights the key components and practical considerations when designing and implementing a dynamic customer risk rating methodology.

TABLE 3.8 • Key Considerations of Dynamic Customer Risk Rating

Component	Key Considerations

Build within Risk Factors	• Group risk factors into clear categories (for example, customer, products or services, distribution channels, and behavioral), scoring each category separately before calculating the overall risk rating
	• Examples within each factor may include the following:
	  ○ Static factors (for example, customer type or complexity)
	  ○ Relationship factors (for example, tenure or target market)
	  ○ Economic factors (for example, industry or occupation)
	  ○ Internal red flags (for example, or SARs/STRs adverse media)
	  ○ PEP-related factors (for example, known close associates)
	• Add new factors as data becomes available (without waiting for a "perfect" dataset)

Standardize the Input Variables	• Use consistent scoring scales (for example, 1–5 or 0–100) for all factors contributing to risk rating and keep a master list • Show category scores visually to highlight higher-risk factors (for example, high transaction volume or operating in high-risk region) even if the overall rating is low or moderate • Validate data sources regularly and train frontline staff to capture accurate data • Ensure accurate and standardized data capture (for example, use dropdowns or codes versus free text)
Set Automatic High-Risk Flags	• Configure rules to instantly flag attributes like adverse media, prohibited industries, or PEP status as high-risk regardless of the aggregate score • Use technology (such as APIs) to centralize and automate rule application
Decide on Missing Data Strategies	• Define and decide in advance what happens when data in the risk factor is missing (for example, defaulting to high-risk if the risk factor is important or reducing the weight if it is less critical) • Trigger alerts if mandatory or regulatory-required data is missing for review and remediation
Define Outputs and Integration	• Ensure outputs are both visual and actionable. The use of dashboards can show customer risk distribution across the FI and by business line, for example • Integrate risk ratings into monitoring and control systems so higher-risk ratings trigger enhanced due diligence automatically
Calibrate and Test the Model	• Calibrate the model using historical cases and typologies to tune and test thresholds and anticipate outcomes before deployment • Conduct scenario testing (for example, increase in transaction volume) to assess the impact of changes in data points • Document the changes stemming from calibration, including the testing conducted, rationale for changes, and test results for audit and regulatory review

Component	Key Considerations
Validate the Model	• Conduct independent validation to confirm the model's accuracy, reliability, and explainability, ensuring it works as intended for all risk factors • Compare predicted risk levels to actual outcomes (for example, flagged cases and regulatory findings) • Periodically revalidate the model and document validation processes, findings, and any adjustments made • Prepare evidence and reporting packages for regulators and auditors showing model performance and validation results • Document changes made to the model and any lessons learned from ongoing monitoring testing
Add Behavioral Analytics	• Create baselines for transaction patterns, monitor changes over time, and adjust risk rating when actual activity shifts • Compare customers to peer groups to spot unusual activity (known as "clustering") while also identifying less risky behavior that leads to lower risk ratings • Feed alerts from transaction monitoring systems (or other relevant systems) into the customer risk rating system to refine customer risk ratings

Source: Original for this publication.

The results of the risk rating process determine both the level of CDD and the intensity of ongoing due diligence. Ongoing due diligence enables an FI's understanding of the customer to remain current and provides the ability to determine if the customer's transactional profile continues to reflect actual behavior. The following sections provide strategies for improving the effectiveness and efficiency of ongoing due diligence.

3.3.5 Strategies for Improving Ongoing Due Diligence

To address ongoing due diligence requirements, FIs have traditionally relied on periodic reviews of customer information (with frequency determined using a risk-based approach). While this remains common practice globally, many FIs are shifting toward near-real-time approaches that continuously monitor and update customer information instead of relying on fixed periodic review. This evolving approach is known as perpetual KYC (or pKYC), and it further enables FIs to maintain dynamic, real-time views of the risk presented by a customer and their activity.

Table 3.9 outlines several phases in the maturity of ongoing due diligence programs.

TABLE 3.9 • Industry Approaches to Managing Ongoing Due Diligence

Periodic Reviews	Trigger-Event-Based KYC	Hybrid pKYC	Fully Automated pKYC
KYC updates are conducted at fixed intervals, with off-cycle updates triggered only by major events. Data collection is manual, siloed, and prone to backlogs, leaving long gaps where changes in customer risk go undetected.	Some automation is introduced, with alerts generated when specific triggers occur, such as sanctions hits or unusual transactions. Most customer files are still updated on a scheduled basis, limiting responses to emerging risks.	Continuous monitoring is applied to high-risk segments, while lower-risk customers remain on periodic review cycles. APIs, external data feeds, and machine learning are used to detect anomalies and initiate event-driven reviews.	All customers are monitored in near-real time, with automated risk rating and workflow routing for exceptions. Internal and external data sources are fully integrated, enabling proactive detection and rapid response to changes in risk profiles.

Source: Original for this publication.

The following sections offer several practices and strategies for FIs looking to conduct more efficient periodic or trigger-event-based ongoing due diligence as well as those in the process of transitioning to fully automated pKYC systems.

3.3.5.1 Practices for Improving Periodic and Trigger-Event-Based Updates

The historical industry practice has been to review information for most customers at fixed intervals and during trigger events (that is, a risk-relevant information update, such as an adverse media alert) to conduct ongoing due diligence.[25] However, many FIs face a challenge in keeping customer information complete, accurate, and updated within established time constraints, often resulting in backlogs. By leveraging modern technology and analytics, FIs can make periodic and trigger event-based KYC more accurate, efficient, and responsive, even without fully transitioning to pKYC (The Wolfsberg Group 2022).

Table 3.10 offers several practices for improving ongoing due diligence.

TABLE 3.10 • Key Considerations in Improving Ongoing Due Diligence

Practice	Key Considerations
Automate Data Collection and Refresh Systems	• Connect internal systems and external sources (for example, corporate registries, sanctions lists, adverse media, and transaction monitoring) via APIs • Schedule automated data pulls ahead of periodic reviews to ensure analysts work with the most current information
Enhance Trigger Event Detection	• Expand triggers beyond regulatory minimums to include operational risk indicators, such as sudden changes in payment counterparties • Use analytics and machine learning to identify subtle changes in customer behavior, ownership, or geographic footprint that may not be caught by basic rules
Prioritize High-Risk Segments and Utilize Dynamic Risk Rating	• Apply a risk-based approach to determine customer segments that require more frequent or deeper reviews (such as classifying lower-level PEPs vs. more senior PEPs) • Use risk rating models to dynamically adjust the review frequency based on evolving risk (as described in greater detail in the prior section on dynamic risk rating)
Integrate KYC with Transaction Monitoring	• Link KYC data to transaction monitoring systems so alerts automatically prompt a profile refresh, enabling trigger event reviews to be informed by both static customer data and real-time activity
Improve Data Quality at Source	• Train frontline staff to capture complete and accurate customer information • Include performance incentives in compensation tied to data completeness and quality metrics (for all staff but priority for senior management overseeing a business unit)
Use Dashboards for Review Management	• Implement dashboards that track review status, outstanding data gaps, and trigger event-based alerts • Prioritize updates for higher-risk relationships
Document and Audit Changes	• Maintain clear audit trails of data updates, triggers, and review decisions • Use workflow tools to ensure consistent handling of exceptions

Source: Original for this publication.

25 The minimum frequency for periodic reviews can vary depending on jurisdictional requirements and customer risk segment. In practice, IFC has observed that most FIs conduct reviews annually for high-risk customers. Medium-risk legal entities are typically reviewed every two years, while medium-risk individuals are reviewed every three years. For low-risk customers, reviews are carried out less frequently, generally every three years for legal entities and every five to seven years for individuals. Some jurisdictions permit less frequent or trigger-event-only refreshes for low-risk individual customers.

3.3.5.2 *Shifting to Perpetual KYC (pKYC)*

pKYC is a continuous, near-real-time approach to ongoing due diligence. Unlike traditional CDD, which is performed at onboarding and revisited at fixed intervals or in response to specific triggers, pKYC uses automated data feeds, APIs, machine learning, and analytics to update customer profiles as new information emerges. This keeps risk ratings current and enables faster detection of material changes.

Applying pKYC offers several notable benefits, including:

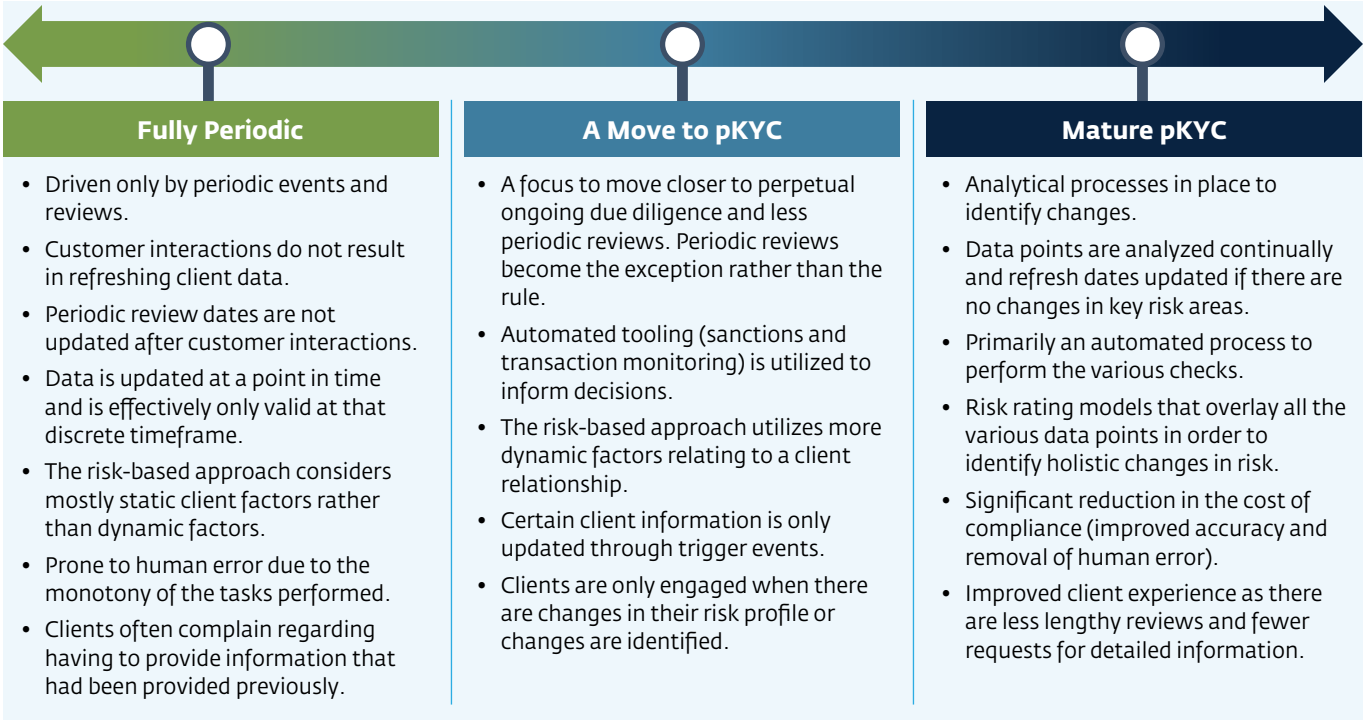
- **Real-time risk awareness** to detect changes in customer risk ratings immediately
- Enhanced ability **to meet emerging regulatory** expectations toward dynamic risk management
- Operational efficiency **in reducing periodic review backlogs** and focusing resources on high risks; and
- Enhanced **customer experience** by minimizing repeated requests for information.

However, there are multiple challenges in shifting to pKYC, including:

- **Data quality and availability** as pKYC relies on timely and accurate internal and external data
- **Integration and scalability of systems**, which must handle large volumes of data
- **Cost and complexity**, as technology, data subscriptions, and integration can be expensive
- **Data privacy**, as real-time access must comply with privacy laws; and
- **Regulatory acceptance**, as regulators may still expect continued periodic reviews.

In practice, many FIs blend elements of pKYC with periodic refresh. Figure 3.1 provides an overview of the pKYC maturity continuum, illustrating where an FI's current practices may fall.

FIGURE 3.1 • Shift to Perpetual KYC



Source: Original for this publication.

Table 3.11 offers several key considerations and best practices—including opportunities for technology and analytics—to support FIs in their transition to pKYC.

TABLE 3.11 • Key Considerations for Information in pKYC

Area	Key Considerations
Information Capture and Storage	• Define field-level data requirements to ensure consistency, accuracy, and completeness of customer information • Tailor onboarding data capture for specific entity types to better identify and evaluate risk • Define storage techniques (for example, whether data is stored at source or in a combined data lake from source systems) • Cleanse data at its source and establish and follow data governance protocols (to enable consistent use of data and reconciliation between source data and downstream systems) • Incorporate trigger events (for example, new products or ownership changes) into ongoing due diligence processes to keep data updated, replacing strictly periodic review cycles • Automate repetitive processes via integrated customer portals and reduce manual interventions • Embed risk-based triggers in workflows to highlight high-risk industries or suspicious activity patterns
Information Access	• Default to digital-first data collection, leveraging e-KYC solutions for most onboarding scenarios • Centralize and govern data to reduce duplication, ensure uniformity, and enable automated access across systems • Validate against authoritative sources (golden sources) before requesting documentation from the customer • Modernize data pipelines by shifting from batch imports to API-driven real-time integrations • Use OCR and digitization tools for document ingestion (for example, ID verification or trade finance documentation) • Store data at its source and allow controlled, periodic system access aligned with risk relevance
Information Analysis	• Maintain dynamic risk ratings that update as underlying data changes • Focus workflows on high-risk cases, routing them to specialized review queues • Track changes in ratings over time for trend detection and emerging risk identification • Consider integrating information obtained from other risk domains (such as fraud) for a holistic view of customer risk • Integrate different teams within a single KYC workflow (albeit with data access rights, as needed) to enable them to integrate insights from different areas (for example, fraud and AML) into a single customer profile • Leverage data visualization tools to quickly detect anomalies and validate model outputs • Adopt machine learning and AI to segment customers, reduce false alerts, and improve decision-making accuracy • Deploy RPA to aggregate data (particularly during enhanced due diligence and alert reviews)

Source: Original for this publication.

4

Practices for Improving Name and Transaction Screening

Chapter 4 builds on previous chapters by further defining opportunities for technology and analytics as well as best practices for leveraging them within name and transaction screening. Screening not only enables compliance with legal and regulatory requirements tied to economic sanctions but also serves as a control to prevent designated criminals or terrorists from accessing an FI's products and services. Screening can also strengthen risk mitigation by improving an FI's knowledge of its customers (for example, identifying PEPs) and supports meeting the expectations of international partners, such as correspondent banks, who may be subject to different legal obligations. Despite its importance, implementing effective screening remains challenging as FIs must process large volumes of data and sift through high numbers of false positives that require significant time and resources to manage.

Among other topics, Chapter 4 will address the following:

- What are the main challenges in conducting effective name and transaction screening?
- What are the capabilities of technology and software solutions available?
- What are sanctions, PEP, and adverse media screening, and their purpose?
- What are the typical scope, frequency, and methods used for screening?
- What functions should automated systems perform and when is manual screening appropriate?
- What are the strategies for reducing false positives?
- What are the best practices for using "fuzzy logic" matching and sensitivity scores?
- What are the practices for improving the underlying data quality?
- What is "alert suppression" and how are FI's utilizing it?
- What are the practices for monitoring the effectiveness of screening?
- What are best practices for program governance and testing?

4.1 Capabilities of Technology & Analytics in Addressing Challenges

FIs of all sizes and maturity face challenges in conducting effective screening. These include the following:

- **Resource-intensive manual processes:** In areas such as adverse media or PEP screening (particularly where reliable lists of PEPs are unavailable), data collection may be manual or incomplete yet still critical for CDD or screening purposes
- **Limited data availability:** Public sources and even some commercial databases may lack reliable or complete information. In many jurisdictions globally, for instance, accurate and up-to-date lists of domestic PEPs are not readily available. In addition, individuals that are family members or close associates of PEPs—or legal entities that are owned or controlled by PEPs, their family members, or close associates—can be difficult to identify through traditional channels
- **High volume of false positives:** Screening often generates large numbers of false positive alerts, many of which require manual review. IFC has seen positive match rates sometimes fall below 0.1 percent of alerts generated
- **Impact of a false negative or incorrect alert resolution:** Failure to identify or properly resolve an alert linked to a sanctioned individual, entity, or jurisdiction can expose an FI to severe legal and regulatory penalties, as well as reputational damage and potential loss of correspondent banking or bank-partner relationships
- **Need for rapid responses:** Screening often requires a real-time response when onboarding customers (particularly in-person at a branch location) or in cross-border payment processing, where delays may disrupt transactions and adversely affect the customer relationship

Technology and analytics can strengthen name and transaction screening by enabling FIs to conduct:

- **Earlier detection of risks** within CDD and when conducting cross-border payments
- Realtime matching **to reduce the risk of delayed payments** through correspondent banks
- Real-time matching **to block or freeze cross-border transactions** with sanctioned parties
- More accurate **matching of customer data** to identify potential hits and limit false positives
- Fuzzy logic **to detect name variations** and reduce false positives
- Alias detection to uncover **hidden identities and connections**
- **Batch screening** of complete customer datasets on an ongoing basis against deltas in the screening lists
- Sentiment analysis to **identify more relevant adverse media** and assess potential risks
- Screening **across multiple jurisdictions** and keeping lists updated; and
- Scalable processing **to handle large data volumes** without compromising accuracy.

There are software solutions and techniques that FIs can use to strengthen screening effectiveness. These include automated screening tools, enhancing governance and oversight, refining name-matching algorithms to improve match quality, and utilizing machine learning techniques to reduce alert volume while preserving effectiveness. The subsequent sections offer insight into the foundational concepts before considering strategies to utilize technology and analytics to address key challenges.

4.2 Foundational Concepts in Name and Transaction Screening

Before highlighting techniques to overcome these challenges, this Good Practice Note first provides foundational information on name and transaction screening. While this section provides useful background information that can benefit experienced compliance professionals, readers that are familiar with these concepts and focused primarily on strategies to overcome challenges may proceed directly to Section 4.3, "Techniques for Optimizing Name and Transaction Screening."

4.2.1 Defining Name Screening and Transaction Screening

Name screening and transaction screening refer to the processes utilized to screen the names of relevant individuals (including customers, employees, and counterparties), legal persons (including their beneficial owners), and transactions (particularly cross-border transactions) against official or other relevant lists. For the purposes of this Good Practice Note, screening is considered inclusive of sanctions screening (for example, official lists of sanctioned individuals, entities, and jurisdictions that are maintained by national or international authorities), watchlist screening (for example, lists of PEPs or internal exclusion lists), and adverse media screening (that is, reviewing public sources for negative news indicative of financial crime risk).

The primary objectives of screening are to comply with applicable laws and regulations (which may obligate an FI to reject or block certain customers or transactions), meet the standards of correspondent banks (which may impose requirements to comply with regulations in their home jurisdiction and be forced to freeze or block certain payments initiated by the originating bank), and to support the FI's broader risk management program (by identifying high-risk customers and transactions and applying enhanced due diligence).

4.2.2 Types of Screening

FIs conduct several types of screening with the exact scope dependent on their legal and regulatory obligations, responsibilities to counterparties, and risk profiles. Table 4.1 summarizes the main types of screening discussed in this Good Practice Note and the techniques commonly used by FIs to conduct screening.

TABLE 4.1 • Types of Screening and Techniques to Conduct Screening

Type of Screening and Purpose	Techniques to Conduct Screening	Key Considerations
United Nations Targeted Financial Sanctions (TF and PF) Intended to identify individuals, entities, and groups specifically designated under UN Security Council Resolutions for the purposes of identifying and freezing assets related to the prevention and suppression of terrorism financing (TF) and proliferation of weapons of mass destruction. The goal is to prevent the risk of terrorist financing, proliferation financing (PF), and other threats to peace and security.	• Checking names against official lists of sanctioned individuals and entities designed by the UN Security Council (to comply with UN Resolutions 1267 and 1373 as well as successor resolutions) • Batch screening or real-time API checks against consolidated sanctions / targeted financial sanctions databases • Use of fuzzy matching algorithms and sensitivity scores to detect variations in automated platforms • Entity resolution to link aliases and alternate spellings (to form a single profile of an entity) • Real-time screening of transactions, counterparties, and intermediaries involved in a transaction • Screening of UBOs, directors (for legal entities) and related parties	• TFS are applied in connection with FATF Recommendations 6 and 7 and require FATF member countries to "freeze, without delay" the funds or other assets of individuals or entities designated for TF or PF purposes • TFS lists are typically binding under international law and focus on asset-freeze obligations • Immediate freezing and reporting to authorities is mandatory when a positive match is confirmed
National and Supranational Financial Sanctions Intended to identify individuals, entities, or jurisdictions, sectors, or activities subject to sanctions issued by national authorities or supranational bodies. The goal is to comply with applicable laws and manage risks (such as of disrupted payments, regulatory fines, reputational damage, or sanctions circumvention).	• Checking names against official government lists of individuals and entities designed by the jurisdictions in which the FI operates • Batch screening and continuous API checks against consolidated sanctions or TFS databases • Use of fuzzy matching algorithms and sensitivity scores to detect variations in automated platforms • Entity resolution to link aliases and alternate spellings (to form a single profile of an entity) • Real-time screening of transactions, counterparties, and intermediaries involved in a transaction	• An example of supranational sanctions are the EU's Consolidated List of Financial Sanctions • Examples of national sanctions lists are the United States OFAC's Specially Designated Nationals and Blocked Persons List and the United Kingdom Sanctions List • Covers broader prohibitions than TFS—may target entire jurisdictions, sectors, or industries • Applicability depends on the FI's operational footprint and any obligations to third parties

Type of Screening and Purpose	Techniques to Conduct Screening	Key Considerations
Official or Internal Watchlist Intended to identify individuals or entities appearing on other official watchlists (such as Interpol notices) or on internal watchlists maintained by the FI (for example, customers exited for financial crime). While not necessarily binding, the goal is to identify criminals, suspects (and their associates), and customers previously exited by the FI due to financial crime.	• Screening against official nonsanctions lists (for example, law enforcement bulletins) • May require an FI to establish a list themselves or keep records of requests (as an official national watchlist may not exist) • Screening against internal watchlists (which may apply group-wide for FIs with affiliates, parent companies, or subsidiaries) • Use of entity resolution (to form a single profile of an entity) to consolidate records	• Not mandated by law but utilized to align with internal risk appetite or contractual or business requirements • Helps prevent onboarding or reengagement with known illicit actors, individuals, or entities previously exited due to financial crime concerns
PEPs and Close Associates Intended to identify PEPs, their close associates or family members, and entities owned or controlled by PEPs to mitigate inherent risks of corruption, bribery, political influence, and regulatory noncompliance.	• Manually searching government or PEP lists (often utilizing third-party databases or government-issued lists) • Screening against both lists of local PEPs and global databases (to identify foreign PEPs) • Relationship mapping (to identify relatives and close associates of PEPs)	• PEP identification is foundational to FATF Recommendation 12, which requires FIs "to have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP" • PEPs can use family members, close associates, or layered ownership to obscure involvement
Adverse Media Intended to identify negative media that is indicative of heightened financial crime risk, such as credible links to fraud, corruption, terrorism, or other illicit activities.	• Conducting internet searches, reviewing local language media articles, and utilizing third-party databases to identify media indicative of financial crime risks • Continuous media monitoring using keyword searches and sentiment analysis (to focus on material adverse media alerts)	• Media may mention associates, shell companies, or related entities; screening should link adverse news to all relevant parties • Sources should be reputable, verified, and periodically reviewed to reduce false positives and misinformation risk

Source: Original for this publication.

In the cases above, FIs should consider whether the outcomes materially impact the financial crime risk and be sensitive to risks of financial exclusion and derisking or debanking. With respect to sanctions, FIs should be cognizant that individuals and legal persons could be subject to sanctions but not listed on an official sanctions list. For example, multiple sanctions regimes consider a legal person to be sanctioned if it is at least 50 percent owned by a sanctioned individual, even if it is not directly listed.

4.2.3 Scope, Frequency, and Screening Methods

Name screening on account opening or as part of ongoing screening of the customer database involves comparing customer attributes (typically name, surname, date of birth, and nationality, at a minimum) against various data sources to identify matches. These matches may be exact, where the customer's details are identical to those in the data source, or partial (also referred to as "fuzzy"), where the captured details are highly similar or correlated to the information in the data source but not an exact match. Transaction screening focuses on reviewing the details of cross-border transactions, such as originator and beneficiary names, account numbers, and jurisdictions, against sanctions lists and other watchlists to detect prohibited or high-risk transfers.

FIs typically face the following questions when designing a screening program:

- Which data sources and lists should be utilized for screening?
- Who and what should be screened (for example, customers only vs. UBOs, related parties, or transaction attributes)?
- When should screening occur (for example, during onboarding) and how frequently?
- How should the matching be performed?
- How should matches be reviewed?
- What should be done if a positive match is identified?

Table 4.2 provides a framework answering these questions, among others.

TABLE 4.2 • Designing Key Process Steps in Screening

#	Key Question	Key Process Steps and Considerations

1	**What data should be utilized for screening?**	• Determine the appropriate data sources for screening, including sanctions lists, adverse media sources, PEP lists, and internal databases
		• Ensure all data sources (including customer information such as UBOs) are current, comprehensive, and aligned with the FI's risk appetite and risk profile
		• Consider minimum jurisdictional requirements, such as:
		  ○ The United Nations Sanctions List (required in all United Nations member states)
		  ○ Local or national sanctions lists
		  ○ Regional or supranational lists (if applicable)
		  ○ Local or national export controls lists (if applicable)
		  ○ Currency-specific lists (for example, for foreign currency transactions)
		• Consider the requirements of correspondent banks and bank partners (who may have their own internal lists and risk appetite or be required to follow certain lists)
		• Consider additional sources of information, such as:
		  ○ Adverse media searches
		  ○ Lists of PEPs (from either government registers or commercial providers)
		  ○ Lists of dual-use goods (that is, goods that can be used for military purposes)
		• For financial groups operating in multiple jurisdictions, determine the strictest applicable standard and document any jurisdiction-specific requirements
		• If using a third-party vendor, determine which lists should be screened (including whether certain lists can be turned off)

#	Key Question	Key Process Steps and Considerations

2	**Who (or what) should be screened?**	• Define the population to be screened, considering regulatory requirements and the following:[26]
		  ○ Direct customers with an established account relationship
		  ○ Nonaccount customers (for example, walk-in customers cashing remittances)
		  ○ UBOs and controlling parties of all direct customers
		  ○ Related parties (such as intermediary banks)
		  ○ Third parties (including vendors, suppliers, and partners)
		  ○ Employees (with a particular focus on those in sensitive roles)
		  ○ Counterparties in payments or commercial transactions with the FI's customers
		  ○ Key information related to the transaction/payment

3	**When should screening occur and how frequently should it occur?**	• Determine the timing of screening, with the following as an industry standard:
		  ○ During the onboarding of new customers, employees, or third parties
		  ○ At periodic intervals (for example, during periodic KYC refreshes or trigger-events)
		  ○ Through batch processes (typically nightly, weekly, or monthly)[27]
		  ○ Upon changes to in-scope sanctions or other watchlists
		  ○ When triggered by specific events (such as a change in ownership)
		  ○ For payments, typically on a real-time or near-real-time basis at initiation, prior to settlement, and/or receipt
		• Consider the FI's risk profile, risk appetite, legal and regulatory obligations, requirements of key partners, and estimated impact when determining frequency

4	**How should the matching be performed?**	• Determine the appropriate methods and technologies for screening, considering the following:
		  ○ Automated vs. manual screening
		  ○ Real-time vs. batch processing
		  ○ Utilization of advanced filtering techniques and parallel processing
		• Ensure the chosen approach can handle large datasets and is designed to prioritize high-risk cases
		• Consider the fuzzy logic matching capabilities and set a sensitivity score appropriate for the institution (as detailed in the following sections)

5	**How should matches be reviewed?**	• Establish clear roles and responsibilities for personnel within an FI routinely resolving alerts (for example, a first-line relationship manager vs. a second-line compliance officer) • Develop written desktop procedures outlining how a match should be resolved and what matches may require a second level of review • Include sample-based quality assurance mechanisms and, in higher-risk cases, manager review or clearance to ensure discarded alerts are false positives

26 FIs should be aware that, in the context of sanctions screening, some jurisdictions have determined that any legal person that is 50 percent or more owned by a sanctioned individual is itself considered a sanctioned entity even if that entity is not included on a government list.

27 The industry best practice for banks is nightly batch screening. In some instances, banks may conduct weekly or monthly batch screening (but this frequency is typically offset by ensuring screening within one day of any changes to relevant lists and prior to the issuance of any new product and service, at a minimum). Some NBFIs, particularly those that offer credit products only or deposit accounts with limited payment functionality, conduct screening less frequently (such as quarterly, semesterly, or during periodic refreshes) provided that screening occurs prior to offering any new product.

#	Key Question	Key Process Steps and Considerations
6	**What should be done if a positive match is determined?**	• Follow escalation procedures, including notification to senior compliance staff and, where necessary, the appointed AML officer or equivalent • Freeze or restrict the relevant accounts, transactions, or relationships as required by applicable law or internal policy. FATF Recommendations 6 and 7 require assets related to targeted United Nations financial sanctions for preventing TF and PF be frozen "without delay," interpreted as within 24 hours • Notify relevant authorities in accordance with legal and regulatory obligations (typically required between one and ten days, depending on the jurisdiction) • Maintain detailed records of actions taken for audit and regulatory review purposes

Source: Original for this publication.

4.2.4 Alert Types Generated

When an alert is generated, it will ultimately be classified as a true negative, false positive, true positive, or a false negative. Figure 4.1 illustrates and defines these concepts.

FIGURE 4.1 • Defining Types of Screening Results and Their Risks

Subject Being Reviewed	On a Sanction List	Flagged by System	Outcome
Lean Whitaker	✗	✗	True Negative ✓
Rajiv Marlowe	✗	✓	False Positive !
Zara Hightower	✓	✓	True Positive 🚨
Dmitri Kavanagh	✓	✗	False Negative !

- False negatives represent the highest risk, as they occur when the system fails to flag customers, counterparties, and/or transactions on sanctions lists, potentially allowing illicit transactions to proceed. This oversight can lead to severe regulatory penalties, reputational damage, and financial losses
- True positives, while inherently risky, indicate that the system has correctly identified matches, provided that timely reporting and action are taken to prevent financial crimes
- True negatives, which are not flagged by the system, indicate the system's ability to prevent alerts for customers, counterparties, and transactions that do not present relevant risks, thereby maintaining operational efficiency
- False positives, although they may not present a risk to the FI, create a potential resource drain and lead to unnecessary investigations

Source: Original for this publication.

4.2.5 Requirements for Automated Systems

Conducting screening with automated systems requires access to reliable source information (for example, customer information and relevant transaction information) and reliable access to the lists against which the information is going to be screened. This not only requires screening against name-based lists (for example, sanctions or PEP lists) but also against lists linked to transaction attributes, such as jurisdictions, counterparties, vessels, or goods.

Table 4.3 highlights key considerations when performing automated screening.

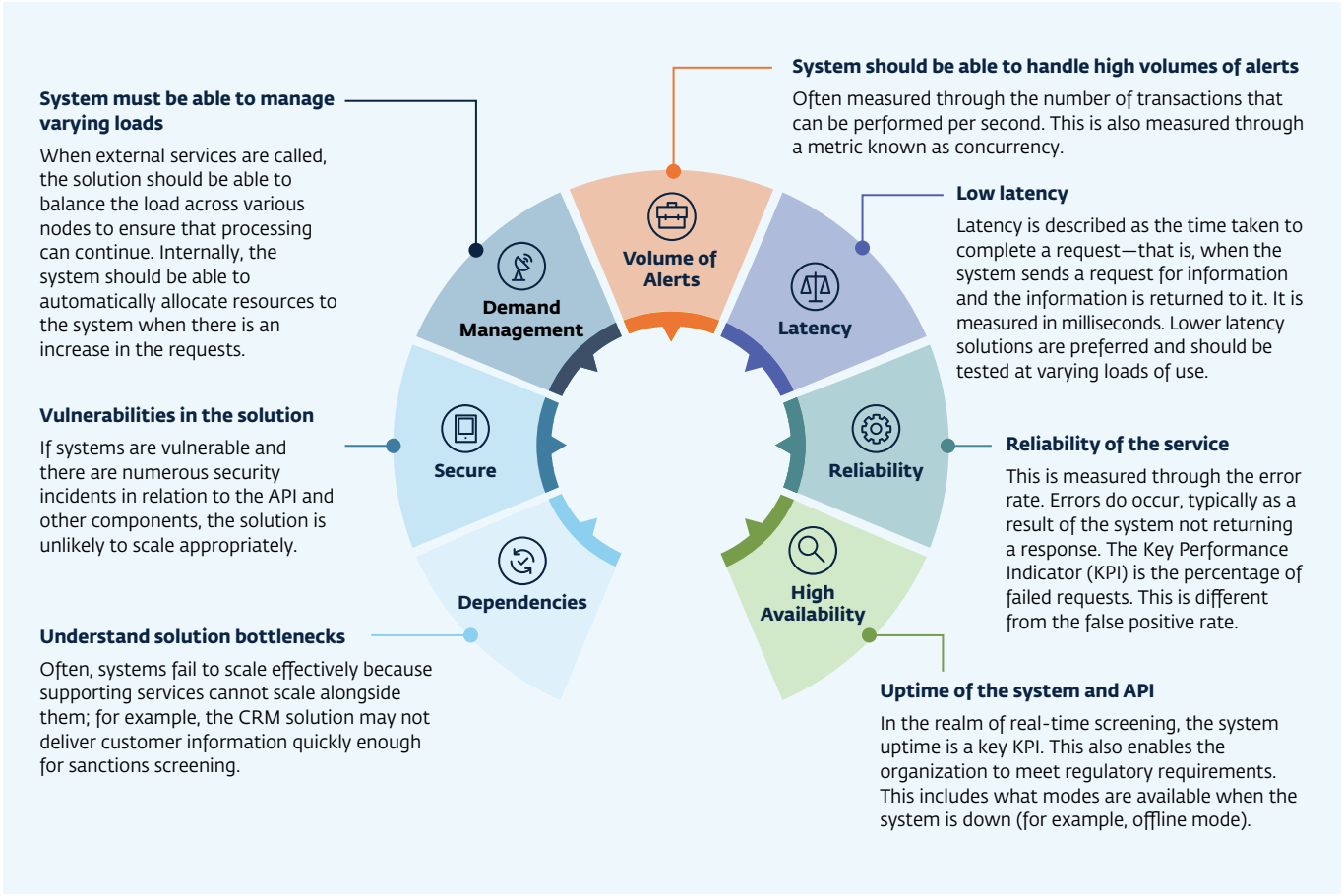
TABLE 4.3 • Key Considerations for Automated Screening Systems

System Attribute	Implementation Considerations	Example Capabilities
Latency Latency refers to the time delay between a user's request of a system and the resulting response. Delays in screening can disrupt customer onboarding and payment processing.	• Use APIs for large datasets; enable caching of results; ensure seamless integration between systems	• Rescreen cached data quickly when lists update • Maintain near-instant lookups for frequently screened parties
Risk-Based Screening Risk-based screening refers to a screening of names and transactions in a manner consistent with the FI's risk-based approach. Risk-based screening supports proportionality and focuses resources on higher-risk transactions.	• Segment payments (for example, cross-border vs. domestic); apply thresholds for alerts; incorporate UBOs in screening	• Apply fuzzy matching algorithms; queue or block high-risk payments until reviewed
Whitelisting Whitelisting refers to the concept of suppressing alerts that appear frequently for the same pattern but have been previously assessed and dismissed. Whitelisting can prevent repeat false positives, improving efficiency without weakening controls.	• Implement suppression rules; maintain audit trail of whitelisted items; review periodically	• Whitelist recurring transactions (for example, remittances); whitelist low-risk product types (for example, local transfers)
Transaction Descriptions Transaction description refers to the system's ability to search for and flag patterns with transactions as opposed to solely the counterparties (to identify risks within payment messages)	• Build keyword dictionaries; screen narratives for prohibited items and destinations; flag unusual terms	• Identify dual-use goods in descriptions; detect hidden sender and receiver names

Source: Original for this publication.

FIs may also consider scalability and the ability of the system to process increasing volumes of data. Figure 4.2 summarizes the key considerations for scalable systems.

FIGURE 4.2 • Scalability Considerations



Source: Original for this publication.

4.2.6 Comparing Manual vs. Automated Screening

Manual screening, once a standard practice, is now largely inadequate due to scalability limits, susceptibility to human error, inability to keep pace with regulatory changes, and the high risk of missing alerts. In emerging markets, challenges such as varied name spellings, honorary titles, and transliteration complicate identity resolution; manual processes can address some nuances but are prone to missed alerts and false matches. Automated systems process large data volumes quickly, reduce missed true positives, and enhance transparency while supporting regulatory requirements, with automated solutions widely available (even to smaller FIs in emerging markets). That said, there may be cases where manual screening can occur for FIs with limited risk profiles and customer operations. Chapter 6 contains several practices for FIs to consider if they must conduct manual screening as part of their operations.

4.3 Techniques for Optimizing Name and Transaction Screening with Technology and Analytics

As previously noted, FIs face many challenges in conducting effective screening, including manual-intensive processes, an abundance of false positives, limitations in the availability of information, and keeping automated systems correctly tuned.

The following sections offer strategies, best practices, and considerations for the following topics.

4.3.1 Strategies for Reducing False Positives

As stated previously, large numbers of false positives remain a key screening challenge for many FIs.

The impact of false positives includes the following:

- **Operational inefficiencies**, as analysts spend excessive time reviewing low-risk cases
- **Processing delays**, as customer onboarding or transactions are held until reviews are completed
- **Dissatisfied customers** who do not understand the reasons for repeated requests for information
- **Heightened risk of errors**, as analyst fatigue can increase the likelihood of oversight or mistakes.

Several technology strategies can be implemented to improve screening outcomes that reduce false positives while avoiding false negatives. These include standardized matching algorithms, entity resolution, alert risk scoring, and fuzzy matching techniques to ensure consistent results. More advanced solutions and techniques, such as AI, NLP, machine learning, contextual analysis, and autonomous decision agents can further enhance review outcomes by increasing the precision of screening processes.[28]

4.3.1.1 Use of Fuzzy Logic Matching Algorithms

Fuzzy logic is a matching technique that identifies potential matches through approximation, rather than requiring exact matches. It is particularly useful for detecting matches when names are misspelled, data quality is poor when entered, information is incomplete (for example, when middle names are not required), words are out of order, or names are spelled using different alphabets or transliterations.

Table 4.4 defines several fuzzy logic matching algorithms, use cases, and examples.

28 Refer to Appendix A for definitions and description of these techniques.

TABLE 4.4 • Defining Types of Fuzzy Logic Matching Algorithms[29]

Technique and Capability	Illustrative Example #1	Illustrative Example #2
Levenshtein Distance Calculates the minimum number of single-character edits (insertions, deletions, or substitutions) needed to turn one name into another. The technique is particularly useful for catching typos, optical character recognition (OCR) errors, or minor spelling differences that can occur in international documents or manual data entry.	A new customer named "Jon Smith" is flagged as possible match to "John Smith" on a PEP list due to a single character difference.	A news article mentions "Sergei Romanov" which generates an alert for "Sergey Romanoff," who is the FI's customer.
Phonetic Matching Uses algorithms (like Soundex or Metaphone) to match names that sound similar but are spelled differently. The technique is particularly useful for international names, transliterations, and cases where names are recorded phonetically.	"Katherine Johnson" is matched to "Catherine Jonson," ensuring pronunciation-based variations are captured.	"Brian O'Neil" and "Bryan O'Neill" are linked, ensuring relevant media is captured despite spelling differences.
Jaro-Winkler Similarity Measures how closely two strings match, giving extra weight to similarities at the beginning of the strings and ignoring spaces or punctuation. The technique is useful for catching differences in company names, abbreviations, or formatting.	"A B C Limited" is matched to "ABC Limited" on a sanctions list, even though the formatting is different.	"Dr. Jane Doe" is matched to "Jane Doe" in a PEP list, ensuring titles or extra spaces do not prevent a match.
Tokenization and Scoring Breaks names or entities into individual components (tokens), compares each part, and generates a composite score to indicate the likelihood of a match. This approach is adaptable, allowing for different sensitivity thresholds for onboarding, transaction monitoring, or periodic reviews.	"ABC Holdings PLC" and "ABC PLC" are scored for similarity in adverse media, ensuring partial matches are not overlooked.	"Maria Teresa Garcia" is matched to "Maria Garcia" in a PEP list, with token scoring accounting for missing or extra names.
Normalization and Transliteration Standardizes data by removing accents, converting all text to a single alphabet, and ignoring case or punctuation. The technique is useful for screening where names may appear in different scripts or with diacritics.[30]	"Mikhail Ivanov" (Latin) is matched to "Михаил Иванов" (Cyrillic) in a PEP list, bridging language barriers.	"François Dupont" in a news article is matched to "Francois Dupont" in the adverse media database, ignoring accents.
Aliases and Variations Leverages databases of known aliases, nicknames, abbreviations, and regional spelling differences to connect entities that might otherwise be missed. This is useful for individuals or legal persons known by multiple names.	"IFC" is linked to "World Bank" in adverse media, capturing stories that use either the parent or subsidiary name.	"Bob" is matched to "Robert" or "Liz" to "Elizabeth" in a PEP database, ensuring informal names are not missed.

Source: Original for this publication.

29 The names in this table were fictionalized to provide illustrative examples and are not intended to reflect any actual individual or legal person.

30 Diacritics are marks added to letters that change their pronunciation or distinguish between similar words or sounds. Common diacritics include accents (´, `, and ^), tildes (˜), umlauts (¨), cedillas (¸), and others.

4.3.1.2 Setting a Sensitivity Score

Fuzzy logic matching algorithms assign a similarity score (for example, 0–100 percent) to potential matches, but only those meeting or exceeding a set threshold (for example, 75 percent) generate alerts. FIs should set these thresholds using a documented, risk-based approach that considers regulatory expectations and the FI's risk profile.[31] Setting a threshold involves assessing customer, product, geographic, and channel risks, reviewing legal requirements, and testing thresholds against historical data to measure the impact on true positives, false positives, and missed matches. The objective is to minimize missed true matches while keeping alert volumes manageable.

Observed practices include the following:

- Applying stricter sensitivity for high-risk customers, products, or jurisdictions (for example, alerting all matches that are 75 percent or greater), and less stringent sensitivity for low-risk, domestic-only relationships (for example, alerting all matches that are 90 percent or greater)
- Using different thresholds for stages of the customer relationship (for example, a lower threshold at onboarding vs. a higher one in overnight batch screening) or for specific products (for example, a lower threshold for cross-border wires)
- Considering vendor-recommended settings (but tuning them to the FI's own profile)
- Requesting input from correspondent banks and bank partners based on their risk appetite
- Conducting regular quality assurance (for example, reviewing a sample of closed alerts)
- Conducting real-time reviews of new analysts' alert decisions at 100 percent for a period of time.

As an example, calibration may show that an 85 percent threshold captures all true matches for high-risk international customers but produces excessive false positives for low-risk domestic customers. A tiered approach—such as 85 percent for high-risk and 90 percent for low-risk—could improve efficiency without compromising detection. However, the rationale, testing process, and results should be documented, with sensitivity scores reviewed at least annually.

4.3.1.3 Suppression of Sanctions or PEP Alerts

FIs can improve efficiency by implementing automated suppression (or "auto closure") processes for low-risk, false-positive matches. This involves configuring screening systems with predefined rules and thresholds that identify alerts meeting specific "safe-to-close" criteria, such as exact matches to internal whitelists, matches to entities located in unrelated jurisdictions, or names with low similarity scores below a set threshold. Alert suppression reduces manual workload, shortens investigation times, and allows staff to focus on higher-risk alerts. However, suppression techniques should be documented, tested, and subject to periodic review, with audit trails maintained for all suppressed alerts.

Table 4.5 outlines example situations where suppression may be justified.

31 The thresholds used in this section are for illustrative purposes only and are not to be viewed as suggestions. FIs should establish a process to determine the threshold based on their risk appetite, observed practices, and expectations from regulators and partners.

TABLE 4.5 • Examples of Suppression Situations

Rule	Description	Example[32]	Control Safeguard
Internal Whitelist Match	Suppress alerts for customers preapproved by compliance.	Longstanding corporate customer with verified beneficial ownership.	Whitelist reviewed quarterly by compliance and audit.
Low Similarity Score	Close alerts below a set match threshold (for example, <70 percent) where no other risk indicators exist.	"John Smith" flagged against "Jon Smythe" with no adverse media.	Threshold tested against historical data to confirm no missed true positives.
Irrelevant Jurisdiction	Close matches to sanctioned entities in jurisdictions with no transaction or business link.	Payment to a local supplier flagged against a sanctioned entity in a distant, unrelated jurisdiction.	Jurisdiction rules reviewed monthly against updated sanctions lists.
Duplicate Alert	Close alerts already reviewed and resolved in the last 90 days.	Repeat match to the same customer name from prior screening cycle.	System crosschecks prior alert ID and closure reason before suppressing.
Known False Positive Pattern	Close alerts matching common names with no adverse media or risk indicators.	"John Smith" flagged with no link to sanctioned individuals.	Pattern list updated monthly based on analyst feedback.

Source: Original for this publication.

Suppression should be implemented with clear governance, documented procedures, and regular validation to check that no true positives are missed. Audit logs should capture the closure reason, rule applied, and system user or process responsible.

4.3.1.4 Use of NLP and Sentiment Analysis in Adverse Media

There are at least two techniques to identify more relevant information within adverse media screening. NLP can automatically extract key information such as names, locations, and events from large volumes of news articles, social media posts, and regulatory bulletins, while filtering out irrelevant content. Sentiment analysis evaluates the tone of the coverage to highlight negative or high-risk narratives, enabling investigators to focus on the most relevant and potentially harmful information.

Table 4.6 outlines these two techniques and key considerations for use.

TABLE 4.6 • Techniques for Improving Relevance of Adverse Media Screening

Aspect	Natural Language Processing (NLP)	Sentiment Analysis
Definition	AI techniques that enable computers to understand, interpret, and process human language in text or speech.	An application of NLP that determines the emotional tone or attitude expressed in text (for example, positive, negative, or neutral).
Purpose	Extract entities, relationships, and events from large volumes of unstructured text to identify relevant content.	Assess the tone of coverage to highlight negative or high-risk narratives for prioritization.

32 The names in this table were fictionalized to provide illustrative examples and are not intended to reflect any actual individual or legal person.

Aspect	Natural Language Processing (NLP)	Sentiment Analysis
Use Case	Identify mentions of a customer, beneficial owner, or related entity in adverse media, even if names are spelled differently or embedded in complex text.	Flag articles with negative sentiment about a customer or entity to focus investigative resources on higher risk cases.
Examples[33]	NLP detects that "Acme Holdings Ltd" in a news article is linked to "John Smith" (a beneficial owner) and a criminal investigation into money laundering.	Sentiment analysis scores the same article as "highly negative" due to language describing criminal charges, prompting escalation for review.

Source: Original for this publication.

4.3.1.5 Use of Entity Resolution and Alert Risk Scoring

There are other, more advanced techniques that can improve match quality and reduce false positives. Methods such as entity resolution, alert risk scoring, principal component analysis, and self-organizing maps, can enable FIs to identify hidden relationships, prioritize high-risk alerts, and automate the closure of low-risk cases while maintaining transparency and auditability.

Table 4.7 provides an overview of each technique as well as use cases and examples.

TABLE 4.7 • Approaches to Reducing False Positives

Technique and Description	Key Functionalities	Examples[34]
Entity Resolution Identifies and links records across different data sources that refer to the same real-world entity (individual or legal person).	• Prevents duplicate screening and reduces false positives • Enables detection of hidden relationships (for example, associates of PEPs, or front companies) • Improves efficiency by consolidating adverse media alerts and reducing analyst workload	An FI is onboarding a customer named "Maria Teresa Garcia." She appears in one internal database as "Maria T. Garcia" and in another as "M. Teresa Garcia." Entity resolution matches these records, deduplicates them, and links her to a known PEP profile. By using entity resolution, the FI avoids missing a PEP due to name variations and can also identify her close associates—such as a spouse or business partners—who may also require screening.
Alert Risk Scoring Assigns a risk score to an alert based on predefined features (for example, alert type, data source, geography, and match quality).	• Prioritizes high-risk alerts for immediate investigation • Enables suppression of low-risk alerts • Reduces analyst fatigue and improves response time to genuine threats • Supports ongoing model tuning and regulatory compliance through documented, consistent scoring	An adverse media alert is generated for a customer mentioned in a news article about financial crime. The risk scoring engine evaluates factors such as the source (for example, a reputable news outlet), the nature of the allegation (for example, fraud versus a minor regulatory issue), and the match quality. A high score prompts more urgent review, while low-risk alerts, such as unrelated negative news, are suppressed or closed. The technique helps analysts focus on the most relevant and serious adverse media cases.

33 The names in this table were fictionalized to provide illustrative examples and are not intended to reflect any actual individual or legal person.

34 The names in this table were fictionalized to provide illustrative examples and are not intended to reflect any actual individual or legal person.

Technique and Description	Key Functionalities	Examples[34]
Principal Component Analysis A statistical technique intended to reduce the number of variables and identify key features that distinguish true positives from false positives in alert data.	• Enables automatic closure of low-risk, repetitive false positive alerts • Reduces manual review workload • Improves operational efficiency	Historical data shows that alerts for local government officials with low transaction volumes and no prior negative news are almost always closed as false positives. PCA identifies these features as key drivers. The system is then configured to suppress future alerts with the same characteristics. The technique reduces unnecessary manual reviews for low-risk PEPs, allowing analysts to focus on more complex or higher-risk cases.
Self-Organizing Maps An unsupervised neural network technique that clusters and visualizes high-dimensional data, revealing patterns and anomalies.	• Clusters similar alerts for bulk review or suppression • Highlights outlier alerts that may indicate new or emerging risks • Supports visual analytics, enabling analysts to quickly identify low- and high-risk clusters • Enhances adverse media review by grouping related articles	Self-organizing maps, often referred to as "SOMs," group adverse media articles by content similarity (for example, corruption, fraud, environmental violations). Clusters of routine negative news are deprioritized, while outlier articles—such as a sudden mention of a customer in a major international scandal—are flagged for urgent review. The technique helps analysts identify emerging risks and focus on significant adverse media events, rather than routine or low-risk news.

Source: Original for this publication.

4.3.2 Strategies for Improving Data Quality

Access to reliable sources is an important requirement for an effective screening process. However, FIs often face an overabundance of sources that can lead to several challenges. For example, the many lists from different public-sector authorities can result in potential conflicting or duplicative information and data quality issues. As another example, related to adverse media bias, news may not be objective or factual, or can be influenced by political, cultural, commercial, or geographical factors). There are several approaches that FIs have taken to improve their access to reliable data sources. Table 4.8 outlines several of these practices and key considerations.

TABLE 4.8 • Practices to Improve Access to Reliable Data

#	Key Practice	Considerations
1	**Understand and Identify Information Sources**	• Ensure list providers clearly identify the sources of information used in their platforms, including how they obtain sanctions lists (for example, directly from government or through aggregators), PEP lists, and adverse media[35] • Regularly review and assess which lists and sources are applicable and required, in consideration of the FI's risk exposure and risk appetite, and in consultation with legal and compliance departments • Avoid screening against every list that is included as a default option in tools from providers • Consider engaging service providers with regional expertise to tailor lists to the FI's geographic footprint • Maintain an ongoing dialogue with legal and compliance teams to adapt to changes in global political and regulatory environments
2	**Utilize Diverse and Reliable Sources for Negative News**	• Leverage multiple news sources to cross-validate information and improve the reliability of screening results • Conversely, consider avoiding or dismissing sources proven to have unreliable or unbiased news, or blogs with personal opinions • Employ technology to aggregate and integrate global media sources, enhancing the relevance and comprehensiveness of adverse news screening • Consider the impact on data volume and complexity, as adding multiple data sources can significantly increase the number of alerts • Consider consulting local human intelligence or completing reference checks (particularly if engaging with a significant prospective customer in another jurisdiction)
3	**Utilize Defined Search Strings**	• Apply focused search parameters to target adverse news specifically related to the legal person (to improve the relevance of search results) • An example of a search string is: "[Individual or Entity Name]" ("fraud" OR "corruption" OR "terrorism OR "tax evasion" OR "human trafficking" OR "migrant smuggling" OR "drug trafficking" OR "arms trafficking" OR "environmental crime" OR "counterfeiting" OR "cybercrime" OR "organized crime" OR "child exploitation" OR "market abuse" OR "insider trading" OR "bribery" OR "embezzlement" OR "forgery" OR "illicit enrichment" OR "extortion" OR "trade secret theft" OR "terrorist financing" OR "laundering" OR "money laundering" OR "scam" OR "Ponzi" OR "financial crime" OR "conviction" OR "investigation" OR "charged" OR "arrested")
4	**Develop and Apply Source Reputation Scores**	• Create a registry of preferred and trusted sources, assigning reputation scores to guide the review and prioritization of news articles, sanctions, and related parties • Use technology to dynamically apply these scores, among others, during the screening process
5	**Enhance Staff Training and Documentation**	• Provide ongoing training to staff responsible for conducting initial screening, interpreting screening results, and/or managing complex cases • Maintain thorough documentation of screening processes and decisions

35 This information may be considered the intellectual property of the list provider platform. While the provider may be able to identity main sources of information to ensure regulatory lists or specific sanctions lists are covered, it may not be able to offer a complete list of sources. Nonetheless, the FI should be able to articulate to regulators how the source information is complete, accurate, and remains updated.

#	Key Practice	Considerations
6	**Implement Filtering and Prioritization Techniques**	• Use advanced algorithms and risk-based criteria to filter and prioritize alerts, focusing on high-risk cases and reducing information overload • Establish clear escalation protocols (with defined roles and responsibilities and timelines) for handling and resolving alerts efficiently
7	**Leverage Machine Learning and Advanced Technologies**	• Automate routine screening and data validation processes to enhance efficiency and accuracy • Implement machine learning techniques to identify and assess bias in news articles, enabling risk ranking of information based on credibility and relevance • Ensure output from machine learning or AI-based systems are reviewed regularly by a human

Source: Original for this publication.

4.3.2.1 Considerations for Identifying PEPs

Most FIs have a dual approach to identifying PEPs: requesting customers to self-declare their status as a PEP (or as a family member or close associate) and screening customer names against reliable lists of PEPs.[36] Many commercial providers offer lists of PEPs, and some jurisdictions maintain formal registers of public officials. However, in some jurisdictions, reliable lists may not exist, *or* PEPs may be removed from a list once they leave office (even though, in line with guidance from the FATF, the PEP may continue to pose a risk through informal influence after leaving public office).[37] FIs should consider both domestic and foreign individuals.

Where reliable lists of domestic PEPs are unavailable, observed practices include the following:

- Recognized third-party service providers (if they can demonstrate an ability to maintain a reliable list of domestic PEPs for the jurisdiction)
- An industry association, such as a domestic banker's association, assembling a list of PEPs accessible to all members (who contribute funds to maintain the list)
- An individual FI assembling its own list of PEPs, with a set practice to update that list after every jurisdiction-wide election
- Conducting open-source intelligence by reviewing public records, media, and news reports, and conducting an analysis of social media profiles (primarily in higher-risk cases)
- Reviewing asset declaration databases that are publicly available
- Gathering human intelligence about the known close associates of PEPs
- Keeping a record of PEP lists (for the purpose of recording PEP status after leaving public office).

4.3.3 Strategies to Monitor and Continuously Improve Effectiveness

The sections that follow provide several governance considerations, such as practices for managing list updates, building internal capacity, and monitoring the effectiveness of a screening program.

36 Per the FATF (2025c), PEPs are defined as individuals who are or have been entrusted with prominent public functions by a foreign jurisdiction (for example, heads of state or government; senior elected officials; senior government, judicial, or military officials; senior executives of state-owned corporations; senior political party officials; ambassadors; and royal families).

37 While foreign PEPs are always to be considered high-risk, certain domestic PEP relationships may be determined to not present higher risk. The FATF's 2013 Guidance on Politically Exposed Persons (Recommendations 12 and 22) states "foreign PEPs are always considered high risk." which requires the application of EDD measures, whereas domestic PEPs that "present a normal or low risk…may not require enhanced due diligence measures" (FATF, 2013) The HYPERLINK "https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf.coredownload.pdf"FATF's guidance contains additional information on performing a risk assessment and the correlated due diligence and monitoring expectations. In addition, an individual may be considered to present a higher risk even if they are no longer entrusted to a prominent public function. FATF's 2013 guidance states "the handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits" (FATF 2013). Regardless of the timing, FIs should have defined risk-based criteria for determining whether he or she still meets the PEP definition after leaving office.

4.3.3.1 Program Governance

Effective name and transaction screening requires strong governance to ensure technology is used appropriately and risks are managed. Strong governance combines detailed policies, clear roles and responsibilities, and advanced technology with reporting processes.

One key area where governance is critical is list management. List management is the process of ensuring that sanctions, PEP, and adverse media lists used for screening are accurate, reliable, and up to date. Outdated or incomplete lists increase the risk of regulatory breaches, adverse customer impact, and reputational damage to the FI.

Best practices for list management include the following:

- Ensuring only reliable and up-to-date data sources are used to prevent reliance on outdated or incomplete information
- Establishing a process to periodically review which lists are screened against and verify that updates are implemented in a timely manner
- Utilizing case management tools and screening platforms to centralize sources, automate updates, and ensure only approved lists are used
- Validating that external systems and list providers refresh their lists regularly
- Monitoring the time required to implement list changes in the FI's systems
- Implementing version control to document which list version was last screened and ensure auditability.

Table 4.9 outlines other key governance elements and best practices.

TABLE 4.9 • Key Governance Considerations

#	Practice	Best Practices
1	**Defined Roles and Escalation**	• Establish clear responsibilities and escalation paths for investigating screening alerts (to ensure accountability, timely handling of high-risk cases, and appropriate oversight) • Utilize workflow and case management systems to automate the routing of alerts, track investigative actions, and ensure proper escalation to authorized personnel
2	**Audit Trail and Documentation**	• Mandate comprehensive documentation of screening, investigation, and decision-making steps (to ensure traceability, support regulatory reporting, and prepare for audits) • Utilize case and document management tools to securely store investigation records, maintain comprehensive logs, and facilitate efficient retrieval for audit purposes
3	**Consistent Investigation**	• Implement standardized procedures, templates, and checklists for investigations (to reduce human error, ensure relevant factors are considered, and promote consistency) • Utilize investigation modules and case management systems to enforce standardized workflows, templates, and checklists for investigators
4	**PEP and Adverse Media Monitoring**	• Conduct ongoing screening for adverse media for high-risk customers • Establish practices to periodically check for adverse media or changes to PEP status for lower-risk customer relationships (for example, during periodic refreshes) • Utilize screening platforms and data aggregators to facilitate both real-time and scheduled monitoring, automatically flagging new risks for review
5	**Reporting and Analytics**	• Conduct regular analysis of screening outcomes, trends, and process effectiveness (to support continuous improvement, regulatory compliance, and oversight) • Utilize case management and analytics tools to generate dashboards, reports, and trend analyses (to support oversight and process optimization)

#	Practice	Best Practices
6	**Data Security and Privacy**	• Protect sensitive customer and investigation data from unauthorized access or breaches, ensuring compliance with data protection laws and maintaining customer trust • Utilize secure case management solutions and access controls that enable restricting data access, encrypting sensitive information, and monitoring for unauthorized activity
7	**Suppression of Alerts**	• Implement thorough governance processes (to ensure rules are continuously tested and refined to prevent risks from being overlooked) • Periodically review thresholds and criteria for suppression based on new risks, regulatory changes, and investigation outcomes • Maintain records of all suppressed alerts (including logic used and results of periodic testing) and conduct periodic quality assurance over suppressed alerts • Utilize screening platforms and case management tools that automate alert closure, facilitate sample testing, and provide reporting modules to support oversight
8	**NLP or Sentiment Analysis Governance**	• Implement processes to ensure models are validated, free from bias, and subject to human oversight • Regularly validate and test NLP or sentiment models on diverse, updated datasets (for accuracy and consistency) • Routinely assess models for unintended bias or systematic errors, especially across different languages, regions, and media types • Utilize NLP engines, AI platforms, and model management tools to analyze media sources, flag potential risks, and facilitate model validation
9	**Focused Adverse Media Review**	• Establish governance standards requiring analysts to focus on the most relevant and recent articles (utilizing a documented risk-based criteria) • Introduce timespan criteria within procedures for evaluating adverse media (for example, prioritizing news within the last one to three years and deprioritizing if five years old or over) • Embed requirements to capture new adverse media since the last periodic review (for existing relationship) • Mandate the use of approved search strings to ensure adverse media reviews target financial crime–related risks while excluding irrelevant information • Require the use of approved screening platforms, media aggregators, and workflow tools to filter, prioritize, and manage reviews, including defined periods and article limits

Source: Original for this publication.

4.3.3.2 Building Human Capital and Expertise

While technology and analytics can enable improved alert quality, skilled analysts are essential for interpreting alerts, applying judgement, and making decisions. FIs are encouraged to offer ongoing training and education opportunities for analysts and investigators.

Considerations for building human capital and expertise include the following:

- Providing comprehensive onboarding training for all staff involved in screening that covers the system use, regulatory requirements, and investigative techniques
- Offering regular refresher courses focused on emerging financial crime typologies, regulatory changes, and any relevant updates to system features and workflows
- Providing point-in-time and tailored training to ensure content is timely, relevant, and immediately applicable to operational needs

- Providing access to training on conducting open-source research, identifying red flags, and identifying network linkages, particularly for second-level investigators
- Providing cross-training to ensure that multiple team members are proficient in adjacent functions to support business continuity during staff absences or staff transitions
- Encouraging participation in industry forums and knowledge-sharing networks to stay current on best practices
- Ensuring proper authorization and protection of staff to enable objective decisions and avoid defensive reporting.

As previously noted, FIs should have written desktop operating procedures that guide analysts and other individuals responsible for reviewing alerts. Written procedures can enable consistency and quality while documenting that decisions follow a controlled governance framework.

4.3.3.3 Utilizing Reporting (KPIs)

Another strategy for increasing the effectiveness of screening is the use of tailored reporting via key risk indicators (KRIs) and key performance indicators (KPIs). KRIs and KPIs can provide benefits even without advanced systems. Table 4.10 offers example KRIs and KPIs, explains how they are measured, describes their implications, and highlights the potential actions an FI could consider to maximize effectiveness and efficiency based on the data.

TABLE 4.10 • Example KPIs and KRIs and Their Implications

KRI or KPI	Measurement	Potential Implications	Potential Actions
False Positive Rate The false positive rate is a key indicator of inefficiency in the screening process. It reflects the amount of noise generated by the system.[38]	Divides the total number of alerts closed as "not a true match" by the total number of matches performed (that is, false positives ÷ all matches). For example, if 800 alerts were closed as false positives out of 1,000 total matches, the false positive rate is 800 ÷ 1,000 = 0.8, or 80 percent.	A lower false positive rate indicates a more effective screening process. A higher rate suggests potential issues with matching logic, warranting review and possible adjustment.	• Implement less stringent alert thresholds so that low-risk alerts are not flagged • Improve fuzzy logic by increasing match stringency • Apply contextual filters (such as geographic factors) to refine results • Incorporate additional identifiers in the search to narrow hits to a specific subject (for example alias and DOB)

38 The term "noise" refers to irrelevant or false-positive alerts that do not indicate genuine risk but can obscure true suspicious activity and hinder operational efficiency.

KRI or KPI	Measurement	Potential Implications	Potential Actions
True Positive Rate This metric measures the percentage of true positives (alerts that correctly identify individuals or entities of interest) detected by the system.	Divides the total number of true positives identified by the total number of true positives that should have been identified. The denominator is the sum of true positives and false negatives (that is, true positives ÷ (true positives + false negatives)). For example, if the system correctly identifies 98 true positives and misses 2 (false negatives), the true positive rate is calculated as 98 ÷ (98 + 2) = 0.98, or 98 percent.	A high true positive rate means the system is effectively identifying individuals or entities that should be flagged. A lower rate increases the risk of compliance and regulatory issues.	• Review outcomes by alert type (for example, the rate may be highest for sanctions and slightly lower for adverse media or PEPs) • Consider using NLP to extract additional context from media sources to support investigations • Regularly audit the system using test files to identify and address any gaps in detection
Positive Predictive Value (Precision) This metric, also known as precision, determines the percentage of all flagged alerts that are true positives.	Divide the number of true positives by the sum of true positives and false positives (that is, true positives + false positives). For example, if there are 40 true positives and 60 false positives, precision is calculated as 40 ÷ (40 + 60) = 0.4, or 40 percent.	Higher percentages indicate greater precision, meaning that the alerts being investigated are of higher quality. Improving this metric reduces the time spent resolving alerts that are not genuine matches.	• If precision is too low, improve the quality and completeness of data sources to enable better matching • Implement risk-based screening thresholds so that matches below set percentages are not flagged (these thresholds can be tailored by alert type) • Use entity resolution to match linked organizations based on interrelationships • Apply (and periodically test) suppression techniques for lower-risk alerts or those with specific attributes
Hit Rate This metric, more commonly utilized in transaction screening, is the number of alerts generated per number of transactions.	Divide the number of alerts generated by the total number of transactions (that is, alerts generated ÷ total transactions). For example, if 150 alerts are generated from 5,000 transactions, the hit rate is calculated as 150 ÷ 5,000 = 0.03, or 3 percent.	A high hit rate may indicate that the system is overly conservative, flagging too many low-risk transactions (especially if the false positive rate is high and precision is low), or it could reflect a genuinely high-risk business if precision is high. Conversely, a low hit rate may suggest a low-risk customer base or product set but could also indicate that the system's thresholds are too high, potentially missing true matches.	• If there is a high hit rate, consider checking data quality, tuning screening parameters, and optimizing watchlist use • If there is a low hit rate, validate detection (through back-testing and sample checks), monitor trends (such as true positive rates), and investigate any unexplained drops in alerts

KRI or KPI	Measurement	Potential Implications	Potential Actions
Missed Match Rate This metric measures the proportion of true matches that the screening system fails to identify (false negatives). It is a key quality control indicator, showing how often the system is missing alerts it should have generated.	Divide the number of missed true matches by the total number of true matches identified through quality assurance processes (for example, back-testing or manual review—that is, missed match rate = missed true matches ÷ total true matches). For example, if a QA review of 1,000 transactions finds 20 true matches but the system only generated alerts for 18 of them, then: 2 ÷ 20 = 0.10, or 10 percent.	A high missed match rate indicates the system is failing to detect a significant portion of true matches, which can lead to regulatory breaches, financial crime exposure, and reputational damage. A low missed match rate suggests the system is effectively identifying true matches, but it should still be monitored to ensure it remains within acceptable risk tolerance.	• If the missed match rate is high, review and adjust matching thresholds, improve data quality (for example, names, DOB, and addresses), update and expand watchlists, and enhance screening algorithms • If the missed match rate is low, continue monitoring through regular QA and back-testing to ensure performance remains strong, and document results for regulatory assurance
Alert Disposition Breakdown Tracks trends over time in key metrics such as false positive rate, medium true positive rate, and positive predictive value, helping to identify shifts in the quality and nature of alerts generated.	Calculate the proportion of false positives and true positives for each alert type (that is, sanctions, PEP, or adverse media) over a given period. This is typically expressed as a percentage breakdown by alert type and risk level. For example, over a month, if 1,000 low-risk alerts are generated and 950 are false positives, the false positive rate for low-risk alerts is 95 percent. If 200 high-risk alerts are generated and 40 are true positives, the true positive rate for high-risk alerts is 20 percent.	The alert disposition breakdown highlights opportunities to tune rules and thresholds for different alert types and risk levels. For instance, a high false positive rate among low-risk alerts may indicate overly sensitive thresholds, while a low true positive rate among high-risk alerts may signal missed risks or inadequate detection.	• Use alert disposition analysis to inform risk appetite and system configuration. For adverse media, this analysis can help determine what types of negative media risk (for example, financial crime or reputational risk) the institution is willing to accept or prioritize for investigation • Adjust thresholds and rules accordingly to optimize alert quality and operational efficiency

KRI or KPI	Measurement	Potential Implications	Potential Actions
Average Time to Resolve an Alert This metric, also known as alert disposition time, measures how long it takes for an analyst to resolve an alert.	Track the time taken to close each alert either manually or automatically through a case management system and calculate the average or median time per alert type over a defined period. For example, if five alerts take 6, 8, 10, 7, and 9 minutes to resolve, the average disposition time is (6 + 8 + 10 + 7 + 9) ÷ 5 = 8 minutes.	A longer disposition time may indicate higher-quality alerts that require more in-depth analysis, but if paired with a high false positive rate, it may signal poor data quality or insufficient information for decision-making. Conversely, a short disposition time with a high false positive rate may suggest thresholds are too low. A short disposition time with a low false positive rate may indicate many alerts could be suppressed without analyst intervention.	• Establish standard time-to-resolve-an-alert ranges based on alert type and criticality, establishing a practice to escalate to second level of review if assessments cannot be cleared quickly • Implement a whitelist to prevent duplicate entries from being repeatedly flagged. For adverse media alerts with long disposition times, consider using NLP to summarize news articles and support faster decision-making
Volume of Alerts Per Analyst Per Day This metric, also known as analyst alert throughput, highlights the total number of alerts an analyst processes in a day.	Calculate the average number of alerts reviewed per analyst per day over a defined period. For example, if an analyst reviews 120 alerts in one day and the daily totals over five days are 100, 110, 120, 130, and 140, the average throughput is (100 + 110 + 120 + 130 + 140) ÷ 5 = 120 alerts per day.	High throughput may indicate that analysts are overworked, which can lead to fatigue and increase the risk of errors or inadequate investigations. If high throughput is combined with high false positive rates and short resolution times, it may suggest alerts are not thoroughly investigated.	• Implement workflow tools to allocate cases evenly among analysts, preventing overload • Consider periodic training and resource adjustments based on throughput trends and alert quality
Geographic Hit Rate This metric tracks alerts triggered because of a specific geography (such as a sanctioned or high-risk jurisdiction) and provides management an indication of actual risk exposure.	Reviewing alerts where a country has triggered that alert and keeping track. For example, there were 100 alerts generated because of hits related to Country X vs. 10 alerts generated from hits related to Country Y.	Leveraged to manage geographic risk and as part of the broader risk assessment processes (to view actual exposure of accounts or transactions with certain geographies). A high frequency to a certain jurisdiction can indicate emerging (or decreasing) risks within business activity.	• Incorporate the inherent risk factor of periodic business line or enterprise-wide risk assessments into the geography • Consider revisions to risk-based controls (for example, additional manual reviews or QA, additional questions for CDD, and changes to sensitivity scores) based on data

Source: Original for this publication.

Table 4.10 is not a comprehensive list of all KRIs and KPIs, but it can be utilized by FIs to measure and track key indicators that could reveal emerging risks, breakdowns in processes, or opportunities to make systems or processes more efficient.[39] Tracking and reporting these metrics over time (for example, weekly, monthly, or quarterly) also enables management to identify trends and demonstrate program effectiveness to auditors, regulators, and correspondent banks.

4.3.3.4 Leveraging System Effectiveness Testing

There is an inherent risk when using algorithm-based screening tools that FIs may miss alerts (false negatives) or incorrectly close them. The use of KRIs and KPIs and quality assurance or quality control mechanisms is valuable for monitoring these risks. However, there is also a need to independently test the effectiveness of systems and processes.

Considerations for ongoing testing include the following:

- Testing should confirm that true matches are detected, the rate of false positives is within acceptable limits, and sensitivity scores remain appropriate as sanctions lists, PEP data, and customer profiles change
- Testing should include pre-implementation analysis with historical data, back-testing to identify missed matches, parallel testing alongside existing processes, and scenario testing with synthetic or "seeded" data
- All testing should be documented, with results reviewed by compliance, IT, and management, and retained for review
- Testing should occur at least annually, and after major system updates, list changes, or shifts in risk profile.

Table 4.11 highlights the key steps and best practices for implementing effective testing.

TABLE 4.11 • Key Testing Considerations and Best Practices

#	Practice	Key Considerations or Best Practices
1	**Development of Comprehensive Test File**	• Include both true positives (for example, known sanctioned entities and individuals, current PEPs, or recent adverse media subjects) and true negatives (for example, common names that should not trigger alerts or generate true matches) • Incorporate edge cases, including spelling variants, transliterations, partial matches, outdated or resolved media cases, and entities with complex ownership structures • Use source data from public regulatory lists, recent adverse media, internal historic case data (where available), and synthetic scenarios • Ensure the test file contains, at a minimum: name (individual or entity), date of birth, jurisdiction, aliases, ownership details, and media article references
2	**Conducting Baseline Testing (Initial Tool Assessment)**	• Upload the test file into the screening tool • Execute the screening process in accordance with standard operational procedures • Capture results by recording which entries trigger alerts, the type of alert (sanctions, PEP, or adverse media), and any missed matches or false positives

39 Other example KPIs and KRIs include alert escalation rates (to determine the alert quality and analyst's ability to independently resolve alerts); alert suppression rates (to track reliance on override and suppression techniques and identify potential governance risks); and alert aging rate (to assess backlogs and determine staffing adequacy).

#	Practice	Key Considerations or Best Practices
3	**Analysis of Results**	• Assess the accuracy of the screening tool by confirming that all high-risk names and entities are detected as true positives • Review the results to identify any false negatives, ensuring no high-risk names or entities are missed • Evaluate the occurrence of false positives by determining if any clean names or entities are incorrectly flagged • Examine the tool's handling of edge cases, including spelling variants, transliterations, and complex scenarios • Assess the quality of generated alerts, focusing on their clarity and relevance
4	**Tuning and Calibration**	• Fine-tune matching thresholds, fuzzy logic, and filter settings to reduce false positives and false negatives • Periodically reconcile source lists to ensure all data feeds are current and comprehensive • Repeat the test cycle with adjusted parameters to verify improvements
5	**Model Validation**	• Model validation is critical to balancing compliance with operational efficiency • As an added best practice, some FIs periodically engage independent consultants and external auditors to test and validate key systems

Source: Original for this publication.

5

Practices for Improving Suspicious Activity Monitoring

Chapter 5 builds on prior chapters by further defining opportunities and best practices for leveraging technology and analytics within suspicious activity monitoring. For the purposes of this Good Practice Note, suspicious activity monitoring and reporting refers to the processes to review customer activity and transactions for indications of potentially suspicious activity, and, when identified, to report such activity to relevant authorities in the form of SARs or STRs. Suspicious activity monitoring serves as a cornerstone of AML/CFT programs that enables FIs to detect and respond to potentially illicit transactions. FIs monitor for suspicious activity not only to fulfill legal or regulatory obligations but also to enable FIs to prevent the exploitation of its products and services for illicit purposes, and, ultimately, to protect the integrity of the FI and the financial system in which it operates. However, implementing an effective suspicious activity monitoring program remains a challenge faced by FIs of all sizes and control maturity as they must analyze large volumes of transactional and behavioral data, often generating high numbers of alerts—many of which are false positives—that require substantial investigative resources to resolve while at times missing false negatives.

Among other topics, Chapter 5 will address the following:

- What are the main challenges in conducting suspicious activity monitoring?
- What are the main steps in conducting suspicious activity monitoring?
- How do FIs decide what to monitor for?
- What is a "coverage assessment" and "rule calibration" and how are they conducted?
- What are some strategies to reduce false negative and false positive alerts
- How can the effectiveness of alert reviews be improved?
- How are machine learning and AI transforming suspicious activity monitoring?
- What are the best practices for ongoing monitoring and continuous improvement of suspicious activity identification?
- What are some examples of FIs in emerging markets utilizing machine learning and AI?

5.1 Capabilities of Technology & Analytics in Addressing Challenges

While technology enables FIs to focus efforts on the transactions and activities most indicative of suspicious behavior, several key challenges remain, including the following:

- **High incidence of false positives:** Many legitimate transactions are flagged as suspicious (in IFC's experience, often as much as 97–99 percent of all alerts), distracting resources and increasing the workload for investigators
- **High costs of investigations:** Thorough reviews require significant time, technology, expertise, and financial resources, which can be prohibitive for smaller FIs. The pressure for faster and more effective quality controls, combined with the regulatory pressures, can create pressures for FIs. For example, developing controls that are fast and agile can lead to compliance risks whereas controls that are more thorough and require more time can lead to more expensive services and financial exclusion. In addition, there is a high demand for skilled investigators, and high workloads can lead to superficial investigations or backlogs
- **Limited effectiveness:** In some cases, in IFC's experience, less than 3–5 percent of alerts result in SARs, STRs, or customer exits, and even fewer lead to criminal prosecution, which has led to calls to modernize the current industry-wide approach to monitoring. In addition, monitoring systems may fail to identify potentially suspicious activity (through false negatives)
- **Static or dated rules and parameters:** Monitoring rules often fail to reflect evolving threats or risks, reducing the relevance and accuracy of alerts and possibly leading to missed suspicious activity. In addition, FIs may use readily available software with preprogrammed monitoring rules and parameters but fail to calibrate them to their risk profiles and operating environments
- **Data quality and integration issues:** Incomplete, inconsistent, or siloed customer and transaction data reduces monitoring accuracy. The lack of integration between core banking, payment, and customer risk systems can lead to missed patterns or duplicate alerts
- **Breakdowns in testing and oversight:** Gaps within monitoring system testing and improper calibration and validation can lead to missed transactions or coverage and have resulted in backlogs, lookbacks, and regulatory penalties in some instances
- **Explainability:** There is reluctance to move toward AI-based transaction monitoring for fear of auditors or regulators not understanding the systems and how they reach their decisions, introducing resistance to innovative and evolving approaches.

While there are multiple root causes of these challenges, they frequently stem from suspicious activity monitoring programs that fail to keep pace with an FI's evolving risk profile and operational footprint.

However, there are software solutions and techniques that FIs can use to strengthen suspicious activity monitoring. In addition to traditional automated transaction monitoring systems, modern monitoring solutions can integrate real-time transaction surveillance, behavioral analytics, and automated alert risk scoring within a unified system, which is a reason why many FIs have moved away from the concept of "transaction monitoring" to focus now on more holistic "monitoring for suspicious activity" (The Wolfsberg Group 2024). These platforms often provide capabilities such as scenario-based monitoring, pattern recognition algorithms, network or relationship analysis, and watchlist screening,[40] enabling detection of unusual or potentially illicit activities as they occur. Additionally, machine learning models can adapt detection thresholds based on emerging patterns, reducing false positives while highlighting genuinely high-risk events. Workflow automation supports efficient case management by prioritizing alerts, assigning investigative tasks, and maintaining complete audit trails.

40 As detailed in Chapter 4, "Practices for Improving Name and Payment Screening," sanctions and watchlist screening are controls distinct from suspicious activity monitoring; however, many systems offer both screening and suspicious activity monitoring capabilities.

5.2 Foundational Concepts in Suspicious Activity Monitoring

Before highlighting techniques to overcome these challenges, the Good Practice Note first provides foundational information on suspicious activity monitoring. While this section provides useful background information that can benefit experienced compliance professionals, readers that are familiar with these concepts and are focused primarily on strategies to overcome challenges may proceed directly to Chapter 5.3, "Techniques for Optimizing Suspicious Activity Monitoring."

5.2.1 Defining Suspicious Activity Monitoring and Reporting

As defined in Chapter 2, suspicious activity monitoring refers to the manual and/or automated processes to review a customer's profile (considering both customer behavior and transactions for indications of suspicious activity, and, when identified, to report such activity to relevant public authorities in the form of SARs or STRs.

Across the financial services industry, most FIs use automated systems to monitor customer transactions and generate alerts that warrant human review. Although there is a growing shift toward incorporating AI to detect anomalies and improve efficiency, most monitoring systems currently rely on predefined "detection rules" or "scenarios" even if AI or machine learning techniques are utilized. These rules trigger an alert when specific transaction patterns are met, serving as warning signals of potentially suspicious activity (for example, transactions inconsistent with a customer's profile, rapid movement of funds, unusual use of high-risk products or channels, or links to high-risk jurisdictions, among others) that subsequently requires additional investigation.

The detection rules may be threshold-based (for example, transactions above or below a certain value), behavioral (for example, deviations from historical activity), or contextual (for example, transactions involving high-risk geographies or products). Industry best practice involves adopting a layered approach, combining static rules, which apply fixed thresholds and parameters defined during system setup, with dynamic, adaptive models that use data analytics and machine learning to more holistically recognize evolving transaction patterns and emerging risks.

While automated systems play a critical role in detecting unusual patterns, human judgement and human-observed behavior similarly are essential to effective monitoring. Suspicious activity monitoring programs should include channels for escalating observed unusual customer behavior, with referrals from employees and branch representatives often providing a valuable source for

THE FATF RECOMMENDATIONS

The requirement to monitor for suspicious activity is embedded across several FATF recommendations—notably Recommendation 10 (Customer Due Diligence) and Recommendation 20 (Reporting of Suspicious Transactions). Recommendation 20 states that "If [an] FI suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)."

Suspicious activity monitoring ties directly to several Immediate Outcomes—notably IO.3. (Preventative Measures for FIs, which considers reporting obligations and confidentiality), IO.6 (Financial Intelligence), IO.7 (ML Investigation and Prosecution), and IO.9 (TF Investigation and Prosecution), since high-quality SARs and STRs serve as a major input for FIUs and for subsequent investigations and prosecution.

identifying and reporting suspicious activity.[41] In addition, there may be times when manual reviews of customer transactions (or reviews outside of systems that use data analysis techniques) identify potentially suspicious activity that lead to high-quality SARs or STRs that may have otherwise been undetected by traditional rules.

5.2.2 Key Process Steps within Suspicious Activity Monitoring

Table 5.1 outlines the primary stages of suspicious activity monitoring, the underlying key components, and several key considerations.

TABLE 5.1 • Key Process Steps in Suspicious Activity Monitoring

STAGE 1 **Data Collection and Integration**	• Gather transaction data from relevant internal systems, such as core banking systems, payment systems, among others, where permitted by data protection and data privacy considerations • Integrate transaction data with customer profile data (CDD or KYC, risk ratings, beneficial ownership, geographic exposure, and product usage)
STAGE 2 **Scenario (or "Rule") Configuration**	• Define the patterns and criteria warranting a review or investigation of customer activity. Within rules-based monitoring, this includes identifying the financial crime typologies related to the FI's products or footprint and defining automated detection rules and thresholds based on the FI's inherent risk exposure, regulatory requirements, and internal risk appetite • Include standard scenarios (for example, structuring) and FI-relevant patterns • Document all detection rules and rationales for their design and inclusion
STAGE 3 **Alert Generation[42]**	• Monitor accounts and customer transactions and generate alerts for transactions or patterns that meet certain parameters or a risk typology • Monitor customer behavior (with escalations of red flags from customer-facing staff) • Apply rules and analytics to transaction data to generate alerts in real time or in batches
STAGE 4 **Alert Prioritization**	• Prioritize alerts based on type, rule, and/or risk rating • Consider machine learning or analytics to reduce false positives and detect anomalies • Include mechanisms for deduplication and suppression of repetitive low-risk alerts
STAGE 5 **Alert Review and Case Investigation**	• Review alerts, gather additional information, and assess whether activity is reasonable or justified • Cross-check with customer history, external data (for example, adverse media or sanctions lists), and peer group behavior • Escalate more complex cases to skilled investigators for additional review

41 Examples of potentially unusual customer behavior include: reluctance or refusal to provide identification, visible nervousness or evasive communication, Interference or control by other individuals, frequent visits with large cash in small denominations, and avoiding discussion about source or purpose of funds.

42 Once an alert is generated, it undergoes an initial review and moves into a case for investigation if the transaction or behavior is potentially suspicious. This process typically occurs within the system's workflow functionality, using a case management tool. Alerts are prioritized based on type or rule, and the reviewer accesses the case to analyze customer information, transaction details, and any additional insights.

STAGE 6 **Internal Escalation and Decision-Making**	• Decide whether to take internal action (such as imposing limits or exiting a relationship) • Decide whether to file a STR or SAR with the FIU • Document findings and rationale for decisions
STAGE 7 **Reporting**	• File SARs and STRs promptly, in line with required deadlines • Maintain detailed records of alerts, investigations, and decisions for quality assurance, training, and audit purposes • Maintain records for minimum required recordkeeping timeframes
STAGE 8 **Continuous Improvement**	• Use feedback (such as from investigations, public-sector authorities, and auditors) to refine rules and scenarios • Conduct periodic tuning of automated systems to improve detection accuracy and reduce false positives • Conduct periodic coverage assessments of detection rules to align with emerging typologies or risks • Create new rules as new products are launched and as automated systems offer new features • Conduct periodic validations of automated systems

Source: Original for this publication.

5.2.3 Comparing Automated, Semi-Automated, and Manual Monitoring

Manual suspicious activity monitoring relies on human review of transactional data and observed customer behavior. It can address certain contextual nuances, but it is limited in speed, scalability, and ability to process large volumes. Automated monitoring solutions—some of which also incorporate AI, machine learning, and advanced analytics—can process transactions in real time, adapt detection scenarios, and integrate multiple data sources to improve accuracy and reduce false positives.

Table 5.2 outlines several phases in the maturity of manual vs. automated monitoring.

TABLE 5.2 • Types of Suspicious Activity Monitoring

Manual	Semi-Automated	Automated (Rules-Based)	Automated (AI-Based)
Staff review transactional data manually (via data extracts, reports, or customer transactional history) or rely on interactions with customers (for example at a branch) to spot red flags.	Systems or spreadsheets generate alerts or identify patterns based on predefined rules, but usually with a manual extract.	Generates alerts for manual review when activity triggers a predefined "rule" that may be threshold-based, behavioral, or contextual.	Uses advanced analytics (utilizing AI) to pull from multiple data sources to identify anomalies in behavior and transactions.

Source: Original for this publication.

While automated monitoring is the industry standard for most financial operations, there are cases (such as for low-risk environments or niche business lines) where manual monitoring may be appropriate. In addition, the manual escalation of potentially suspicious behavior identified by customer-facing staff often provides a highly productive source of suspicious activity that should be analyzed along with transactional activity.

Table 5.3 outlines the primary differences between manual and automated monitoring.

TABLE 5.3 • Comparing Manual vs. Automated Monitoring

Aspect	Manual Monitoring	Automated Monitoring
Speed	• Often slower detection of potentially suspicious activity, conducted on a batch or periodic basis (with some exceptions, for example, trade finance) • Best for low transaction volumes or niche products	• Real-time or near-real-time review of transactions • Best suited to high-volume, high-risk environments
Scalability	• Limited capacity and scalability, requiring human time and resources for large volumes • Best suited for smaller FIs with limited customer bases and transaction volumes, or niche business lines	• Scalable to higher transaction volumes with minimal additional staffing to detection purposes • Best suited for most FIs, particularly those that enable funds transfers and have heightened volumes
Detection Approach	• Relies on manual identification of patterns as opposed to use of automated systems • Can be effective for context-specific typologies and niche product areas	• Uses detection rules and scenarios to escalate transactions that meet certain patterns • Best for complex or evolving typologies detected through multiple transactions
Data Integration	• Often requires manual cross-checking information between systems	• Able to integrate multiple internal and external data sources automatically
Accuracy	• Can capture local and contextual nuances but typically a higher risk of failing to detect suspicious patterns • Conversely, can detect certain anomalies that systems may struggle to detect	• Typically enables more detection of potentially suspicious activity but with false positives • Accuracy can be enhanced through periodic review and calibration of detection rules
Audit Trail	• Can be difficult to document alerted activity and rationale for review	• Automated logging of alerts, investigations, and decisions for compliance review

Source: Original for this publication.

Although manual monitoring may be appropriate in certain environments, automated transaction monitoring systems enable FIs to detect a wide range of patterns that would be impractical to identify manually. These systems apply predefined rules and analytical models to large volumes of transactional and customer data and help FIs spot deviations from expected customer behavior or known ML/TF typologies. Table 5.4 summarizes the characteristics of such rules and patterns within automated monitoring.

TABLE 5.4 • Rules or Patterns Detected in Automated Monitoring

#	Rule or Pattern	What It Tries to Identify	How It Enables Identification
1	**Static Risk Characteristics**	Transactions linked to inherently higher-risk customers or sudden changes in static data (new beneficiaries, account details)	Integrates customer data from multiple systems to flag static risk factors or detect changes in near-real time
2	**Excessive Transaction Patterns**	Unusually high value or volume of activity within a chosen period	Aggregates and counts transactions automatically, enabling users to modify the review period and thresholds
3	**Behavioral Patterns**	Known ML or TF behaviors (such as rapid deposits/withdrawals, layering)	Enable complex rule logic and conditional statements at scale (such as a transaction meeting more than one parameter)
4	**Interrelationships Between Accounts**	Unusual transaction flows among linked personal or business accounts	Maps relationships across internal datasets and traces funds faster than manual methods
5	**Transaction History Analysis**	Current activity that deviates from a customer's own historical behavior	Stores historical baselines and applies statistical tests to detect anomalies in current behavior
6	**Peer-Group Profiling**	Activity that falls outside norms for a predefined peer segment (such as age or industry)	Groups customers by chosen attributes and compares individual customer against the group's behavior
7	**Clustering**	Emerging risk patterns among customers grouped by data-driven similarities	Employs algorithms to form clusters and identify new typologies automatically
8	**Predictive Analytics**	Behavior that diverges from a customer's expected activity	Maintains expectation models, tracks actual behavior over time, and retrains models as patterns evolve

Source: Original for this publication.

Detection rules are typically derived from a combination of regulatory requirements, risk assessments, and typology libraries. The next section provides guidelines on designing detection rules.

5.3 Techniques for Optimizing Suspicious Activity Monitoring with Technology and Analytics

The following sections outline strategies to address several common challenges, including methods to enhance detection coverage and tuning, improve the quality of alert reviews and investigations, test and refine monitoring systems, and integrate with machine learning and AI-based approaches.

5.3.1 Strategies for Improving Detection Quality and Reducing False Positives

One of the main challenges faced by FIs is the high incidence of false positive alerts and limited productivity in terms of generating SARs and STRs. The impact of false positives and low productivity includes:

- **Operational inefficiencies**, as analysts spend excessive time resolving nonsuspicious alerts.
- **Delays in transaction processing**, with legitimate activity held pending review.
- **Customer dissatisfaction**, driven by repeated and unexplained requests for information.
- **Analyst fatigue**, increasing the risk of oversight and investigative errors.
- **Regulatory and reputational risk**, as true suspicious activity may be missed or reported late.

Several technology and analytics-enabled strategies can improve monitoring outcomes by reducing false positives while avoiding false negatives. While there are advanced strategies (such as those using machine learning and AI), simple strategies (such as establishing and maintaining processes to revisit and calibrate the detection rules used in automated systems) can have a dramatically positive impact on the effectiveness and efficiency of automated transaction monitoring systems. The following sections highlight practices for selecting, designing, and tuning the detection rules used in many automated monitoring systems.

5.3.1.1 *Practices for Designing Detection Rules*

FIs should have established processes to select the detection rules utilized in a monitoring system. The primary practice adopted by FIs to select these rules is commonly referred to as a "coverage assessment."

5.3.1.1.1 *Process Steps in Conducting a Coverage Assessment (Rule Selection)*

As a foundational step before selecting detection rules, FIs should have a thorough understanding of their customers, products and services, distribution channels, geographies, and the associated inherent risks and typologies to those risk factors.[43] Rule selection should be informed by a risk-based approach (considering its understanding of its risk exposure as well as the risk posed by the customer). FIs should then design mechanisms to identify activity or behavior consistent with the risks and typologies (for example, by leveraging the results of national risk assessments and typology reports) and integrate them into rules-based monitoring systems (that alert investigators of potentially suspicious activity). Table 5.5 outlines the common steps involved in a coverage assessment.

TABLE 5.5 • Typical Process Steps for Conducting a Coverage Assessment

#	Step	Key Activities
1	**Understand Inherent Risk Exposure and Typologies**	• Identify inherent risks (preferably via the formal enterprise-wide risk assessment process)[44] • Review reports issued by authorities relating to the current risks and typologies within the jurisdiction and industries serviced by the FI (for example, through national risk assessments, regulatory advisories, and bulletins) • Review data on prior STR and SAR filings to understand the characteristics of the reported behavior and if it is linked to specific criminal activity (for example, drug trafficking) • Review threat intelligence reports (for example, the UNODC's World Wildlife Crime Report to identify wildlife trafficking typologies, the FATF's Comprehensive Update on Terrorist Financing Risks with respect to terrorism financing, INTERPOL's 2026 Global Financial Fraud Threat Assessment and/or the FATF's 2023 paper on cyber-enabled fraud for fraud typologies, and typology reports from FSRBs and/or financial intelligence units)
2	**Map Risks and Typologies to Monitoring Requirements**	• Map each typology relevant to each product or service and existing coverage (whether through automated systems or manual monitoring) to ensure identified typologies are monitored • Identify the required data elements (for example, true cash transactions, internal funds movements, and individual product platforms) to identify patterns consistent with the relevant typology • Consult industry guidance and typology reports for example detection rules and typologies (with examples of such guidance detailed in Section 5.3.1.1.2) • Define the proposed detection rule utilized to identify patterns consistent with the illicit activity
3	**Assess Current Inventory of Rules and Models**	• Develop a catalog of the currently implemented rules in existing automated systems • Map existing rules to risks and typologies currently or previously identified • Understand the thresholds or parameters and products and services covered by the rule • Document alert volumes and alert-to-SAR or -STR conversion rates on a historical basis (for example, 30 percent of alerts led to an STR or SAR in Q1 as opposed to 1 percent of alerts in Q2)

43 Typologies are the patterns, behavior, methods, and techniques utilized to launder funds, finance terrorism, or commit other financial crimes.

44 These inherent risks are often determined through a periodic or ongoing enterprise-wide ML/TF risk assessment. Please refer to Section 3.3 of IFC 2019.

#	Step	Key Activities
4	**Identify Gaps and Design Rules to Identify Gaps**	• Map the identified risks and typologies into the current rules implemented • Identify any gaps (for example, product, geography, or emerging risks) not covered in current rules • Prioritize remediation of gaps that relate to higher-risk or regulatory required scenarios • Test the remediation of the identified gaps with the use of actual or synthetic data (to confirm if the system does, in practice, detect the activity patterns the rule is designed to detect) • Define initial parameters and thresholds for the rule addressing the missing coverage and consider testing different iterations of the rule (to determine effective and efficient coverage) • Involve IT and the system vendor (if a third-party provider) to determine if and how the rule can be implemented within the system • Identify other channels for identifying typologies and products not conducive to automated monitoring (such as through internal escalations; information shared or requested by other FIs, correspondent banks, or law enforcement; and activity identified during ongoing due diligence)
5	**Identify Legacy Rules to be Enhanced or Decommissioned**	• Determine if a rule has a historically low productivity rate or does not map to any regulatory requirement or identified risk • Develop a list of proposed rules for tuning, addition, or removal (often referred to as "decommissioning" and document the rationale for the changes
6	**Document Key Changes**	• Change or make modifications to the proposed rule • Document the nature, purpose, and rationale for each new rule or change prior to implementation • Establish a transaction monitoring governance committee to formalize rule selection and review • Obtain any approvals required to change the rules (for example, by management or governance committees) • Report on changes and their rationale to appropriate management and board • Be prepared to explain the changes and rationale to auditors or regulators

Source: Original for this publication.

The current industry practice is for FIs to conduct a coverage assessment in connection with periodic enterprise-wide risk assessments or upon de launch or a new product or emergence of new typology, with best practice involving an ongoing approach to rule selection.[45] The result of the coverage assessment (as well as the status of remediating gaps in coverage) should be reported to management or the applicable governance committee.

5.3.1.1.2 *Considerations for Designing Detection Rules*

The individual detection rules are typically derived from a combination of regulatory requirements, risk assessments, and typology libraries. Regulators generally expect that baseline detection rules address a range of key risk areas, including static risk factors (for example, transactions involving high-risk jurisdictions or PEPs), volume or threshold-based rules (for example, unusually

45 The 2023 updates to the Wolfsberg Questionnaire asks respondents to declare when the automated transaction monitoring application was last calibrated. Best practice is to have processes that enable a calibration at least once every year (The Wolfsberg Group 2023b).

high numbers or values of transactions within a defined period), and behavioral anomalies (for example, activity that deviates from a customer's typical profile, such as multiple or recurring international remittances or multiple unidentified deposits into a salaried employee's account within a short timeframe). FIs can reference multiple sources when developing such rules, including typology libraries, vendor-provided "out-of-the-box" scenarios, guidance from competent authorities (particularly in the context of public-private partnerships) and guidance from consultants supporting system implementation, among other sources.

FIs may also consider guidance from the following sources:

- FATF and FSRBs[46]
- Wolfsberg Group
- Egmont Group
- UNODC
- Local and foreign regulators
- FIUs
- Industry associations
- Academic journals
- Conferences and webinars
- Typology reports
- Consultants and vendors
- Correspondent banks

This Good Practice Note contains information on several common typologies (such as fraud, drug trafficking, illegal mining, among others) and example detection strategies deployed by FIs (in Annex C, Detection Strategies for Common Typologies). The table below, Table 5.6 contains two examples of utilizing information pertinent to a typology and product, respectively, to design a detection strategy.

TABLE 5.6 • Example Detection Strategies

Typology	Potentially Suspicious Patterns	Considerations for Detecting Patterns
Human Trafficking Typology Example Human trafficking often involves organized networks facilitating the recruitment, transportation, and exploitation of victims, with financial activity characterized by structured payments, use of intermediaries, and transactions linked to travel, accommodation, or movement of individuals.	• Payments to travel, hospitality, medical, or visa services for unrelated individuals • Payments to adult service websites or for adult clothing • Frequent funding to hostels or hotel chains • Rapid transfers between unconnected parties • Payments at off-peak times of day (after midnight and before dawn) • Multiple small deposits from diverse geographies • Transactions inconsistent with customer profile • Activity in high-risk sectors or known trafficking corridors • Repetitive small payments for atypical services • High volume of activity involving ATMs	• Lower monitoring thresholds for high-risk merchant codes (for example, hospitality, travel, and ceremonies) • Monitor frequent, low-value payments • Flag transfers to high-risk regions • Identify payments related to property rentals or purchases outside the customer's usual region • Detect payments made without matching travel bookings

46 An example of a typology report from the FATF or an FSRB is the Asia/Pacific Group on Money Laundering's Yearly Typologies Report available at https://apgml.org/sites/default/files/documents//2024_APG_Typologies_Report.pdf (APG 2024). Multiple FSRBs publish annual typology reports, such as (GAFILAT 2025) publication, available in Spanish at https://biblioteca.gafilat.org/wp-content/uploads/2026/02/Informe-de-Tipologias-Regionales-LA-FT-25.pdf.

Typology	Potentially Suspicious Patterns	Considerations for Detecting Patterns
Lending and Leasing Product Type Example Lending and leasing products, while generally lower risk, may be misused to legitimize proceeds of crime through early repayments, third-party funding, or complex ownership structures.	• High-value leases without clear proof of income • Repeated early lease terminations accompanied by lump-sum payments • Complex loan or lease structures or potential use of shell companies • Rapid or unexplained loan repayments/ early buyouts • Refinancing of recently acquired property by a PEP, relative, or close associate • Related-party lending or leaseback transactions with no clear rationale • Leasing of luxury assets inappropriate to income • Loan collateral from high -risk jurisdictions	• Monitor early lease terminations and lump-sum cash payments • Identify lease/loan payments funded by third parties or large cash payments • Flag high-value leases with no logical business connection • Detect multiple leases/loans involving related entities • Monitor repayment velocity/rapid repayment inconsistent with profile • Identify multiple loan applications in a short period • Scrutinize collateral value exceeding (e.g., >150%) market benchmark or sourced from high-risk jurisdictions • Flag loan proceeds rapidly withdrawn in cash

Source: Original for this publication.

Refer to Appendix C, "Detection Strategies for Common Typologies" for a summary of potentially suspicious patterns and detection strategies for several common typologies.

5.3.1.1.3 *Considerations for Developing a Ruleset or Rule Library*

The volume and type of detection rules depend on an FIs' inherent risk profile. In practice, the number may range from as few as 10–20 to as many as 80–150. The compilation of all detection rules has generally been considered a "ruleset" or a "rule library," and is increasingly referred to as "features". Table 5.7 outlines key process steps and considerations for developing an overall ruleset and benchmarks for the volume and types of typical rules.

TABLE 5.7 • Stages of Building a Ruleset

#	Step	Key Activities	Typical Rule Volume and Nature
1	**Baseline Rule Development**	• Ensure rules meet regulatory expectations • Cover basic typologies (for example, smurfing) • Cover high-risk transactions • Cover main sources of inherent risk	• Around 20–30 simple, threshold-based or static rules focusing on cash-intensive transactions (for example, rapid deposits or withdrawals), core ML and TF typologies, and high-risk transactions (for example, higher-risk jurisdictions or customer types)
2	**Expansion of Ruleset**	• Broaden coverage to include product- and customer-specific risks • Develop specialized rules for individual business lines or product types (for example, loans) • Align and cross-reference with rules from other risk domains, such as fraud	• An additional 20–30 rules covering product-specific risks or differentiated risks for customer types (for example, stricter thresholds for PEPs)

#	Step	Key Activities	Typical Rule Volume and Nature
3	**Optimization of Ruleset**	• Take measures to reduce false positives and improve precision • Consolidate multiple alerts for the same customer or event • Introduce composite alert risk scoring that incorporates customer attributes (for example, PEPs, adverse media, or client located in a high-risk jurisdiction) • Prioritize alerts by severity or frequency	• An additional 10–20 rules combining multiple risk indicators (for example, unusual amount, routing, or pattern) for richer analysis
4	**Implementation of Advanced Analytics**	• Continue to reduce false positives and improve precision • Implement peer grouping, clustering, and other analytical techniques to tailor rules to specific customer types • Introduce machine learning or advanced analytics to suppress repetitive low-risk alerts	• Migrate from segmented thresholds by customer or product to adaptive, data-driven models • More advanced measures deploy ML-based tuning to continuously refine detection and reduce noise

Source: Original for this publication.

Regardless of the stage of control maturity, FIs should maintain clear documentation for their rulesets that define the main risks addressed by the rules, rationalize the reason for the chosen thresholds, memorialize tuning history (as detailed in the next section), and designate an owner for each rule.

5.3.1.2 *Practices for Calibrating Detection Rules*

After defining the rules, FIs should select the parameters or thresholds for generating alerts that are adapted to the FI's overall understanding of its risk exposure as well as the risk posed by the customer. Parameters and thresholds are the specific, quantifiable values — such as transaction amounts, frequency limits, or geographic boundaries — that trigger an alert when customer activity exceeds or deviates from what the FI has determined to be normal or acceptable risk. FIs should have processes to set and periodically review (and revise) parameters and thresholds based on an FI's understanding of risks and historical data.

5.3.1.2.1 Process Steps in Calibrating Detection Rules (Rule Calibration or Threshold Setting)

Table 5.8 outlines the common steps involved in calibrating the rules and assigning parameters.

TABLE 5.8 • Steps for Calibrating Rules

#	Step	Description of Activities	Best Practices
1	**Define Rule Objective**	Clearly articulate what the rule is designed to detect, referencing the FI's risk assessment and key ML and TF typologies.	• Align each rule's purpose with identified typologies and regulatory expectations • Document the intended outcome and rationale
2	**Analyze Historical Data**	Use historical transaction data in a "sandbox" environment to understand customer behavior and transaction patterns (for example, minimum, maximum, mean, median, percentiles, and statistical distributions) to identify rules producing excessive false positives or high true positives.	• Segment data by channel, customer type, geography, and product • Analyst alerts that have historically resulted in higher incidence of SARs/STRs • Identify natural patterns, outliers, and other variations to inform threshold setting

#	Step	Description of Activities	Best Practices
3	**Segment Data for Granular Risk Assessment**	Segment data to reflect key static and dynamic risk factors (for example, PEPs, high-risk customers, and product-specific risks).	• Apply tighter and targeted rule thresholds for higher-risk customers or products • Base segmentation on the FI's documented risk assessment and business profile
4	**Establish Initial Thresholds and Rules**	Set preliminary thresholds and define rules based on data analysis and segmentation results.	• Use statistical outputs (for example, expected transaction ranges and percentiles) to select thresholds • Document rationale for chosen thresholds
5	**Test Rules on Historical Data**	Apply new rules to historical data to estimate alert volumes, identify true and false positives, and assess overall effectiveness.	• Review alert outcomes to confirm that rules detect intended behaviors • Adjust thresholds if excessive false positives occur
6	**Document Rule Development Process**	Maintain clear documentation of rule objectives, data segmentation, assumptions, and limitations.	• Ensure documentation supports model governance requirements and regulatory reviews and audits • Keep a version history to track changes and rationale
7	**Implement Model Governance Controls**	Establish controls and oversight for ongoing rule management, including periodic review schedules and performance monitoring.	• Define review frequency (at least annually, if not more often) and responsible parties • Define how rule changes will be tested and approved
8	**Monitor and Review Rule Performance**	Continuously evaluate performance using metrics such as alert volumes, conversion rates, and false positive ratios, and by performing periodic above-the-line (ATL) and below-the-line (BTL) testing.	• Identify underperforming or obsolete rules for recalibration or elimination • Conduct periodic reconciliation to source systems and periodic model validation to ensure system and rules work as intended

Source: Original for this publication.

5.3.1.2.2 *Considerations for Initial Calibration of a New Detection Rule*

FIs often face challenges in calibrating detection rules, particularly when implementing a system for the first time or introducing a new rule without historical data or established parameters. In these situations, selecting initial thresholds can feel random and unstructured.

Table 5.9 outlines a structured approach to setting and refining initial thresholds.

TABLE 5.9 • Guiding Principles for Initial Calibration of a New Detection Rule

#	Step	Key Activities and Best Practices
1	**Define Rule Objective**	• Clearly identify the risk typology the rule aims to detect • Start with conservative thresholds through testing to capture a broader set of transactions, anticipating that this will initially produce a higher volume of false positives • Use vendor or consultant recommendations cautiously, ensuring to adapt them to the FI's risk profile. • Document the rationale for all parameters and detection logic

#	Step	Key Activities and Best Practices
2	**Establish Baseline Thresholds**	• If possible, draw on historical transaction data, peer benchmarks, or typology insights to define initial thresholds • Perform basic statistical analysis (for example, mean, median, mode, and percentiles) to understand transaction distributions and typical behavior • Segment data by customer risk level, geography, and product type to tailor thresholds
3	**Build Test Scenarios**	• Create realistic examples of suspicious (and normal) behavior, including "edge cases" to test system sensitivity • Map red flags and typologies to each scenario and ensure that the rule logic (for example, entity, frequency, and lookback period) aligns with these patterns • Segment test data by channel, customer type, and geography to detect outliers • Conduct testing in a sandbox using historic data to evaluate outcomes (for example, if the system identifies activity that previously resulted in an SAR or STR)[47]
4	**Segment Rules for Risk Sensitivity**	• Start with highest-impact segments to show value quickly • Apply stricter thresholds for higher-risk customers, products, or regions and broader thresholds for lower-risk categories • Use KYC and risk-rating data to group customers into peer sets for more targeted monitoring • Test thresholds in a controlled environment before deployment. Review sample alerts both above and below the threshold to assess quality and accuracy • Adjust the rule parameters based on testing results and the institution's risk appetite
5	**Plan Iterative Improvements**	• Monitor alert volumes and false positive rates closely to assess effectiveness • Compare outputs against historical cases and past SAR and STR filings to confirm that the rule captures relevant behavior • Apply statistical sampling in a sandbox to test whether threshold changes improve accuracy and reduce unnecessary alerts • Revisit and recalibrate parameters within six to twelve months of launch, using insights from production data and analyst feedback

Source: Original for this publication.

5.3.1.2.3 *Considerations for Tuning (with Above- and Below-the-Line Testing)*

When calibrating detection rules, FIs must strike the right balance between capturing genuine suspicious activity and avoiding excessive false positives. Above-the-line (ATL) and below-the-line (BTL) testing provide a structured, statistical way to validate thresholds by reviewing alerts just above and just below the set limit. This approach helps FIs finetune rules to better identify true risks, reduce noise, and ensure monitoring resources are focused where they matter most.

Table 5.10 explains ATL and BTL testing.

47 Refer to table 5.13 for additional information regarding sandbox test environments.

TABLE 5.10 • Definitions and Purposes of ATL and BTL Testing

Definition	Purpose	Example
ATL Testing Refers to reviewing alerts above a threshold (existing or proposed) to confirm they are indicative of suspicious activity and worth investigating.	Intended to ensure the threshold is not set too high. If many high-risk alerts are found above the line, the threshold may be appropriate or could be lowered to capture more relevant activity.	Threshold: $9,000 for cash deposits. ATL test: Review alerts for deposits over $9,000 to confirm they align with typologies and risk expectations.
BTL Testing Refers to reviewing transactions just below the current threshold to see if suspicious activity is being missed.	Intended to ensure the threshold is not set too low or missing important cases. If many suspicious transactions are found below the line, the threshold could be lowered.	Threshold: $9,000 for cash deposits. BTL test: Review alerts for deposits of $7,000–$8,999 to check for structuring or other suspicious patterns.

Source: Original for this publication.

Applying ATL and BTL testing involves systematically adjusting the threshold values for various transaction types to identify the optimal point where true suspicious transactions are detected while minimizing false positives. The process begins by establishing the upper and lower bounds of transaction values, then increasing or decreasing the threshold to observe the impact on alert generation. Alerts are reviewed for their relevance, and thresholds are further refined based on these findings. The iterative nature of this testing enables models to remain sensitive and efficient.

Table 5.11 offers guiding principles for conducting ATL and BTL testing (in a test environment before launch):

TABLE 5.11 • Guiding Principles for ATL and BTL Testing in Rule Calibration

#	Step	Description	Key Considerations
1	**Select Threshold**	Choose an initial limit (amount, frequency, or score) based on historical data, typology reports, peer benchmarks, and risk appetite.	Use conservative thresholds initially to capture more activity, expecting higher false positives during early testing.
2	**Run ATL Test**	Review a sample of alerts above the set limit to ensure they align with the intended risk typology and scenario logic.	Select a statistically significant sample, including different customer types, geographies, and products.
3	**Run BTL Test**	Review transactions just below the set limit to detect structuring, evasion tactics, or other missed risks.	Focus on "near-miss" ranges (for example, 5–10 percent below threshold). Include high-risk customers and jurisdictions.
4	**Compare Results**	Assess the proportion of false positives above the line and true positives below the line.	Adjust thresholds to reduce noise while ensuring high-risk activity is captured. Document trade-offs.
5	**Adjust Thresholds**	Modify limits based on ATL or BTL findings, risk tolerance, and investigative capacity.	Apply changes. Monitor impact on alert volumes in the test environment.
6	**Document and Review**	Record methodology, sample sizes, findings, and rationale for changes.	Keep an audit trail. Repeat ATL or BTL testing periodically (for example, quarterly or after major typology changes).

Source: Original for this publication.

As an example, an FI is deciding whether to set the alert the threshold for at $50,000–$100,000 for transactions involving higher-risk jurisdictions (table 5.12). After completing ATL and BTL testing, the FI identified the following:

TABLE 5.12 • Example of ATL/BTL Testing in Rule Calibration

Rule	Option A	Option B	Analysis
Wires exceed $xx in a month to high-risk jurisdictions.	At a $50,000 threshold, transfers generated 200 alerts last year, of which 20 resulted in SARs or STRs and 2 in customer exits.	At a $100,000 threshold, transfers generated 20 alerts last year, of which 2 led to SARs or STRs, but missed 18 others where SARs or STRs was filed.	The FI recognizes that setting a higher threshold would have resulted in a significant percentage of alerts that converted into SARs or STRs not being detected. As a result, the FI would apply the lower threshold (to avoid missing false negatives).

Source: Original for this publication.

Ultimately, applying ATL and BTL testing helps FIs balance sensitivity and efficiency (by avoiding missing true positives while controlling false positives), supports evidence-based calibration (enabling decisions based on actual alert outcomes), and provides regulatory defensibility (demonstrating a structured, statistical, documented, and risk-based approach to threshold setting).

5.3.1.2.4 Other Techniques for Rule Refinement

FIs will not always have historical data to perform ATL or BTL testing—for example, when implementing a new rule. However, there are multiple strategies that they can undertake to establish parameters for rules and test their outputs before implementation. Table 5.13 outlines several strategies for refining and maximizing rule effectiveness and enabling testing before rules are live.

TABLE 5.13 • Techniques for Rule Refinement

Approach	Activities	Use Cases
Sandboxes	Allows testing of rules in an offline environment using historic data. Rule settings are adjusted to assess their impact on alert generation. Enables ATL and BTL testing and "what-if" scenarios (for example, changes in transaction values or customer base).	Testing new rules, tuning thresholds, coverage assessments, and simulating scenarios like increased transaction values or customer growth.
Synthetic Data	Artificially generated data mimics real-world conditions. Used to test rare or extreme scenarios, boundary conditions, or when real data is unavailable. Quality checks are needed to confirm data validity.	Testing rare scenarios, low data availability, peer group deviations, and high-risk transactions. Generating realistic customer profiles and transaction data for testing.
Predictive Rules	Historical data from known SARs and STRs is analyzed to train models. Analytical methods like Random Forest or logistic regression are used to identify patterns and risks across datasets.	Combining multiple rules for complex scenarios. Detecting hidden risks and anomalies that may not be immediately apparent.

Source: Original for this publication.

5.3.1.3 The Importance of Public-Private Partnerships in Focusing Detection Efforts

Public-private partnerships are useful for effective monitoring because they enable FIs and government agencies to share intelligence, typologies, and red-flag indicators that may otherwise remain siloed. This collaboration can improve the quality of detection rules, enhance investigative efforts, and accelerate the identification of suspicious activity, all under the larger aim of maintaining a common understanding of risk between the public and private sectors (in line with the FATF's Immediate Outcomes 1, 3, and 4).

A case documented in the Egmont Group's "Best Egmont Case Award Book" from 2021-2023 illustrates the impact of public-private partnerships and information sharing. The case study below highlights how enhanced public-private information led individual FIs to share financial intelligence that later led to the disruption of a human trafficking network and arrests (Egmont Group 2024, 33–34).

5.3.2 Strategies for Improving Quality of Alert Reviews and Investigations

As previously noted, many FIs face a challenge in managing the volume of alerts requiring manual review within required regulatory timeframes. This challenge results in significant costs for FIs and imposes regulatory and audit challenges if alerts cannot be reviewed in required time frames or with sufficient rigor.[48] While many of these challenges can be addressed by refining detection rules and their parameters, FIs can also improve the effectiveness and efficiency of their alert review and investigation processes through the use of more efficient review stages, coupled with defined procedures, technology to facilitate alert reviews and investigations, the use of composite alert risk scoring, and suppression of alerts.

Factors that contribute to these delays include the following:

- Legacy systems that generate high alert volumes and excessive false positives, overwhelming teams
- Lack of automation, which makes reviews, investigations, and documentation slow and labor-intensive
- Staffing shortages or high turnover that create backlogs
- Complex cross-border or multientity cases that require more time for analysis and evidence gathering
- Accessing data spread across multiple systems, which can consume up to 90 percent of investigation time
- Inefficient workflows and outdated case management tools that cause further delays.

CASE STUDY • Egmont Group Featured Case Study on Public-Private Partnership in Disrupting Human Trafficking

An FIU issued a request to domestic banks for SARs and STRs for unusual activity linked to named individuals and legal persons. Several banks responded with SARs and STRs showing frequent small deposits from multiple regions, rapid cash withdrawals, and payments to travel agencies and accommodation providers. The FIU consolidated this intelligence and shared it with law enforcement, enabling the jurisdiction's authorities to map the trafficking network's financial flows, freeze accounts, arrest key perpetrators, and identify additional victims. This case demonstrates that structured cooperation between public authorities and private institutions can focus private-sector monitoring efforts and result in usable financial intelligence.

48 From a regulatory perspective, authorities expect reviews to be started and/or completed within specific timeframes (with some jurisdictions setting timelines as short as several days with others closer to 30 days).

The following sections provide examples of strategies taken to close low-priority alerts and conduct complex investigations when needed.

5.3.2.1 *Refining Alert Review Stages*

Industry practice related to alert disposition typically involves multiple levels of reviews with each reflecting a different depth of analysis. This tiered approach creates a triage system that prioritizes high-risk cases for immediate, expert attention while allowing low-risk alerts to be resolved more quickly or by less specialized staff. This approach can reduce time spent reviewing false positives, facilitate investigations and enable resources to focus on high-impact cases. However, many FIs continue to only have one level of alert review or spend significant time on low-impact cases, which introduces a risk of missing suspicious activity.

Table 5.14 outlines the typical alert review process adopted by FIs and several considerations for improving processes:

TABLE 5.14 • Typical Alert Review Stages

Step and Purpose	Best Practice
Level 1 (L1) – Initial Review Review the alert and quickly determine if it can be dismissed as a false positive or requires escalation. The initial review is typically completed within 1-5 days of the alert generation. All alerts enter L1 stage.[49]	• Utilize alert risk scoring to prioritize and possibly even immediately escalated high-risk alerts) • Utilize workflow tools so that alerts are automatically routed to individuals for review • Enrich the data accompanying the alert by including customer profile and transaction data • Consider suppression techniques to triage likely false positives or recurring alerts • Aim to close or escalate most alerts in minutes • Document rationale for escalation/closure
Level 2 (L2) – Case Investigation[50] Conduct a deeper analysis of alerts escalated by L1 and determine if the alert warrants a complex investigation and/or filing of an SAR or STR. Approximately 10-25 percent of alerts enter L2 stage.	• Assign to experienced investigators • Utilize workflow tools to assign alerts to experienced investigators • Enrich the data accompanying the alert with additional information (such as CDD) • Apply link or network analysis (to visualize relationships between entities) • Document rationale for escalation/closure • Determine if requires complex investigation or automatically proceed to SAR/STR submission • Provide ongoing feedback to L1 regarding productivity of escalations
SAR and STR Submission Prepare and submit an SAR or STR to the FIU (within timelines required locally). Approximately 1-3 percent of initial L1 alerts result in a SAR or STR (although figures differ within the industry).	• Follow jurisdiction-specific guidelines and timelines required to file SAR or STR • Use clear, factual language and include relevant facts, transactions, and parties • Maintain confidentiality and take measures to avoid "tipping off" the customer • Keep an internal copy and document rationale for escalation/closure • Provide ongoing feedback to L2 regarding productivity of escalations

Source: Original for this publication.

49 Benchmarks vary by the entity type (for example, bank vs. NBFI) and nature of products, services, and customers. For example, alerts generated from retail banking often have higher L1 auto-closure rates than alerts generated for correspondent banking, which can involve more complex typologies and operations.

50 Many FIs have additional levels of review (such as L1, L2, and complex investigations, particularly if investigated activity is indicative of a network of illicit actors.

FIs should utilize written procedures that define process steps, minimum investigative steps depending on the stage, criteria for making escalation or false positive decisions, and quality assurance processes.

5.3.2.2 *Utilizing Alert Risk Scoring to Prioritize Alerts*

Many FIs also use alert risk scoring (also known as "composite risk scoring") to prioritize alerts. Alert risk scoring is the process of assigning a numerical or categorical score to each monitoring alert based on its risk characteristics, enabling FIs to prioritize investigations and allocate resources more effectively. Instead of treating all alerts equally, alert risk scoring uses defined criteria (for example, customer risk rating, transaction characteristics, and typology matches) to rank alerts from low- to high-risk. Alert risk scoring offers several benefits, including the following:

- **Prioritization**, by focusing investigative resources on the highest-risk alerts
- **Efficiency gains** through reducing backlogs and improving case turnaround times
- **Reducing unnecessary analysis** of low-risk cases by suppressing alerts below a threshold
- **Consistency**, by applying uniform criteria across all alerts, reducing investigator bias
- **Enabling direct routing** of higher-risk alerts to more experienced investigators
- **Ability to initiate** other activities, such as conducting updated CDD or EDD over a customer.

As opposed to generating alerts based on a simple trigger (such as a transaction exceeding a specific value), composite risk scoring evaluates multiple risk factors simultaneously, ultimately producing a more nuanced view of risks that helps prioritize high-risk activity and reduce false positives.

The following examples illustrate the benefits of applying composite risk scoring in two instances:

TABLE 5.15 • Examples of Alert Risk Scoring

Rule	Traditional Threshold Trigger	Composite Risk Score Method	Benefits of Composite Risk Scoring
Wire to High-Risk Jurisdiction	Every international wire transfer exceeding $50,000 to a high-risk jurisdiction triggers an alert. This rule often results in numerous alerts, including for customers whose transfers are legitimate and consistent with their profiles.	The system assigns weighted scores based on several dimensions. For instance, a base score of 50 points for any international transfer to a high-risk jurisdiction and an additional 20 points for repeat transfers within 30 days. In this case, a repeat transaction would be assigned a score of 70, placing it in the "escalated case" range for senior analyst review.	Rather than treating every transaction equally, the model prioritizes repeated or patterned activity, focusing investigator attention where the risk is elevated. This targeted approach improves efficiency and can enable more consistent, risk-based decisions.
Early Loan Repayment	Any loan repaid within 30 days might trigger an alert assuming early repayment could indicate layering or misuse of funds. In practice, however, many such repayments are made by short-term borrowers or small business customers with legitimate reasons and present lower risks.	The same transaction starts with a base score of 15 points. If the customer is identified as a PEP, a multiplier of 1.5 is applied, resulting in a final score of 22.5 - below the escalation threshold. The system records the event but does not generate an alert. An escalation would occur only if additional high-risk factors are present such as multiple early repayments, third-party repayment, or links to high-risk jurisdictions, which would raise the cumulative score above the escalation threshold.	This approach captures meaningful risk patterns while avoiding unnecessary alerts, improving both precision and operational efficiency.

Source: Original for this publication.

Table 5.16 below offers guiding principles for FIs in implementing and applying alert risk scoring.

TABLE 5.16 • Guiding Principles for Applying Alert Risk Scoring

#	Step	Description	Example or Considerations
1	**Define Clear Criteria**	Identify measurable factors that influence alert risk. Each rule must generate a score when triggered.	Typical scoring factors include customer risk rating, transaction value, geography, product type, and typology match.
2	**Assign Weights**	Assign greater weight to factors with higher risk impact to reflect their relevance in overall scoring.	Consider factors such as frequency and/or severity of occurrence (for example, if repeated behavior) and customer profile (for example, high-risk customers).
3	**Set Risk Thresholds**	Define ranges that determine escalation actions, either numeric (score-based) or tiered (that is, low, medium, or high risk).	Example: 0–29 = No case; 30–59 = low risk (alert review); 60–99 = medium risk (escalation); 100+ = high risk (escalation and increased likelihood of SAR or STR).
4	**Consider Multipliers**	Use additive or multiplier logic to emphasize elevated risks.	Examples: PEP customers multiply total score by 1.5. Repeat frequency (for example, 3 times in 90 days) adds 20 points.
5	**Develop Decision Protocol**	Develop structured escalation procedures linked to score ranges. Embed them within system workflow.	Example: 0–29 = no case, but system logs for statistical learning only; 30–59 = alert created, analyst reviews and escalates or closes with justification; 60–99 = case is escalated and requires senior analyst approval; 100+ = full investigation and likely STR or SAR.
6	**Automate Scoring in System**	Integrate the scoring model within the transaction monitoring or case management system.	Apply scores automatically at alert creation for realtime prioritization.
7	**Test and Validate**	Evaluate the accuracy and effectiveness of scoring logic using historical data and confirmed cases.	Compare scores to past SARs or STRs and investigation outcomes to verify accuracy and reliability.
8	**Document Rationale**	Maintain clear documentation of scoring logic, weighting decisions, and threshold settings.	Maintain an audit trail for internal and regulatory reviews.
9	**Review and Adjust**	Periodically reassess scoring parameters and thresholds as risks, typologies, or business models evolve.	Review at least quarterly or following major risk events or regulatory or internal audit findings.

Source: Original for this publication.

5.3.2.3 Utilizing Suppression of Alerts

Many FIs also utilize suppression mechanisms for monitoring alerts. Suppression in monitoring is the automated dismissal of alerts that meet predefined, low-risk criteria without requiring manual analyst review. It is designed to filter out false positives (for example, alerts triggered by lower-risk transactions) so investigators can focus on higher-risk cases. Suppression In monitoring is similar to suppression used for name screening, but instead of matching names against watchlists, it applies rules to transaction data and customer activity.

Table 5.17 offers guiding steps for FIs adopting alert suppression.

TABLE 5.17 • Guiding Steps for Applying Alert Suppression Techniques

#	Step	Description	Example or Considerations
1	**Identify Low Risk Alert Types**	Determine which alerts consistently prove to be false positives.	Review historical alert data. Select patterns with no SAR or STR filings (for example, routine payroll deposits from lowrisk customers).
2	**Define Closure Criteria**	Set measurable parameters that must all be met for suppression.	Use transaction type, amount range, customer risk rating, geography, and product. Exclude highrisk profiles and jurisdictions.
3	**Enrich with Contextual Data**	Integrate customer and transaction context before suppression logic.	Combine CDD information, historical transaction behavior, sanctions screening, and product risk to validate that the alert poses minimal risk.
4	**Build Rule Logic in Systems**	Configure suppressed rules within the monitoring systems.	Apply "if/then" conditional logic to automatically close qualifying alerts upon generation. Set exceptions for borderline or ambiguous cases, routing them for manual review.
5	**Document and Embed Governance**	Ensure rule design, testing, and approval processes are properly documented and governed.	Maintain an audit trail, record all rule parameters and rationales, and require necessary approvals before deployment. Store documentation in case management system.

Source: Original for this publication.

Table 5.18 provides an example of a suppressed rule in practice.

TABLE 5.18 • Example of Suppressed Rule in Practice

Scenario	Suppressed Rule	Outcome
A retail bank's transaction monitoring system is configured to flag all cash deposits exceeding $5,000. Through historical analysis, the bank determines that deposits between $5,000 and $6,000 made by salaried employees classified as "low risk" consistently occur on standard paydays (the 15th and 30th of each month) and have never resulted in a SAR or STR filing over two-year review period.	Based on this evidence, the bank establishes a suppressed rule that applies when all the following parameters are met: • Customer risk rating: Low • Transaction type: Cash Deposit • Amount: $5,000–$6,000 • Date: Within two days of the 15th or 30th of the month • Rationale: Historical testing confirms 100 percent of alerts in the past two years were determined to be false positives	Under this configuration, qualifying alerts are closed within seconds, freeing investigators to focus on genuinely suspicious activity. However, the suppressed rule remains subject to documented rationale, periodic retesting, and quality assurance reviews to ensure that true positives are not inadvertently dismissed as false positives.

Source: Original for this publication.

5.3.2.4 Building Human Capital and Expertise

Effective transaction monitoring relies not only on technology but also on skilled analysts that interpret alerts and make informed decisions. To build expertise of internal staff, FIs can consider the following practices:

- **Deliver onboarding training** for analysts and other monitoring staff, covering typologies, rule mapping to typologies, system navigation, regulatory requirements, investigative techniques, and escalation protocols.

- **Offer regular refresher courses** focused on new products, emerging ML/TF typologies, regulatory changes, and updates to the monitoring system features and workflows
- **Implement cross-training initiatives** to ensure that multiple team members are proficient in critical functions, supporting business continuity during absences or staff transitions
- **Facilitate participation in industry forums**, **knowledge-sharing networks** and public-private partnerships (where applicable), so that analysts and investigators can stay abreast of emerging risks and evolving best practices
- **Establish and maintain clear desktop operating procedures**, providing step-by-step guidance for analysts and staff tasked with reviewing system alerts and conducting investigations. Written procedures help standardize reviews, improve accuracy, support regulatory compliance, and enable transitions during staff absences or turnover
- **Apply quality control over output from new analysts**, with team leads or experienced investigators reviewing all alert decisions and analysis until staff are trained and exhibit low error rates

IFC has also seen a practice, particularly in mid-sized or larger FIs, of creating teams that mentor other staff, share best practices, and share insights from recent alert reviews or case investigations. Many FIs also share practices with peer institutions, particularly in the context of public-private partnerships or working within an industry association.

5.3.2.5 Utilizing Tools to Support Complex Investigations

Complex investigations in transaction monitoring often involve large volumes of data spread across multiple systems, intricate cross-border transaction flows, and networks of related entities. Investigators can spend much of their time gathering and reconciling information rather than analyzing it, leading to delays and potential missed risks. Leveraging advanced technology tools—such as link analysis, geospatial mapping, and automated document retrieval—can streamline data access, reveal hidden connections, and highlight unusual patterns. By embedding these capabilities into the investigative workflow, FIs can overcome data fragmentation, accelerate case resolution, and focus resources on the highest-risk alerts.

Table 5.19 highlights several technology-enabled offerings to support complex investigations.

TABLE 5.19 • Technology Options for Complex Investigations

#	Technology	Purpose	Best Practice
1	**Link Analysis and Network Visualization**	Map relationships between accounts, counterparties, and transactions to identify hidden connections.	Use to detect mule networks, layered transactions, and beneficial ownership links. Integrate with case management for realtime updates.
2	**Data Enrichment in Case Management**	Consolidate KYC, sanctions, and historical transaction data into a single investigative view.	Automate data pulls from multiple systems. Ensure enrichment includes customer risk ratings, typology matches, and past alerts, SARs, or STRs related to the client.
3	**Geospatial Mapping**	Visualize transaction flows and geographic clusters to spot unusual routes or highrisk corridors.	Overlay with jurisdiction risk ratings. Use to detect cross-border structuring or tradebased money laundering patterns.
4	**Pattern Recognition and Machine Learning Models**	Identify anomalies and suspicious patterns that rules may miss.	Train models on historical SAR and STR cases. Regularly retrain to adapt to emerging typologies.
5	**Automated Document Retrieval and OCR**	Quickly extract and search data from trade documents, contracts, and payment records.	Integrate OCR into transaction monitoring systems. Use keyword and entity recognition to flag relevant content.

Source: Original for this publication.

5.3.2.6 Incorporating Monitoring Outcomes

The primary outcome of an investigation is a determination of whether to file an STR or SAR (which is required within regulatory time frames). As noted, technology can enable FIs to generate draft SAR or STR filings or narratives to speed up the filing process. Even if an FI is not considered a required reporting entity in its home jurisdiction, the results of suspicious activity monitoring can support the FI in its risk management efforts.

For example, IFC has observed a practice of multiple SARs or STRs within a specified period as leading to a customer exit conversation and/or resulting in a temporary increase in the customer risk rating or other product or transaction volume limits. The results of suspicious activity monitoring can also inform the FI's risk assessment, alignment with risk appetite, customer due diligence practices, and future monitoring thresholds.

In addition, the results of monitoring can provide valuable information for FIs to comply with FATF Recommendation 16 related to payment transparency and vice versa. In June 2025, the FATF published updates to FATF Recommendation 16 and accompanying explanatory note that clarified among others, that "information received on the intended beneficiary should inform beneficiary financial institution's monitoring, with the objective of detecting misdirected payments (e.g. due to possible money laundering, fraud, or error)" (FATF 2025f). As per the updated FATF Recommendation 16, the outcome of monitoring should feed directly into risk based follow up measures.

5.3.3 Strategies to Monitor and Continuously Improve Effectiveness

The following sections provide several governance considerations, such as practices for managing rule updates, building internal capacity, and monitoring the effectiveness of a monitoring program.

5.3.3.1 Program Governance

Effective transaction monitoring requires strong governance to ensure technology is used appropriately, rules are risk-aligned, and operational processes are efficient. Strong governance combines detailed policies, clear roles and responsibilities, documented authorization paths for system changes, and technology with reporting processes.

Table 5.20 outlines key governance elements, their importance, and the role of technology.

TABLE 5.20 • Key Governance Considerations for Suspicious Activity Monitoring

#	Practice	Best Practices
1	**Rule Management**	• Ensure rules are based on reliable typology intelligence, customer risk ratings, and product or geography risk • Establish a process to periodically review and update rules to reflect emerging risks • Utilize case management and transaction monitoring platforms to centralize rule libraries, automate updates, and ensure approved rules are deployed • Monitor time required to implement rule changes • Implement version control to track rule versions and their application history
2	**Defined Roles and Escalation**	• Establish clear responsibilities and escalation paths for investigating transaction monitoring alerts • Utilize workflow and case management systems to automate alert routing, track investigative actions, and ensure proper escalation to authorized personnel

#	Practice	Best Practices
3	**Audit Trail and Documentation**	• Mandate comprehensive documentation of alert review, investigation, and decision-making steps • Utilize case or document management tools to securely store investigation records, maintain logs, and facilitate efficient retrieval for audit purposes
4	**Investigation Standards**	• Implement standardized procedures, templates, and checklists for investigations to reduce human error and promote consistency • Utilize investigation modules and case management systems to enforce standardized workflows and templates
5	**Reporting and Analytics**	• Conduct regular analysis of transaction monitoring outcomes, trends, and process effectiveness • Utilize case management and analytics tools to generate dashboards, reports, and trend analyses to support oversight and optimization

Source: Original for this publication.

5.3.3.2 *Utilizing Reporting (KRIs and KPIs)*

Another strategy for increasing the effectiveness of monitoring is the use of tailored reporting in the form of KRIs and KPIs (which does not require advanced or automated systems to provide benefit). Table 5.21 lists example KRIs and KPIs, how they are measured, their implications, and potential actions an FI could consider to increase the effectiveness and efficiency of monitoring processes.

TABLE 5.21 • Example KRIs and KPIs and Implications

KRI or KPI	Measurement	Potential Implications	Potential Actions
False Positive Rate The false positive rate is a key indicator of inefficiency in the monitoring process. It reflects the amount of noise generated by the system.	Divides the total number of alerts closed as a false positive over all alerts (that is, false positives ÷ all alerts). *For example*, if 800 alerts were closed as false positives out of 1,000 total alerts, the false positive rate is 800 ÷ 1,000 = 0.8, or 80 percent.	High percentages of false positives indicate inefficiency and excessive noise. Low percentages suggest overly strict thresholds that risk missing suspicious activity.	• Tune rules to reduce low-risk alerts • Apply contextual filters (for example, customer risk, geography, and product) • Use auto-closure for clearly low-risk scenarios
SAR or STR Conversion Rate The conversion rate (also known as the productivity yield) indicates the productivity of alerts in generating SARs and STRs.	Divides the total number of SARs or STRs filed by all alerts (that is, total SARs or STRs ÷ total alerts investigated). *For example*, 200 SARs or STRs from 5,000 alerts = 4 percent.	Low conversion may indicate poor alert quality or misaligned rules. High conversion suggests targeted detection.	• Review rules with low conversion rates • Focus on high-risk typologies • Enhance data enrichment to improve alert quality

KRI or KPI	Measurement	Potential Implications	Potential Actions
Alert Escalation Ratio The alert escalation ratio identifies if too few or too many alerts are escalated by level 1 (L1) to secondary review or investigations.	Divides the number of escalated alerts relative to all alerts (that is, level 2 or L2 alerts ÷ L1 alerts). *For example*, 500 escalations from 5,000 L1 alerts = 10 percent.	High escalation may indicate weak L1 triage. Low escalation may suggest overly strict L1 thresholds. IFC's experience is that industry benchmarks are approximately 10–25 percent of escalations.	• Strengthen L1 triage criteria • Train analysts on escalation standards
Average Case Resolution Time The average case resolution identifies if investigators are spending too little or too much time on cases (per level).	Divides the total time to close a case by the total number of cases (that is, total time to close cases ÷ number of cases). *For example*: 1,000 hours ÷ 500 cases = 2 hours per case.	Long resolution times may indicate complex cases or inefficient workflows. Short times with high false positives suggest poor alert quality.	• Route workflows to appropriate investigators • Use automation for data gathering to enable human time on analysis • Apply link analysis to speed investigations
Analyst Throughput The analyst throughput identifies whether analysts are reviewing too few or too many cases per analyst.	Divides the alerts reviewed per analyst per day (that is, alerts ÷ review days). *For example:* 1,000 alerts per 20 days = 50 alerts per day.	High throughput with high false positives may indicate rushed reviews. Low throughput may signal overly complex alerts or resource constraints.	• Balance workloads • Use workflow tools for even allocation • Provide training to improve efficiency

Source: Original for this publication.

The early establishment of KRIs/KPIs for suspicious activity monitoring can also provide an FI with an ability to evaluate how automated systems integrate into the broader AML/CFT risk management program and can enable an objective evaluation of the system's performance against established objectives.

5.3.3.3 *Leveraging System Effectiveness Testing*

While transaction monitoring systems play a critical role in detecting suspicious activity, ongoing vigilance is essential to address risks such as missed alerts (false negatives) or the inappropriate closure of alerts (particularly when suppression is used). Monitoring KPIs and KRIs assist in monitoring for emerging risks, but regular testing is necessary to ensure systems remain effective as customer profiles and transaction patterns evolve and as new risks and typologies emerge.

FIs should implement structured, documented testing programs that include the following:

- **Validating system performance:** Confirming that true suspicious activity is identified, false positives are within acceptable limits, and sensitivity scores are recalibrated as needed
- **Comprehensive testing approaches:** Incorporating preimplementation reviews using historical data, back-testing to discover missed alerts, parallel testing with legacy processes, and scenario testing with synthetic datasets
- **Cross-functional oversight:** Ensuring results are reviewed by compliance, IT, and business stakeholders, with reports retained for regulatory and audit purposes
- **A regular testing schedule:** Conducting reviews at least annually and after significant system upgrades, rule changes, or changes in risk profile.

Table 5.22 highlights key elements for FIs to consider when planning and executing ongoing testing of their monitoring systems.

TABLE 5.22 • Example Steps for Model Testing and Validation

#	Step	Key Activities
1	**Conduct Data Integrity Reviews**	• Verify the accuracy, completeness, and timeliness of data feeding into transaction monitoring systems • Ensure all relevant data sources (for example, customer profiles and transaction records) are integrated correctly
2	**Test Rule Configuration**	• Create test scenarios that simulate real-world transactions, including both legitimate and suspicious • Evaluate whether thresholds for alerts are appropriate using historical data and adjust them if necessary to reduce false positives and false negatives • Test the system's ability to detect unusual patterns or deviations from expected customer behavior
3	**Validate Alert Generation**	• Review the alerts generated to check if they are relevant and actionable • Test whether the system is flagging suspicious transactions accurately and not missing critical risks • Assess alert quality to minimize unnecessary investigations of false positives
4	**Perform Back Testing**	• Use historical transaction data to test the system's performance retrospectively • Compare the system's output against known cases of suspicious activity to evaluate effectiveness
5	**Conduct Stress Testing**	• Simulate high transaction volumes or complex scenarios to test the system's capacity and performance under pressure • Ensure the system can handle peak loads without compromising accuracy or speed
6	**Evaluate System Updates**	• Test the system after updates or changes to ensure configurations, rules, or features work as intended • Validate that updates do not introduce errors or reduce the system's effectiveness
7	**Consider Data from KPIs**	• Monitor KPIs (for example, number of alerts generated, percentage of false positives and false negatives, and time taken to investigate alerts)
8	**Obtain Feedback from Users**	• Ensure staff involved in monitoring and investigating alerts are trained on system updates and testing results • Gather feedback from users to identify areas for improvement in the system's usability and functionality

Source: Original for this publication.

Ultimately, robust model validation is critical to balancing compliance with operational efficiency. As an added best practice, some FIs periodically engage independent consultants and external auditors to test and validate key systems.

5.3.4 Considerations for Implementing Machine Learning and AI

As noted throughout this Good Practice Note, emerging market FIs are increasingly leveraging machine learning and AI to strengthen monitoring and identify complex suspicious activity patterns. FIs use machine learning and AI to both expand detection of potentially suspicious activity

as well to review alerts (and, in some cases, suppress alerts that meet certain lower-risk criteria). However, migrating from traditional rule-based solutions to advanced technologies requires planning, governance, and readiness across data, people, and processes. FIs must be prepared to explain (to management, regulators, and key third parties) how risks associated with the migration process are considered and managed (to build trust and support for responsible innovation.

5.3.4.1 Process Steps for Implementing Machine Learning and AI in Suspicious Activity Monitoring

Table 5.23 offers a typical roadmap and best practices for FIs considering utilizing machine learning and AI in transaction monitoring.

TABLE 5.23 • Migration Phases for Machine Learning and AI Monitoring

Phase	Key Actions	Best Practices
Phase 1: Preparation	• Conduct a comprehensive data audit (for example, transaction, KYC, and cases) and address data gaps, inconsistencies, and quality issues • Define the intended role of the new automated monitoring platform in meeting broader program objectives • Engage regulators early to discuss migration plans and expectations • Define governance framework and assign roles and responsibilities	• Prioritize data quality (as well as personal data protection and ethical use of data) before model development • Document all decisions and assumptions • Plan for user acceptance testing (UAT) • Build trust through transparency and proactive communication
Phase 2: Pilot	• Select a limited, lower-risk segment or product line for initial machine learning and AI testing • Develop hybrid models combining rules-based scenarios with machine learning outputs • Train staff on interpreting AI-driven alerts • Monitor performance metrics (false positives or negatives and detection rates)	• Conduct UAT • Keep pilots small and controlled • Use explainable AI techniques to ensure transparency • Involve compliance and investigative teams early
Phase 3: Rollout	• Gradually expand machine learning and AI coverage to additional products, geographies, or customer segments • Integrate models into production systems with full audit trails • Update policies and procedures to reflect new workflows • Maintain ongoing regulatory communication	• Scale the model in stages to manage model risks and broader operational risks • Ensure investigators have access to model logic and alert rationale • Keep governance documentation current
Phase 4: Optimization	• Continuously monitor model performance and adapt to evolving typologies • Conduct periodic revalidation and sensitivity testing • Update data sources and retrain models as needed • Review governance framework annually	• Use feedback loops from investigators to refine models • Track emerging threats and adjust parameters • Maintain a culture of continuous improvement

Source: Original for this publication.

5.3.4.2 The Importance of Proactive Communication with Regulators and Critical Third Parties

Migration to machine learning and AI can heighten expectations for regulatory oversight. Sustained, transparent communication with regulators and other key stakeholders is essential, particularly during system migration.

Best practices for engaging with regulators (and key third parties) include the following:

- **Early and ongoing engagement:** Initiate dialogue before starting the transition. Share technology goals, expected benefits, risks, and project timelines, and provide updates at key milestones
- **Detailed documentation:** Supply materials covering model design, development, data hygiene, governance, and risk assessments. Document the rationale for model selection, training, validation, and monitoring approaches
- **Highlight fallback plans and model validation Plans:** Present evidence of performance metrics (including false positive and negative rates), underlying data quality, independent validation, and fallback measures, such as parallel monitoring (i.e., continuing to monitor using preexisting systems) that will be used during rollout
- **Change management transparency:** Explain plans for system rollouts, pilot phases, data quality improvements (if needed), and staff training, as well as how the FI will handle unexpected model behavior or alert anomalies
- **Ongoing monitoring and reporting:** Commit to regular reporting on model performance, effectiveness, and tuning activities, especially after significant updates or system changes
- **Model explainability:** Support transparency by adopting explainability frameworks and other tools that clarify how decisions are made
- **Maintaining a detailed audit trail:** Record decisions, communications, testing results, and regulatory interactions. Make records accessible for inspection to demonstrate continuous oversight
- **Highlighting the benefits:** Signal that migrating to machine learning and AI enables more detection of relevant suspicious activity that may not otherwise be captured through traditional models.

Machine learning–enabled systems and tools have been present in emerging markets for several years. As an example, representatives from an FI interviewed by IFC shared several lessons learned from its experience building a system internally and explaining that model to internal stakeholders, regulators, and third parties, detailed in the following case study. Refer to Chapter 9.1.4, "Evolution of Artificial Intelligence" for additional information on the use of AI in AML/CFT controls.

CASE STUDY • Maintaining Dialogue in Developing a Machine Learning-Based Model for Suspicious Activity Monitoring

OBJECTIVES: A bank located in Latin America sought to increase the effectiveness of its rules-based monitoring and limit the number of false positives (so that investigators could focus on high-risk alerts) through machine learning and data analytics.

SOLUTION: The bank developed its own internal system (after determining that "building" enabled greater flexibility to allow it to adapt to emerging risks and business changes). The bank was able to do so due to advanced IT and analytics culture and capabilities, which included having data scientists within the bank's AML Department and support from senior management to invest in technology and innovation. The bank ultimately developed a transaction monitoring system utilizing machine learning and AI that adopted composite risk scoring and alert suppression, which improved efficiency by over 80 percent.

SOLUTION DEVELOPMENT: The bank's representatives explained that the first initial challenge was internal credibility (as machine learning within AML/CFT was then emerging). The bank had to conduct a pilot to demonstrate the benefits, and with the results, was able to gain trust and support from management and key internal stakeholders. The next challenge was explaining the benefits to its regulators and supervisors. To address these challenges, the bank maintained thorough communication with its regulators and conducted regular internal and external testing to ensure the model functioned as intended and was aligned with international best practices. The bank also implemented a continuous monitoring strategy to determine if models, monitoring systems, or rules require calibration.

LESSONS FOR OTHER FIS: When asked about best practices and lessons learned to share with other FIs, the bank's representatives stated: "Technology is a means, not an end. In the development of risk management, it is crucial to connect with the contexts and incorporate all new knowledge and methods into the technology" and encouraged banks to "focus communication on the benefits of the technological upgrade to align the expectations of stakeholders."

Source: An FI interviewed by IFC

6

Practices for Utilizing Manual Controls

Many FIs, particularly those with smaller customer bases or limited product offerings, can meet regulatory requirements using manual processes and/or less advanced technology. This approach works well when supported by clear procedures, appropriate oversight, and a sound understanding of risk exposure that align with the FI's risk profile. Even without advanced automated technology solutions, there are opportunities for FIs to leverage accessible technology without incurring substantial costs. However, as FIs grow and become more complex, relying solely on manual processes and basic technology can constrain efficiency, consistency, and the ability to demonstrate control effectiveness. Chapter 6 expands on prior chapters with the goal of assisting FIs that must rely on manually deployed controls and lower-cost technology to improve effectiveness and efficiency.

Among other topics, Chapter 6 will address the following:

- What low-tech options for AML/CFT currently exist?
- When might manual controls be appropriate?
- How can FIs conduct manual screening and suspicious activity monitoring?
- When is outsourcing an option and how should it be managed?
- When should FIs migrate to automated solutions and advanced technology?
- What are some examples for NBFIs such as microfinance institutions?

6.1 Practices for Utilizing Manual Controls and Low-Tech Tools

The following sections provide examples of low-tech tools, outline considerations for using manual processes (particularly in screening and monitoring), discuss when and how to outsource certain controls, and provide strategies for transitioning from manual controls to automated solutions.

6.1.1 Low-Tech Tools and Use Cases in AML/CFT

Even without advanced systems, FIs can meaningfully strengthen AML/CFT controls utilizing existing tools within the institution, such as preprinted forms and instructions, spreadsheets, sanctions screening databases, and low-code automation platforms. These solutions offer several benefits, including cost efficiency (as most tools require no additional licensing), more simple development and maintenance, potential alignment with risk profile (for FIs with lower inherent risk), and rapid improvements in operational effectiveness.

Table 6.1 highlights examples of "low-tech" tools, use cases, and key considerations.

TABLE 6.1 • Example "Low-Tech" Tools and Use Cases

Tool	Use Cases	Key Considerations
Digital Forms[51]	• Onboarding forms • Requests for information	• Capture standardized data digitally to reduce manual errors • Use validation checks and dropdowns to ensure completeness • Add conditional fields to improve accuracy and user experience
Spreadsheets	• Transaction monitoring • CDD records • Case management • Risk assessments • Customer risk rating	• Structure data for easy filtering, searching, and consolidation • Use dropdowns, color coding, and conditional formatting to flag risks • Maintain templates for transaction reviews and case outcomes • Support case management through structured templates that record transaction details and outcomes
Spreadsheet Formulas	• Transaction monitoring • Risk assessments • Customer risk rating	• Automate calculation of risk ratings via formulas • Use color coding and conditional formatting to visually flag high risks • Use lookups to check against sanctions and PEP lists • Summarize data for trend and risk analysis
Cloud Storage	• Recordkeeping	• Store documents securely in compliance with recordkeeping requirements • Organize files in structured folders for quick retrieval during audits • Choose private or public cloud based on legal requirements

51 In certain cases, FIs may only have the option of utilizing printed forms. Printed forms pose several drawbacks (such as the inability to query data in a standardized format) but are still utilized in some instances (particularly in the context of customer onboarding). When utilized, printed forms should include all required fields, highlight critical fields for clarity, and be accompanied by checklists to guide consistent data entry and corresponding risk rating.

Tool	Use Cases	Key Considerations
Graphics Tools	• Transaction monitoring • Management reporting • Customer risk rating	• Visualize transaction patterns and anomalies • Use dashboards to track case progress and investigation stages • Highlight trends for management reporting
Email	• Requests for information • Customer onboarding • Escalation	• Categorize and filter emails by compliance topic • Use group mailboxes and rules to route messages efficiently • Set reminders for deadlines and required actions
Workflow Tools	• Transaction monitoring • CDD and KYC reviews • Screening alert reviews	• Use built-in automation to route tasks or approvals • Standardize review steps to ensure consistency • Track case status for timely resolution
Internet Searches	• CDD • PEP and adverse media • Customer risk rating	• Use internet searches to identify adverse media linked to financial crimes • Use internet searches or maps to verify information (for example, location) • Use internet searches to identify PEPs or associations with PEPs

Source: Original for this publication.

6.1.2 Deploying Manual Controls in CDD, Monitoring, and Screening

Manual controls are most effective when volumes and inherent risks are low. For certain small FIs, manual controls can meet AML/CFT obligations if they are consistent, documented, and subject to oversight. However, as customer numbers grow, transactions become more complex, or regulators require faster processing, these controls should be supplemented or replaced by automation. Table 6.2 outlines practical actions for performing key AML/CFT controls without advanced systems.

TABLE 6.2 • Considerations for Deploying Manual Controls

#	Approach	Control Suggestions
Customer Due Diligence		
CDD	• Standardize onboarding forms or checklists • Color-code mandatory fields to ensure completion • Prepopulate standardized forms with data such as onboarding channel and product • Collect and check authenticity of government-issued ID and proof of address • Attach document copies and record verifier's initials • Use spreadsheets to calculate and record customer risk ratings • Gather UBO information via standardized forms • Obtain senior officer approval for high-risk customers	• Perform dual review of forms for accuracy checks • Conduct periodic spot checks to correct errors • Validate mandatory fields before account opening • Use a checklist to confirm required UBOs identified • Cross-check ownership against public or company records • Apply clear criteria for when cases should escalate to EDD • Deliver refresher training to staff annually

#	Approach	Control Suggestions
EDD	• Request additional documents for high-risk customers (for example, source of funds and business activity) • Document reason for highrisk classification and EDD • Obtain senior management approval before opening	• Use checklist for required documents • Apply clear criteria for when EDD is applied • Maintain audit trail of all EDD steps
Ongoing Due Diligence	• Schedule periodic reviews in accordance with risk rating (for example, every 12 months for customers rated High Risk) • Use spreadsheets to track completion rates (prioritizing higher-risk customers) • Use checklists to confirm if documents are current and updated	• Set automated reminders via calendar or email • Track completion in review logs • Conduct sample-based quality assurance checks • Escalate overdue reviews
Name Screening and Transaction Screening		
Sanctions	• Use publicly available or subscription-based sanctions lists (ideally in spreadsheet format, if possible)[52] • Manually search customer names during onboarding and periodically thereafter • Apply phonetic variations and common aliases to improve match detection • Record search date, source, and results in customer file	• Update sanctions lists periodically or as changes are published • Use checklists to document that required steps were followed • Perform dual reviews of potential matches • Escalate confirmed matches to compliance • Record the date and/or save records of the list at that time
PEP	• Maintain a list of PEPs, PEP associates, and close relatives from public sources or vendor data • Manually search customer names during onboarding • Document relationship type (domestic, foreign, or international organization) and risk level • Record search results and reviewer's initials	• Update PEP list regularly • Use checklists to document that required steps were followed • Escalate potential matches for EDD • Conduct sample-based quality assurance checks
Media	• Use internet search engines and news databases to check customer names for negative news • Apply search terms combining name with keywords (for example, "fraud," "money laundering," and "sanctions") • Save relevant articles or screenshots in customer file. • Document search date, sources, and findings	• Use standardized search terms and sources for consistency • Conduct periodic spot checks to assess search quality • Escalate cases with adverse findings for review • Maintain audit trail of all searches and outcomes
Payments	• Manually review payment details against sanctions lists before processing • Check beneficiary names, banks, and jurisdictions • Verify cross-border payments against high-risk jurisdiction lists • Record screening results and reviewer's initials	• Maintain current lists for sanctions and high-risk jurisdictions • Use checklists to document that the required screening steps were followed • Escalate suspicious or restricted transactions immediately • Perform periodic spot checks to confirm process adherence

52 The United Nations Security Council Consolidated List is available at https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list.

#	Approach	Control Suggestions
Suspicious Activity Monitoring		
Monitoring	• Download transaction data periodically (for example, weekly or monthly) • Use spreadsheet filters to identify red flags (for example, large cash deposits, multiple transactions just below thresholds, rapid fund movement, or high volume of activity) • Apply conditional formatting to highlight transactions that exceed limits and/or deviate from peer groups	• Record findings in review log with case reference, description, and outcome • Follow a documented process for when alerted activity should be investigated and for when investigated activity may be reportable
Alerts	• Produce alerts from monitoring or manual reviews • Verify alert details against customer records • Gather supporting documentation • Record investigation steps and findings in a case log • Escalate reportable and suspicious cases for potential SAR or STR filing	• Use standardized investigation templates • Perform dual reviews for high-risk or complex cases • Track case files monthly for completeness • Close alerts within defined timeframes • Sample closed alerts for quality assurance purposes
SAR and STR Filing	• Use preprinted SAR and STR templates or Excel forms to capture key information, such as customer details, nature of activity, activity details (for example transaction dates and amounts), investigation steps, date of filing, and narrative • Maintain secure SAR and STR log with case numbers, customer identification information, status, and submission dates • Restrict access to SAR and STR records to authorized personnel	• Apply access controls to SAR and STR files • Monitor logs for compliance with timing requirements • Follow a documented SAR and STR submission workflow • Train staff annually on SAR and STR confidentiality and handling procedures
Recordkeeping	• Store documents in labeled physical files or structured digital folders in a secure server or cloud • Maintain master control log with customer names, onboarding dates, last review dates, and next review due dates • Retain records per legal requirements	• Restrict access to authorized personnel only • Back up digital records at least weekly • Enforce retention policies consistently • Adopt record maintenance protocols that include retention policies (for at least five years)

Source: Original for this publication.

6.1.3 Considerations for Outsourcing AML/CFT Controls

Outsourcing can help FIs access specialized expertise, advanced technology, and additional capacity, enabling them to maintain effective controls even when internal resources are limited. In the context of AML/CFT, outsourcing refers to engaging an external service provider to perform certain functions on behalf of the FI, such as completing CDD, reviewing monitoring alerts, or reviewing screening alerts. However, while outsourcing can improve efficiency and scalability, the FI retains ultimate responsibility for compliance and must ensure strong oversight and governance of the outsourced activities. As such, FIs must conduct due diligence on the provider before entering into an agreement and monitor their work for alignment with established policies, procedures, and agreements.

Table 6.3 outlines several frequently outsourced AML/CFT controls, along with related governance practices.

TABLE 6.3 • Examples of Outsourced AML/CFT Controls and Governance Considerations

	Examples of Outsourced Controls	Rationale for Outsourcing	Governance Practices
CDD	• Identity and document verification • EDD for high-risk customers • Beneficial ownership verification • Ongoing customer profile reviews	Access to specialized verification tools and global data sources; ability to scale onboarding quickly.	• Define clear data security requirements • Ensure providers are trained and follow the FI's CDD policy or procedures and risk rating methodology • Conduct regular quality control or quality assurance • Subject outsourced resources to the FI's training • Maintain audit trail of outsourced reviews • Subject to internal audit as if it were internally performed
Screening	• Sanctions list screening • PEP list screening • Adverse media screening • Alert case management	Use of advanced screening platforms with uptodate global lists; reduction of manual workload.	• Validate lists and update frequency • Set and test match accuracy and thresholds • Maintain oversight of decisions on potential matches • Require reporting on metrics (for example, false positives) • Subject outsourced resources to the FI's training • Conduct regular quality control or quality assurance
Monitoring	• Alert review and triage • Case investigations • Batch transaction reviews • Drafting SARs and STRs	Gain investigative expertise and capacity to handle complex or large alert volumes efficiently.	• Set service-level agreements (SLAs) • Set clear timing expectations (for example, 24-hour review) • Require standardized documented steps • Conduct periodic quality assurance • Ensure reports meet deadlines • Retain final approval authority in-house • Subject outsourced resources to the FI's training • Conduct regular quality control or quality assurance
Others	• Enterprisewide risk assessments • Policy or procedure drafting • AML/CFT staff training	Access to independent expertise, fresh perspective, and regulatory best practices.	• Align assessments with risk appetite • Retain final policy approvals and ownership in house • Verify that content meets requirements • Subject outsourced resources to the FI's training • Conduct regular quality control or quality assurance

Source: Original for this publication.

Table 6.4 offers an example decision matrix for deciding whether to outsource AML/CFT controls.

TABLE 6.4 • Decision Matrix for Deciding Whether to Outsource AML/CFT Controls

Criteria	Low	Medium	High
Need Internal capability gap (for example, staff, skills, or technology)	Existing staff and tools can meet policy and regulatory timing requirements.	There may be some gaps in internal expertise or capacity, leading to occasional delays.	There are significant gaps in internal skills, technology, and capacity. Controls are at risk of failure.
Risk Impact on compliance risk and risk of control failures	Outsourcing adds minimal risk. The provider is proven, has experienced staff, and may even be regulated.	Outsourcing introduces some execution risk as the provider may have untested staff or high turnover.	Outsourcing introduces heightened execution risks as the provider may not have sufficient experience.
Cost Relative to the cost of deploying controls internally	Executing controls internally is cheaper and more sustainable than engaging a provider.	The costs are comparable to internal execution. Outsourcing offers moderate efficiency gains.	Outsourcing is notably less expensive than internally-deployed controls and is faster to implement.

Source: Original for this publication.

In general, FIs consider outsourcing when the "Need" criteria is considered "High," the "Risk" criteria is considered "Low" or "Medium," and the "Cost" criteria is considered "Medium" or "High." There are also instances where they may temporarily outsource some controls (for example, as an overflow capacity if there are temporary spikes in the number of alerts or an existing backlog of alert reviews). However, FIs should generally avoid outsourcing when the "Risk" is considered "High." In all cases, when outsourcing, FIs must document the decision rationale for outsourcing, establish clear contractual responsibilities, and monitor ongoing performance.

6.1.4 Considerations for Migrating Beyond Manual Controls

As FIs grow and regulatory expectations evolve, manual processes and low-tech tools may no longer be sufficient for the institution's operations and risk profile. Implementing more advanced technology can be essential for maintaining compliance, improving efficiency, and managing increasing risks.

FIs should consider transitioning to more advanced technology solutions when

- Scaling operations, such as an increase in customers, transactions, products, or branches
- Risk profile increases, such as by entering new markets or onboarding more high-risk customers
- Manual processes negatively impact customer experience or operations
- Regulatory expectations increase, requiring systemized processes and stronger controls; and
- Auditability becomes challenging, and stronger evidence of control effectiveness is required (to respond to evolving risks or regulatory requirements and expectations).

Table 6.5 highlights examples of when to consider adopting more advanced technology solutions.

TABLE 6.5 • Considering When to Migrate to Advanced Technology

#	Scenario	Technology Considerations
Alert Management and Monitoring Efficiency		
1	**High Volume of Screening Alerts with Low True Positives**	• Use automated screening tools with fuzzy logic • Maintain whitelist to reduce unnecessary alerts • Integrate tools (for example, screening providers) to internal systems via APIs • Align screening frequency with risk profile
2	**Unmanageable Manual Monitoring Reviews or Alert Backlog**	• Introduce case management tools • Use rule-based spreadsheets to filter transactions • Apply alert risk scoring to prioritize alerts • Adopt dynamic, risk-based rules • Use predefined rule libraries to save development time
3	**Increased Alerts Requiring SAR or STR Filing**	• Use alert prioritization and alert risk scoring (even via spreadsheets) • Implement workflow tools and email alerts for escalation and deadline tracking • Implement case management for investigations
4	**Increased Regulatory Pressure or Scrutiny or Findings**	• Centralize document storage for audit readiness • Automate template population for consistency • Track remediation progress (for backlogs) and test systems independently
Emerging Growth and Complexity		
5	**Expansion to High-Risk Jurisdictions or Customer Types**	• Implement automated monitoring solutions with advanced risk-based rules • Use real-time screening for high-risk products or geographies • If advanced systems are not feasible, use scripted spreadsheets for targeted monitoring scenarios
6	**Growing Customer Base with a Need to Improve Customer Experience**	• Use structured onboarding templates and enable online self-entry • Store documentation in centralized KYC systems to produce metadata • Enable network analysis to identify customer connections
7	**More Complex Products and Services (for example, Cross-Border Payments)**	• Update sanctions lists more frequently (for example, daily) for higher-risk products • Implement real-time screening for beneficiaries, geographies, and transactions
8	**Multiple Branches or Agent Locations**	• Centralize customer data to avoid duplication • Automate screening as data volumes grow • Deploy case management to meet geographic regulatory requirements

Source: Original for this publication.

Ultimately, FIs move from manual controls to automated monitoring and real-time screening when alert volumes, customer growth, or transaction complexity exceed the capacity of manual review, or when regulatory expectations demand faster, more consistent coverage and documentation. Persistent backlogs, high false positive rates, and expansion into higher-risk jurisdictions are also indicators that automation should be considered. Real-time screening is especially critical for high-risk transactions such as cross-border payments, where delays in identifying sanctioned parties can lead to compliance breaches or operational delays in upstream processing. Migration toward automation can be done in phases or for different functions (for example, focusing initially on suspicious activity monitoring), but FIs should consider the compatibility of the systems to avoid fragmented approaches.

7

Practices for Designing a Technology Selection Strategy and Selecting a Vendor Partner

The poor selection or implementation of an unsuitable technology solution can have far-reaching negative consequences, including operational disruptions, negative impacts on customer experience, and reduced profitability. Chapter 7 focuses on risks and pitfalls that arise during technology selection and strategic planning—the stage before deployment—and the measures FIs can take to ensure that technology is fit-for-purpose, adaptable, and aligned with institutional needs. Section 7.1 identifies both key outcomes that signal poor strategy or vendor selection and the root causes behind them. Sections 7.2–7.4 then outline best practices for designing a technology strategy, selecting vendors, and preparing for deployment, directly addressing the challenges outlined in 7.1. Chapter 8 subsequently provides practices for deploying a system and maintaining a system once operational.

Among other topics, Chapter 7 will address the following:

- What are the key challenges and common pitfalls when implementing technology solutions?
- What factors do FIs need to consider when developing a technology strategy?
- How do FIs determine whether to build technology or acquire from a vendor?
- What are the guiding principles for selecting a vendor?

7.1 Key Challenges in Technology Strategy and Selection

FIs often encounter multiple risks and challenges with technology selection and deployment that can undermine transformation objectives. Potential adverse outcomes experienced by FIs include the following:

- **New solutions fail to improve effectiveness and efficiency:** Detection quality or operational performance does not improve because underlying data or process issues remain unresolved
- **Selected technology does not meet current or future needs:** The system proves unsuitable for the FI's risk profile, creates gaps in coverage, and limits adaptability
- **Concerns from regulators stall deployment:** Concerns expressed by regulators could postpone rollouts of new systems and tools (particularly those leveraging new and emerging technology)
- **Failure to achieve full program benefits:** The FI's investment does not deliver the intended strategic, operational, or compliance results.

These challenges are often attributed to one or more of the following root causes:

- **Poor vendor selection:** Weak request for proposal (RFP) and request for quote (RFQ) processes, limited stakeholder input, and proprietary systems result in vendor lockin and restricted integration
- **Insufficient regulatory engagement:** Failure to involve regulators early, provide adequate documentation, and conduct thorough testing increases compliance risk
- **Poor data quality and readiness:** Incomplete, inaccurate, or fragmented data reduces system effectiveness at golive. FIs may fail to calibrate vendor-provided systems to their risk profiles and operating environments
- **Ignoring scalability and integration needs:** Selecting systems that cannot accommodate future products, geographies, or evolving AML/CFT requirements limits scalability and long-term compliance
- **Weak assessment of program readiness:** Selecting advanced technology without first strengthening governance, controls, and existing processes results in ineffective implementation and limits risk-management benefits
- **Weak communication with regulators:** Failure to proactively keep regulators (or other third parties) advised of key changes, rationale, and oversight gaps, and/or the inability to properly explain model and risk management outcomes undermines transparency and confidence in the technology's capabilities.

The following sections set out practical steps that FIs can take to address these outcomes and root causes—from building a fit-for-purpose technology strategy and engaging stakeholders to selecting capable vendor partners and preparing for effective deployment.

7.2 Designing an AML/CFT Technology Development and Use Strategy

Before procuring or deploying technology, FIs are encouraged to define an AML/CFT technology strategy that aligns with the overall business objectives, broader IT strategy, and the current and anticipated inherent risks faced by the FI. For context, the FATF's Recommendation 15 requires FIs to "identify and assess the ML or TF risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products." As an example, if an FI's strategic plan emphasizes growth in the use of digital delivery channels, per the FATF's recommendation, the FI's AML/CFT systems should be able to accommodate increased transaction volumes and new data sources, and,

if not require enhancements prior to the launch of new or developing technologies. While adherence with the recommendation requires risk management considerations beyond solely technological capabilities, a forward-looking technology enablement strategy can enable an FI to proactively grow while proportionally managing risks. However, the development of an effective strategy requires coordination between multiple areas (such as compliance, business lines, IT, and enterprise risk functions, among others) to ensure that design decisions reflect not only regulatory requirements but also inherent risks, operational realities, customer experience, and financial inclusion.

While this section does not offer an exhaustive list of decisions or components of an IT strategy, the section does highlight key considerations specific to AML/CFT technology implementation drawing on lessons learned from FIs that have undertaken technology-driven transformations.

A formal strategy document typically includes

- The **business rationale** for technology adoption, specifying regulatory, risk management, or operational drivers
- **Target outcomes and performance indicators** (for example, reduction in manual workload and improvement in detection)
- **Architectural principles** governing interoperability, data management, and cybersecurity
- **Decision criteria** for build vs. buy, cloud vs. on-premises, and legacy-system migration
- **Governance arrangements**, including steering committees, accountability lines, and change-control processes
- **Implementation roadmap and budget envelope** aligned to institutional priorities.

Some of the key decisions in formulating a strategy for AML/CFT technology include:

- **Build vs. buy vs. blend:** Whether to develop solutions internally, purchase commercial software, or pursue hybrid models
- **Cloud vs. on-premises deployment:** How to host applications given regulatory, security, and infrastructure constraints
- **Migration and decommissioning of legacy systems:** How to transition data and processes without disrupting ongoing compliance
- **Vendor partner selection and management:** How to identify, contract, and supervise external providers
- **Programmatic readiness and maturity:** Whether the FI's AML/CFT framework can absorb advanced technology and how to address foundational processes in connection with an upgrade.

The following sections offer guiding principles for these five key decisions.

7.2.1 Build vs. Buy vs. Blend

Determining whether to construct technology in-house, acquire a vendor product, or combine both approaches is among the earliest and most strategic choices.

Building solutions internally allows tailoring to specific workflows and contexts, but demands substantial development capability and long-term maintenance resources. Buying off-the-shelf technology offers faster deployment and access to proven functionality, yet may limit customization and create dependency on vendor updates. Blended models, such as integrating an in-house risk-scoring engine with a commercial case-management platform, can balance flexibility with speed, but require careful integration and governance.

Decision criteria typically include the following:

- **Strategic differentiation:** If AML/CFT capability is seen as a competitive advantage (for example, enabling faster onboarding or strengthened correspondent bank relationships), building or heavily customizing solutions may be warranted
- **Resource capacity:** FIs with mature IT teams and development pipelines can sustain in-house builds, whereas smaller FIs may need to rely on external vendors
- **Regulatory expectations:** Supervisors or third parties may prefer recognized vendor solutions although they also value the increased transparency of in-house solutions

- **Cost and scalability:** Total cost of ownership (TCO) should consider not only development but also upgrades, patching, and ongoing support by internal IT resources.

Table 7.1 outlines key considerations in determining whether to build, buy, or blend.

TABLE 7.1 • Considering Build vs. Buy vs. Blend

	Build	Buy	Blend
Description	The FI identifies specific requirements to address a targeted problem or use case. The solution build can be done by insourcing or outsourcing the necessary skills, with key business requirements (or inputs) and IT expertise required.	The FI purchases a commercially available off-the-shelf solution (typically ready-made solutions that can be deployed relatively quickly). The solutions may have limited core functionality with a limited ability for customization.	Blend involves building custom features and functionalities on top of off-the-shelf solutions to tailor the system to specific business needs. Customization is often necessary when the required functionality is not available in the standard product.
Examples	FIs may build a customer risk rating scoring in-house to replace manual processes (such as those using spreadsheets) or develop screening tools and case management systems.	FIs may acquire off-the-shelf solutions that provide modular functionality (for example, transaction monitoring) or end-to-end functionality (for example, customer risk rating, screening, and monitoring).	FIs often blend transaction monitoring systems where standard rulesets are enhanced with custom logic and advanced analytics to improve detection or alert risk scoring.
Main Benefits	✔ Tailored to business needs ✔ Customizable ✔ Scalable and adaptable ✔ Efficient integration	✔ Access to proven expertise ✔ Rapid deployment ✔ Vendor support ✔ Predictable upfront costs ✔ Reduced development risk ✔ Continuous innovation	✔ Increased flexibility ✔ Cost efficiency ✔ Customization that aligns with existing data or process ✔ Less reliance on vendors ✔ Encourages innovation
Main Drawbacks	✖ High development costs ✖ High maintenance costs ✖ Internal prioritization delays ✖ Exposure to turnover or attrition in internal technical support ✖ Lack of dependability ✖ Regulatory or audit reluctance ✖ Extended implementation timeframe ✖ Higher testing or validation burden	✖ Limited customization ✖ Desired features bundled with others ✖ Vendor reliance (that is, limited control over calibration or system upgrades) ✖ Intellectual property risks (for example, owning and understanding the internal logic) ✖ Limited innovation ✖ Compatibility issues ✖ Limited control over ongoing costs	✖ Increased integration and coordination complexity ✖ More complex change management

Source: Original for this publication.

A 2022 study found a 32 percent and 31 percent average reduction in manual workloads for "buy" and "build," respectively, while noting that 82 percent of surveyed buyers were able to scale successfully, as opposed to 67 percent of builders. On the other end, several contributors interviewed by IFC stated that in-house developed systems provided them more flexibility to customize and continuously scale their systems (LexisNexis 2022).

7.2.2 Cloud vs. On-Premises Deployment

Hosting decisions should consider cost, scalability, security, and regulatory obligations. Cloud environments offer processing power suited for advanced functionalities, such as analytics and machine learning, while on-premises deployments provide greater control and compliance with data residency requirements. Hybrid architectures, such as storing sensitive information on-premises while using cloud resources for compute-intensive tasks, are increasingly common.

Key considerations include the following:

- Regulatory compliance: Data-localization laws may restrict cross-border transfer of customer information
- Security posture: Cloud providers often invest more heavily in cybersecurity, but FIs remain accountable for configuration and access control
- Connectivity and infrastructure: In regions with unreliable bandwidth, cloud latency may affect performance
- Operational resilience: On-premises servers pose a risk of physical disruption. Cloud models rely on stable internet and provider continuity
- Scalability and innovation: Cloud deployment can enable experimentation with advanced analytics at lower entry cost.

Table 7.2 outlines key considerations in deciding between cloud and on-premises hosting.

TABLE 7.2 • Considering Cloud vs. On-Premises Deployment

	Cloud Deployment	On-Premises Deployment
Description	Cloud deployment refers to delivering computing services, such as servers, storage, databases, networking, or software, via the internet—typically by a third-party cloud provider.	On-premise deployment refers to an institution hosting applications and data on servers located within an FI's physical premises.
Benefits	✔ Flexibility and speed ✔ Allows institutions to scale up computing resources (for example, to support transaction monitoring or AI-based risk models) and scale back when necessary ✔ Generally faster to implement and avoids upfront costs of hardware	✔ Full control over systems and data ✔ Able to customize security and compliance ✔ Reliable access ✔ Infrastructure can be tailored to the FI's needs
Drawbacks	✖ Some laws or regulations may require data to be stored locally (with cloud storage in violation of such rules) ✖ Concerns about data protection (cybersecurity) ✖ Reliant on stable internet connectivity and local infrastructure	✖ Typically requires significant upfront investment ✖ Typically requires significant ongoing maintenance ✖ Can require dedicated IT resources to manage updates and hardware replacements ✖ Risk of data loss in event of failure (if no reliable backup system is in place)

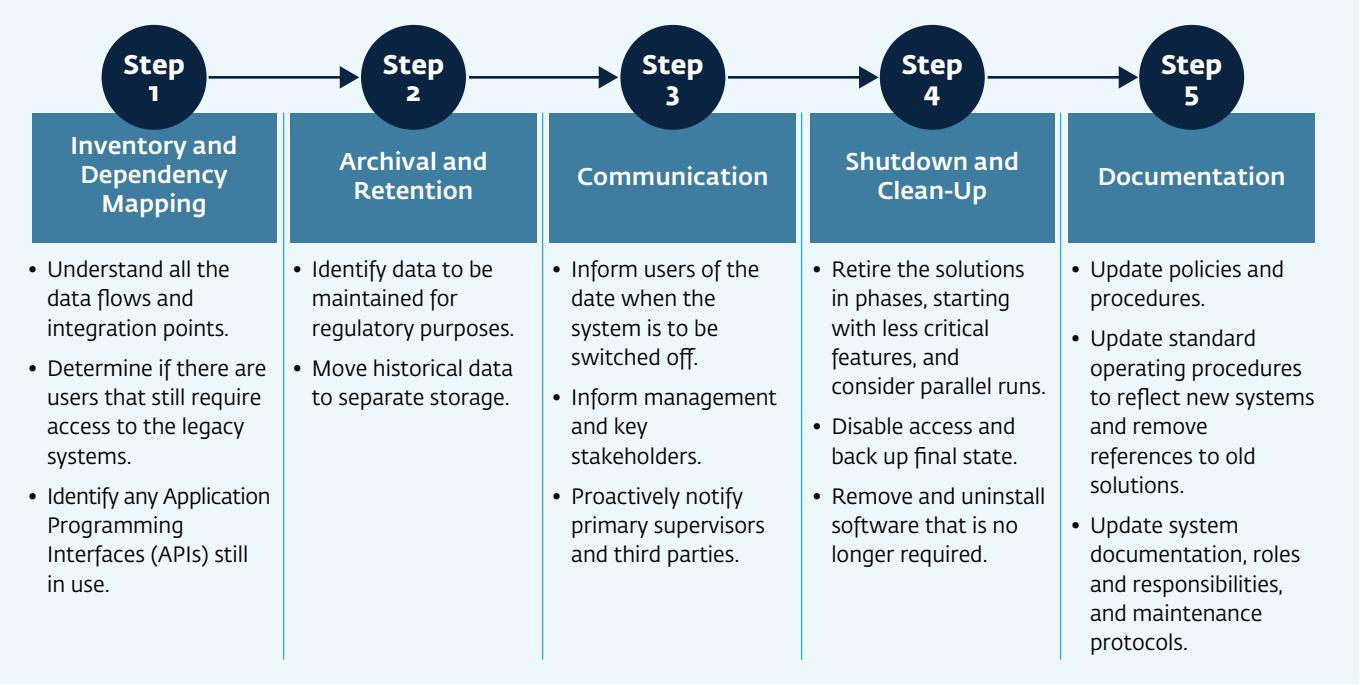
Source: Original for this publication.

Ultimately, the decision between on-premises and cloud computing services is guided by factors such as in-house expertise and technology, budget, security needs, compliance requirements, and growth plans.

7.2.3 Migration and Decommissioning of Legacy Systems

A key risk related to the migration to new systems relates to the ability to continue to comply with regulatory obligations and internal policies without interruption. There are multiple migration options that an FI can consider when transitioning systems, with benefits and costs associated with each, and several key governance principles that FIs are encouraged to consider. Figure 7.1 outlines the overarching principles for followed by best practices and migration options In Table 7.3.

FIGURE 7.1 • Typical Steps in Migrating and Decommissioning Legacy Systems



Source: Original for this publication.

Best practices include:

- Conducting **comprehensive data profiling** to identify inconsistencies before migration
- **Mapping data elements** between old and new systems, documenting transformation rules
- Defining **cutover strategy** based on system interdependencies and risk appetite
- Maintaining **read-only access to decommissioned systems** for audit and regulatory queries
- Performing **validation checks and reconciliations after migration** to ensure functionality and data completeness.

Table 7.3 outlines the main migration options with key considerations for each approach.

TABLE 7.3 • Migration Options and Key Considerations

Strategy and Definition	Risk	Use Cases
Big Bang All users and processes switch from the legacy system to the new system at a single point in time, enabling a faster transition.	• Can lead to significant disruptions if issues arise with the new system • Requires confidence in the readiness and stability of the new system • Ideal only when the ability to roll back (that is, restore a technology system or its configuration) is straightforward, in case of issues with the new system • In the absence of data migration, lack of access to historical information may jeopardize risk management	• Suitable when it is too costly, time-consuming, or risky to run systems in parallel • Often applied to smaller systems with low interdependencies
Phased Separate system components, such as modules, user groups, or business functions, are migrated to the new system in stages.	• Potential for slower overall implementation • Potential challenges explaining and integrating outputs from multiple systems • Potential discrepancies in processes and/or outputs from different business areas • Potential data synchronization challenges across linked systems	• Best suited for large or complex systems with multiple detection rules, user roles, or data sources • Typically used by FIs with low tolerance for information disruption • Ideal for staggered or gradual implementation of a solution where the information must flow into multiple downstream systems
Parallel The legacy and new systems run simultaneously on the same inputs for a defined period to compare outputs and validate accuracy.	• Increase in resource overhead, at least temporarily (comparing results from systems or sampling of legacy system to new outputs to confirm consistency) • Complexity in reconciling discrepancies, particularly when comparing transaction monitoring outputs	• Useful in highly regulated environments where false positives or negatives must be validated • Provides assurance to regulators and auditors regarding system integrity
Pilot The new system is deployed in a limited, controlled environment (for example, in a regional office or single business line).	• Requires careful selection of pilot groups • Offers limited value if pilot scope is too narrow or not aligned with broader operations	• Can be effective when introducing new, unproven vendors or custom solutions • Can enable gathering of user feedback and improvements prior to institution-wide rollout • Valuable for evaluating new transaction monitoring rulesets and tuning alert thresholds before full deployment
Coexistence Both legacy and new systems operate together long-term, often dividing responsibilities across functions, regions, or data types.	• Maintenance and compliance efforts are higher • Legacy systems may introduce security vulnerabilities if not kept updated	• Appropriate for migrations where immediately retiring the legacy system is not possible • Some products or businesses (for example brokerage or trading operations) may be more effectively monitored using a legacy or separate solution

Source: Original for this publication.

7.2.4 Vendor Partner Selection

When selecting a vendor partner, FIs are encouraged to take a strategic and holistic approach, to ensure the provider can deliver consistent support throughout system migration, implementation, and subsequent ongoing maintenance.

Refer to Section 7.4, "Considerations for Selecting a Vendor Partner," for considerations when selecting a vendor partner.

7.2.5 Assessing Control Readiness and Maturity

Effective technological implementation heavily depends on the strength and the quality of the FI's underlying AML/CFT risk management program. Technology cannot compensate for weak foundational controls or inefficient processes. Rather, it can amplify both strengths and deficiencies. An FI embarking on a technological adoption journey should not only have a clear knowledge of the control areas that would benefit from the use of technology but also understand the maturity of each control area and the associated process.

Before implementing a certain technology, an FI may first need to address foundational AML/CFT control challenges (such as process improvements and lack of data availability). Control readiness refers to the degree to which an FI's governance, data, and operational processes are prepared to support automated AML/CFT solutions. A readiness assessment helps determine whether the environment can deliver the expected benefits of technology and comply with regulatory expectations during and after deployment.

This Good Practice Note includes indicative stages of control maturity in Appendix B, "Control Maturity Matrix" for the purposes of assisting FIs in self-assessing their control maturity.

7.3 Designing an AML/CFT Technology Selection and Implementation Strategy

After defining an internal technology strategy and assessing control readiness, FIs should develop a structured plan for selecting and implementing technology that emphasizes stakeholder engagement, governance, data readiness, and regulator communication.

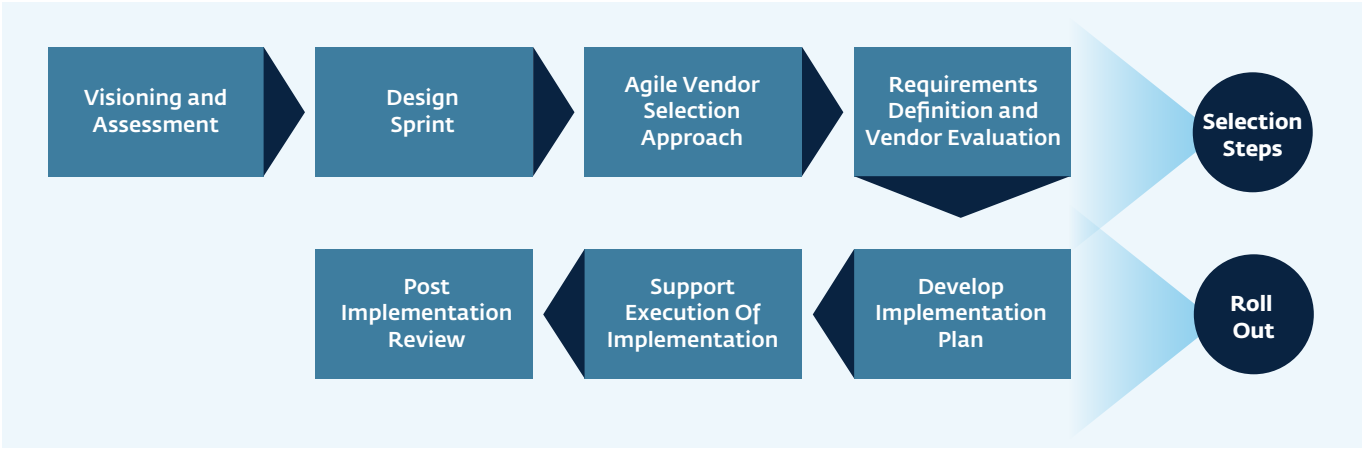
Key elements of a plan may include the following:

- **Stages of system selection and implementation:** What steps and milestones should an FI include to ensure the selection of an appropriate system and an effective implementation?
- **Change management:** How can an FI build buy-in from relevant stakeholders? How can the FI avoid a dip in productivity (or a productivity gap) during the implementation? What change management initiatives should be considered from the onset?
- **Governance and oversight:** What governance, oversight, and accountability mechanisms should be in place to ensure an appropriate system implementation?
- **Communicating with regulators and third parties:** How do FIs communicate with regulators and third parties (such as correspondent banks) when undergoing a system migration to build support?
- **Data readiness and data governance:** What data is needed to ensure an effective migration? How can FIs go about cleaning and updating data for migration?

7.3.1 Stages of System Selection and Implementation

FIs are also encouraged to adopt a structured process to select and implement systems. While the steps needed may differ based on the size, sophistication, and profile of the FI, Figure 7.2 outlines several commonly observed steps in selection and deployment. Table 7.4 subsequently outlines key activities for consideration within each step.

FIGURE 7.2 • Typical Stages of System Selection and Implementation



Source: Original for this publication.

Table 7.4 further explores each phase of selection and deployment.

TABLE 7.4 • System Deployment Stages and Key Activities

Step and Definition	Key Activities Considerations
System Selection Steps	
Visioning and Assessment The initial phase involves assessing current systems to identify gaps and compliance needs, defining a future-state vision aligned with strategic objectives, prioritizing requirements, determining key enablers, and engaging stakeholders early to ensure alignment.	• Review existing technology to identify strengths, weaknesses, and pain points and pinpoint where current tools fall short of regulatory, risk, or efficiency requirements • Define a target environment aligned with strategic and compliance goals • Identify high-impact requirements and determine key enablers, such as data quality improvements, integration upgrades, or stakeholder alignment • Implement structured project governance and establish oversight committees and action plan and status reporting • Involve the FI's procurement and vendor management teams to define operational requirements • Adopt modularly by starting with a focused domain, business line, or product, and then expanding
Design Sprint Translate the strategic vision into solution requirements by defining capabilities, creating user stories, developing a scoring framework for a vendor evaluation process, gathering stakeholder input, reviewing available solutions, and issuing a RFI to shortlisted vendors.	• Define capabilities and requirements to address challenges, including core functionalities, user stories, and both functional and nonfunctional needs • Establish evaluation criteria by creating a scoring framework, conducting a market scan of vendor offerings, and prioritizing "must-have" versus "nice-to-have" features • Engage end users through workshops and questionnaires to capture pain points, operational needs, and technical environment details • Develop baseline documentation by consolidating inputs into a business requirements document that guides vendor engagement • Draft and align the RFI with baseline requirements, covering implementation, architecture, integration, vendor viability (that is, long-term operational capacity), credentials, and pricing • Shortlist vendors to a manageable number for focused evaluation • Issue the RFI to selected vendors with clear submission guidelines, deadlines, and required supporting background materials
Agile Vendor Selection Approach Evaluate RFI responses using predefined scoring criteria aligned with the business case and future-state vision and assess functionality through structured demonstrations, document findings for transparency, and secure sponsor approvals at key milestones.	• Evaluate RFI responses by scoring submissions against core requirements, functional fit, and cost-effectiveness • Select vendors for technical demonstrations and obtain sponsor approval • Coordinate demos by scheduling sessions, providing scripts, and ensuring consistent presentations • Document results from RFI reviews and demos, including costs, technical notes, and red flags • Capture insights from stakeholder feedback, align with criteria, and refine scoring for final recommendations

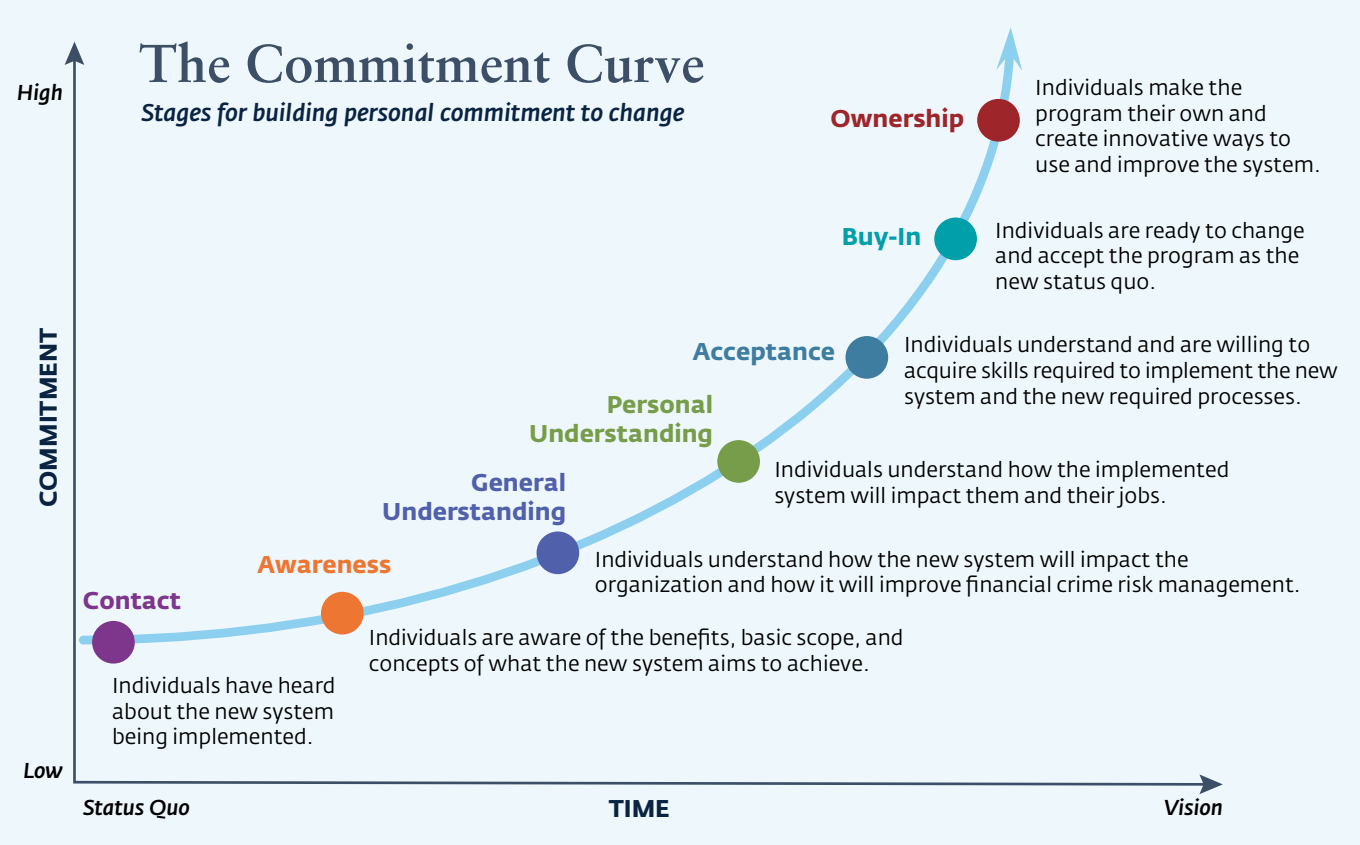
Step and Definition	Key Activities Considerations
Requirements Definition and Vendor Evaluation Document RFI evaluations and demo outcomes, refine requirements, issue an RFP to shortlisted vendors, apply due diligence to validate capabilities, and collaborate across legal, compliance, and IT to finalize contracts covering intellectual property, data protection, service levels, liability, exit strategies, and pricing to ensure enforceable agreements and a scalable implementation.	• Present RFI and demo results to sponsors and outline the RFP framework with evaluation criteria, weightings, and mandatory requirements • Refine technical and business specifications with IT and stakeholders, then issue the RFP to shortlisted vendors with clear submission guidelines and timelines • Evaluate proposals through due diligence on vendor viability, financial stability, cybersecurity posture, and regulatory alignment, and finalize the business case • Engage compliance, legal, IT, and business teams in evaluating responses and negotiating contract terms, as necessary • Define intellectual property ownership, data protection clauses, liability limits, service level agreements (SLAs), termination rights, and dispute resolution processes in contracts • Establish scope change procedures, pricing structures, payment terms, and cost controls to manage implementation and ongoing support • Select and contract with a vendor partner (if an external solution is decided upon)
System Implementation Steps	
Establish Implementation Framework Create a structured implementation plan outlining scope, timeline, resources, and communication, with risk mitigation, milestone tracking, and change management considerations to facilitate structured rollout.	• Define objectives and scope to set clear expectations, align stakeholders, and outline desired outcomes • Develop a phased project plan with milestones, deadlines, dependencies, and assigned responsibilities • Allocate resources by determining personnel, technology, and budget needs, including contingency funds • Create a communications plan with regular updates, training, and support to prepare the FI for adoption
Support Execution of Implementation Monitor progress with KPIs, maintain stakeholder communication, provide technical support, and apply change management to facilitate adoption and smooth execution.	• Establish a protocol to track implementation progress against the plan • Establish reporting to monitor compliance with deadlines and achievement of key objectives • Regularly review progress reports and adjust plans as needed to address deviations or challenges • Implement change management strategies to support user adoption of the new technology • Engage internal audit in governance and conduct control reviews throughout the project
Post Implementation Review Evaluate whether the solution met its objectives by reviewing performance metrics and gathering stakeholder feedback to ensure continued effectiveness and value.	• Assess goal achievement by comparing actual outcomes against objectives and project metrics • Gather stakeholder feedback through surveys, interviews, or focus groups to identify challenges and opportunities for improvement • Review KRIs and performance metrics to track the solution's effectiveness and value delivery (over time, starting several months after launch)

Source: Original for this publication.

7.3.2 Change Management

Change management is often the hardest part of any implementation. Without coordinated strategies and staff buy-in, even the best technical solution can fall short. New systems change how people work, requiring patience, reassurance, communication, training, and a clear strategy to mitigate resistance. Aligning stakeholders early, addressing friction before go-live, and proactively managing the transition reduces confusion, disruption, and adoption risk. Figure 7.3 depicts a typical "commitment curve" illustrating how individuals' commitment to change typically grows over time as they progress through the change journey.

FIGURE 7.3 • A Change Management Commitment Curve



Source: Original for this publication adapted from Gopalakrishnan (2013).

While the commitment curve highlights an example path to building buy-in, FIs must also anticipate common pitfalls that can derail change efforts. The change process can lead to a so-called "productivity dip"—a temporary decline in performance, efficiency, and/or output that occurs when FIs transition to new systems, processes, or technologies. While a productivity dip is expected in most system transitions, the magnitude of the decline can be lessened by measures such as thorough communication, training, and oversight. One of the most effective ways to prevent change management failures is through early and sustained involvement of business stakeholders. Their input enables the system design and deployment to reflect operational realities, align with user needs, and increase adoption across the FI.

Key principles for effective engagement include:

- **Engage early and broadly:** Involve a diverse range of users, including frontline staff, investigators, and operations teams, at the start of the project to identify real challenges, validate requirements, and build shared ownership of outcomes
- **Map and challenge existing processes:** Collaborate with stakeholders to review and streamline current workflows. Avoid automating outdated or inefficient

processes and distinguish between necessary controls and legacy habits

- **Rationalize business rules:** Include compliance and operations teams in reviewing existing rulesets to ensure only relevant, risk-based rules are migrated. This strengthens both efficiency and regulatory alignment
- **Codesign and test in real contexts:** Engage end-users in the testing and pilot phases to confirm usability and process fit. Collect structured feedback and demonstrate visible action on improvement suggestions to reinforce confidence
- **Plan for continuity and resilience:** Involve stakeholders in contingency and scenario planning to prepare for go-live challenges. Clear communication of rollback and escalation protocols helps maintain confidence and operational continuity during transition.

While these principles are often vital, many AML/CFT system deployments fail because common pitfalls are not anticipated or mitigated. Table 7.5 outlines some of the most frequent change management challenges and provides actionable strategies to prevent them.

TABLE 7.5 • Strategies to Avoid Common Change Management Pitfalls

Common Pitfall	Strategies to Avoid Pitfalls
Ineffective Stakeholder Mapping Failure to identify all critical stakeholders (for example, IT, legal, audit, and first-line users) can lead to misalignment and resistance.	• Conduct stakeholder analysis at project start and maintain ongoing engagement • Identify decision-makers early across departments, such as risk, compliance, IT, and business • Hold early cross-departmental workshops (involving compliance, IT, and others) to uncover dependencies, secure buy-in, and anticipate impacts to downstream or upstream systems
Weak Communications Strategy Lack of timely updates leads to misinformation, concerns, and misalignment across regions.	• Create a structured and sequenced communications plan covering business case, timelines, decisions, and milestones, tailored to the varying audiences • Use multiple formats (for example, briefings, newsletters, intranet, and town halls) for updates • Appoint team representatives as two-way communication conduits • Frame messages around observed pain points, future benefits, and relevant use cases
Key Person Dependency Overreliance on a single champion or technical lead creates risks, such as knowledge silos, loss of momentum (if that individual is absent or leaves the organization), and sustainability challenges.	• Create a shared knowledge base for centralized accessible information • Document processes thoroughly and deliver targeted training for skill transfer • Form cross-functional teams with designated backups for each project phase • If using external experts, define a clear handover and knowledge transition plan
Failing to Codesign with System Users Lack of early engagement of system users, such as investigators, compliance officers, and operations, leads to poor adoption and shadow systems.	• Publicly recognize change champions and super-user networks • Engage frontline users in design, wireframing, pilots, and feedback loops • Test workflows in mock-ups or sandbox environments before final build • Gather feedback after deployment and visibly act on reasonable suggestions

Common Pitfall	Strategies to Avoid Pitfalls
Underestimating Change Fatigue Adding new requirements to already stressed teams without first assessing change impact can cause burnout, resistance, and poor implementation quality.	• Review existing workloads before setting milestones • Align rollout schedules with team capacity or add temporary staff or consultants • Deliver quick wins to build momentum • Stagger deployments to reduce strain but avoid a multiyear adoption timeframe • Boost morale with public recognition, progress dashboards, and visible impact of efforts

Source: Original for this publication.

7.3.3 Governance and Oversight of System Implementations and Upgrades

Successful system implementations and changes require governance and oversight. Best practice is to establish a governance structure and the system development life cycle adapted to fit the system.

Key governance elements to consider include the following:

- **Steering committee:** Establish an executive-led forum composed of representatives from business, IT, compliance, risk management, and operations. The committee provides strategic direction, reviews progress, resolves escalations, and enables alignment with institutional priorities and regulatory obligations
- **Project management office:** Establish a dedicated planning and coordination team responsible for project design, resource allocation, risk tracking, regular reporting, and communication. The project management office, often referred to as a "PMO," maintains a live issue log and enables decisions to be documented and reported to the steering committee
- **Change control board:** Extend oversight beyond core IT production changes to also cover modifications to thresholds, rules, workflows, and other project components. This enables traceability, version control, and proper authorization of changes affecting AML/CFT systems
- **Data governance:** Appoint data stewards early to oversee data quality and migration. Strong governance can provide assurance over the integrity and accuracy of data transferred into the new system
- **Model validation committee:** Establish a dedicated committee to review and validate model logic, ensure explainability documentation, and oversee testing before deployment for behavioral, AI, and machine learning models.

7.3.4 Communicating with Regulators and Third Parties

Even with strong governance in place, a critical challenge in implementing new technologies is maintaining the confidence of regulators and other third parties. Regulators may be concerned that new system implementations could weaken risk management processes, especially during the transition period, and may question whether the new system will perform as reliably as the legacy system. These concerns can be amplified when AI and machine learning techniques are introduced, as unfamiliar approaches can create uncertainty. To address these concerns, FIs should consider engaging regulators early and maintain open communication throughout the project.

Key actions for effective engagement of regulators and third parties include the following:

- **Engage early:** Initiate discussions at the outset to build collaboration, align expectations, and integrate regulatory requirements from the start
- **Assess and communicate impact:** Evaluate how changes will affect upstream and downstream

processes, systems, and compliance obligations, and share findings clearly with regulators

- **Ensure regulatory alignment:** Design changes to meet current regulations and anticipate future developments to maintain ongoing compliance
- **Maintain transparency:** Provide regular updates, comprehensive documentation, and clear governance to build trust and demonstrate accountability
- **Explain AI or machine learning models:** Develop explainability frameworks that make models transparent and understandable for management and regulatory review
- **Implement interim controls:** Put temporary measures in place during transition to maintain compliance and mitigate risks
- **Prepare staff:** Deliver training and update standard operating procedures so users and stakeholders understand new processes and compliance responsibilities.

Proactive, transparent engagement with regulators and third parties not only reduces implementation risk but also builds the trust needed to adopt innovative technologies and sustain long-term compliance.

7.3.5 Readiness of Data and Data Governance

Even with strong governance and communications with regulators and third parties, technology and analytics can fail to deliver the desired outcomes if the underlying data is of poor quality, incomplete, inconsistent, and/or fragmented. Data quality issues can complicate system integrations, delay progress, increase costs, and ultimately undermine efficiency, decision-making, and risk management. For AML/CFT systems in particular, accurate and reliable data is essential to effectively identify and manage risk and to meet regulatory requirements.

High-quality data in AML/CFT is critical because it:

- **Supports decision-making:** Reduces uncertainty and enables informed business choices (which is needed when making material decisions related to customer relationships and reporting)
- **Improves process effectiveness and efficiency:** Minimizes errors, rework, and low-impact work to enable processes to run more optimally
- **Enables compliance:** Helps identify and mitigate risks while meeting policy and procedure requirements and regulatory obligations
- **Enables deeper analysis:** Allows human intervention to focus on insights rather than data cleansing or remediation; and
- **Builds trust:** Gains confidence with employees, customers, and external parties when data is managed effectively.

Common causes of poor data quality include the following:

- **Lack of seamless data exchange:** No real-time or on-demand data flow to support AML/CFT
- **Lack of strong recordkeeping protocols:** Lack of regular removal of legacy accounts or customers inflates and complicates the dataset
- **Legacy codes:** As products, distribution channels, and customer activity evolve, systems may be populated by numerous codes representing the same activity. For example, many FIs have a variety of codes for cash transactions
- **Overlapping systems:** Multiple nonintegrated applications create duplicates and inconsistencies
- **Ownership or governance:** No defined accountability or processes to enforce data quality (particularly during data collection and validation processes)
- **Ambiguous or inconsistent definitions:** Unclear data elements and processes cause errors
- **Complex application landscape:** Expanding systems make consistent data harder to maintain
- **Escalation process:** No formal path to raise and resolve data quality issues
- **Poor quality control with third parties:** Lack of data accuracy or completeness derived from third parties
- **Lack of data quality standards:** Lack of consistent standards for data quality, validation, and format.

In the context of system implementation, while many FIs may aim for perfect data before deployment, the process itself can be a powerful opportunity to improve data

quality. Many FIs have even voluntarily incorporated data issues into risk models on a temporary basis while adding additional controls (such as rating customers as high-risk if a key data field is unknown).

The preparation for system implementation provides an opportunity to enhance and improve data, with several best practices including the following:

- **Improve data tracking and ownership:** Implement processes and tools that log and map customer and transaction data from its original source through each stage of collection, transformation, storage, and usage, while clarifying ownership and structure
- **Define minimum data requirements:** Set clear metrics for proofs of concepts or pilot phases to measure success
- **Flag and address gaps continuously:** Identify and resolve data issues throughout implementation
- **Use profiling and dashboards:** Monitor accuracy and completeness in production to proactively address problems
- **Apply validation thresholds:** Only transfer the data that meets minimum quality criteria to prevent migrating errors into the new systems
- **Apply controls for missing data:** Define an approach to missing data fields (such as defaulting to a higher risk rating if data is unknown)
- **Adopt data reconciliation protocols:** Adopt processes to compare, verify, and harmonize datasets from multiple sources (to identify any discrepancies, duplications, or missing records)
- **Independent testing:** Obtain an independent viewpoint on data controls and standards.

Data quality should be treated as an integral part of system deployment, supported by preparatory work such as a data readiness checklist to assess the current state and define tasks for implementation.

Key aspects of a data readiness checklist include the following:

- **Data sources:** What data exists and where is it located?
- **Data dictionary:** Are there documented standards and a centralized repository of the FI's data?
- **Core identifiers:** Are customer and account IDs consistently available and aligned across systems?
- **Transaction data:** Are transactions properly timestamped and consistently categorized?
- **Entity resolution:** Is it possible to consolidate multiple customer records across existing data?
- **KRIs and KPIs:** Have data quality metrics been defined?
- **Governance:** Are processes in place to support implementation?
- **Iteration:** Can improvements be made over time?
- **Access:** How can data be pulled into upstream or downstream systems—APIs, extract, transform, load (ETL) processes,[53] or batch processes?

For AML/CFT systems to work as intended, thorough data cleaning is essential to enable the high-quality, consistent, and reliable data that is required to implement effective control processes. Clean data underpins accurate customer risk ratings, enterprise-wide risk assessments, and monitoring and screening systems, while reducing errors and redundancies and enabling skilled resources to focus on analyzing data insights.[54] Investing in data cleaning practices (in the context of a system implementation and on an ongoing basis) can enhance decision-making, strengthen regulatory compliance, and support seamless integration across systems.

53 ETL, or extract, transform, load, is a data integration process that gathers information from multiple sources, cleans and formats it, and then loads it into a target system for storage, analysis, and reporting.

54 The format in which payment data is transmitted is equally critical to data quality. Legacy payment messaging formats may impose structural limitations on the volume and granularity of data that can accompany a transaction, often resulting in truncated or incomplete originator and beneficiary information — with direct implications for compliance with FATF Recommendation 16, which requires that full relevant originator and beneficiary information travel with transfers throughout the payment chain. Having systems compatible with ISO 20022, an internationally recognized messaging standard supporting richer, structured, and machine-readable data, can address this gap by enabling complete payment information to be transmitted end-to-end in a format that AML/CFT systems can process effectively. FIs should therefore assess whether their payment infrastructure supports sufficiently rich data formats, as this is a foundational prerequisite for Recommendation 16 compliance.

7.4 Considerations for Selecting a Vendor Partner

Vendor selection is critical to the long-term success of any technological transformation. Choosing the wrong vendor can lead to costly delays, poor integration, and limited scalability, while the right partner can enable innovation, knowledge transfer, and sustainable compliance processes. Beyond technical fit, the right provider must offer expertise, compatibility, and ongoing support that aligns with the FI's strategic goals. To guide this critical decision, FIs can assess vendors across a range of strategic factors. This section provides guiding principles, best practices, and lessons learned for identifying suitable providers.

7.4.1 Considerations for Procurement Processes

A well-structured procurement process sets clear procedures for gathering information from potential vendors, evaluating their proposals, and documenting decisions to promote accountability and manage risks of bias.

In practice, there are three main methods to gather information during procurement—RFIs, RFQs, and RFPs, as outlined in table 7.6.

TABLE 7.6 • Common Methods of Procurement; RFIs, RFQs, and RFPs

	Request for Information (RFI)	Request for Quote (RFQ)	Request for Proposal (RFP)
Description	Requests general information from vendors about their products, capabilities, and market innovations; helps institutions survey the landscape before specifying requirements.	Solicits price quotes for specific, standardized products or services where requirements are clear; primarily focused on cost and quantity.	Seeks comprehensive proposals from vendors for defined projects, including technical approaches, pricing, support, and implementation plans.
When Used	Early in the procurement process, when business needs or technical requirements are still being refined and institutions want to identify potential solutions. Typically precedes RFP.	When the institution knows exactly what it needs, with clear specifications, and the main differentiator is price or delivery terms.	When ready to choose a partner for a complex solution, project, or system migration, and detailed information is needed. Typically follows an RFI process.
Benefits	Provides a broad overview of available options, reveals vendor innovations, helps refine selection criteria, and opens dialogue with industry leaders.	Enables quick price comparison among qualified vendors, simplifies selection for certain solutions with clear benefits, and supports budget management.	Allows for deep evaluation of vendors' capabilities, approaches, and alignment with business objectives, helping enable the best fit for complex needs.
Drawbacks	May result in uneven or marketing-driven responses, lacks actionable details for decision-making, and requires follow-up steps before procurement.	Focus on price may overlook solution fit or service quality; assumes standardization across vendors that may not always exist for specialized needs.	More resource-intensive and time-consuming, requiring well-defined requirements and substantial review of detailed proposals by the FI.

Source: Original for this publication.

These approaches are commonly used in sequence or together. It is advantageous to start with an RFI, enabling FIs to assess the full range of available solutions before narrowing the options. The subsequent RFP phase focuses on a shortlist of qualified vendors, allowing for more detailed information exchange and selection of the best implementation partner.

To create an effective RFP, FIs can work with their procurement teams and use a structured template that includes project scope, objectives, evaluation criteria, and submission requirements. In addition, it is essential to seek input into the RFP from relevant stakeholders, such as IT and key system users. This approach attracts qualified vendors, improves response quality, and supports objective, transparent evaluation.

Table 7.7 outlines a sample structure for an RFP in an AML/CFT technology procurement project:

TABLE 7.7 • Example RFP Structure

Example RFP Structure	
Introduction	
• Overview of the Organization and Project • Purpose and Objective of the Request for Proposal (RFP) • Background and Context (current system landscape and transformation goals) • Intent to Bid and Restrictions on Vendor Communication	• RFP Schedule and Key Milestones (for example, issue date, question and answer deadline, submission date, interview requirements, demo period, and award date) • General Instructions and Response Requirements
AML/CFT Technology Requirements and Scope of Work	
• Current State Overview (systems, data, and challenges) • Future State Vision and Conceptual Architecture (interoperability, analytics, scalability, and innovation roadmap)	• Scope of Work • Implementation Guidelines (phasing, integration, testing, and handover)
Submission Instructions and Legal Considerations	
• Submission Guidelines (for example, format, language, delivery mode, and contact point) • Bid Validity Period and Binding Clauses • Procedures for Declining to Respond	• Financial Verification Requirements • Use of Subcontractors and Approval Rights • Proprietorship and Ownership of Materials
Evaluation and Selection Process	
• Evaluation Methodology and Scoring Framework (including mandatory criteria) • Supplier Performance Management • Shortlisting, Technical Demonstration, and Due Diligence Stages	• Disqualification Criteria • Rights Reserved by Issuer
Bidder Declarations and Undertakings	
• Required Representations by Bidders • Legal Undertakings and Acknowledgement	• Nondisclosure and Confidentiality

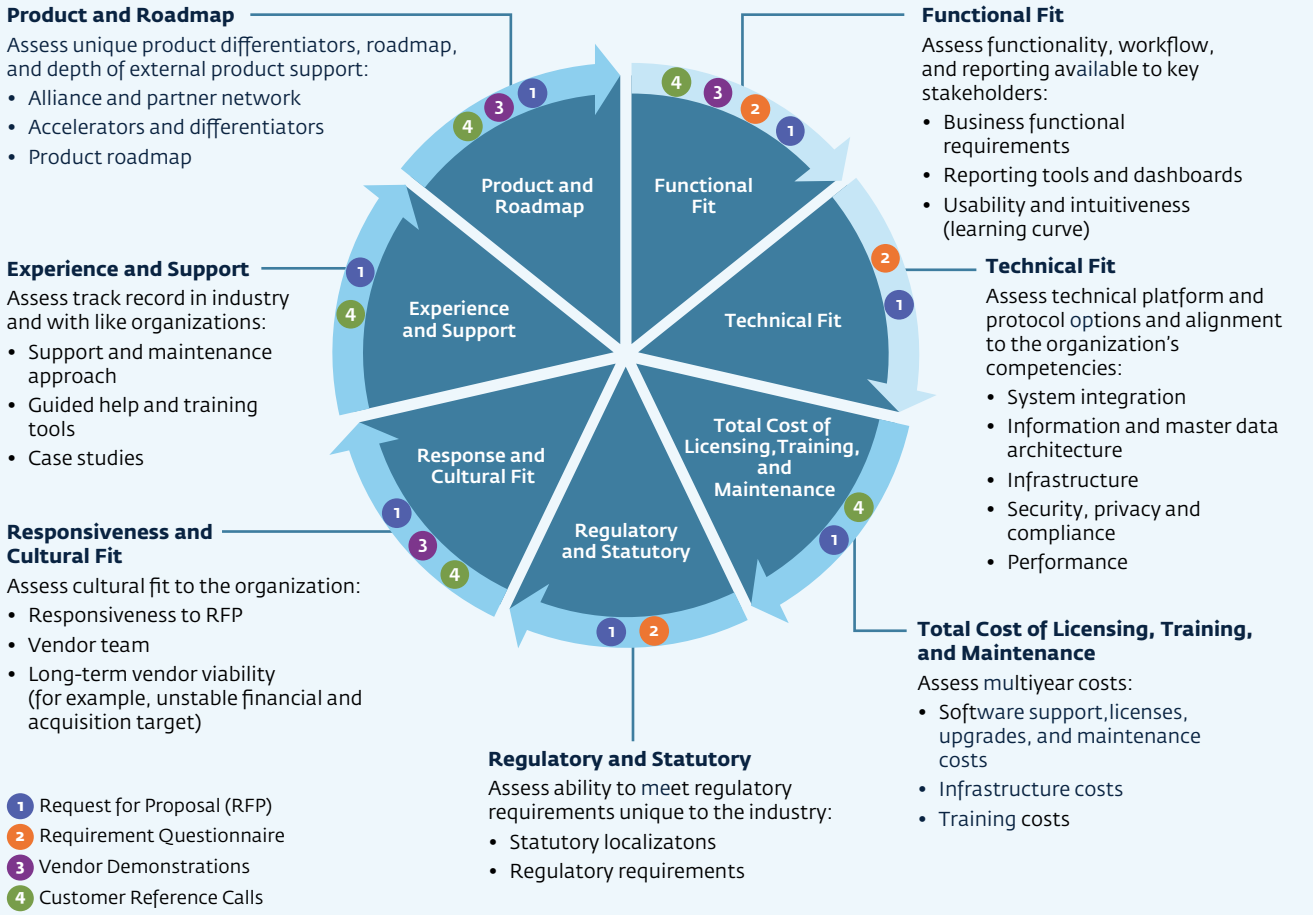
Example RFP Structure	
Desired RFP Response Structure	
• Technical Response Template • Mapping of Requirements to Use Cases • Proposed Project Team and Key Personnel	• Implementation Methodology and Timeline • Training and Change Management Approach • Assumptions, Dependencies, and Risk Mitigation
Technical Demonstration Requirements	
• Indicative Agenda for a Demonstration • Examples of Scenarios or Workflows to be Demonstrated	• Demonstration of Evaluation Criteria
Contractual Considerations	
• Legal Terms and Conditions • Nondisclosure and Confidentiality Agreement • Service Level Agreements (SLAs) and Performance Metrics • Termination, Transition, and Exit Provisions	• Postimplementation Support, Maintenance, and Upgrade Terms • Data Ownership and Data Privacy Considerations • Cybersecurity Considerations • Other Applicable Considerations (for example, contract matrix)
Mandatory Bid Documentation	
• Required Documentation Checklist (for example, vendor profile, company information, references, case studies, and team resumes)	• Supporting Industry Certifications • Financial statements
Pricing Information	
• Detailed Pricing Breakdown (for example, licenses, implementation, customization, support, and maintenance) • Optional Components and Add-On Modules	• Geographic or Currency Adjustments • Applicable Fees, Taxes, and Discounts • Total Cost of Ownership Over Defined Period (for example, five years)

Source: Original for this publication.

7.4.1.1 Considerations for Evaluating Vendor Solutions and Proposals

Selecting the right technology partner requires a structured and transparent evaluation process that balances functional, technical, financial, and strategic considerations. Figure 7.4 illustrates a holistic vendor selection framework that institutions can apply to assess and compare potential AML/CFT technology providers. The framework covers seven core evaluation dimensions: functional fit; technical fit; total cost of licensing, training, and maintenance; regulatory and statutory fit; responsiveness and cultural fit; experience and support; and product and roadmap. Each dimension is evaluated through multiple assessment inputs, including RFP responses, requirement questionnaires, vendor demonstrations, and customer reference calls.

FIGURE 7.4 • Overview of the Selection Framework



Source: Original for this publication.

7.4.1.2 Considerations for FI Preparation for Vendor Technical Demonstrations

Vendor demonstrations (or demos) are an important step in selection as they provide an opportunity for FIs to observe systems in action and evaluate their alignment with specific business needs. To maximize the value of demos, FI can internally establish clear objectives and focus on scenarios relevant to their operational environment. Requesting demonstrations that reflect real use cases and workflows enables institutions to assess integration, functionality, and overall suitability. In addition, involving key stakeholders and end-users can provide valuable insights into usability and practicality and enable the solution to be evaluated from multiple perspectives.

Best practices for FIs to host vendor demonstrations include the following:

- Preparing a structured demo script covering key workflows and risk scenarios
- Asking focused questions about integration, scalability, audit trails, reporting, and support
- Interviewing proposed vendor leads for the project, focusing on experience and differentiation from other teams
- Encouraging demonstrations to observe system performance firsthand
- Evaluating vendor performance against predefined criteria related to technical requirements.

Table 7.8 provides an example script to guide vendor presentations on risk rating capabilities.

TABLE 7.8 • Example Script for Vendor Technical Demonstrations

Example: Demonstration Script for Vendor on Customer Risk Rating Capabilities
1. **Risk rating and scoring workflow:** Demonstrate how the system assigns an overall risk rating or score to individual customers based on configurable parameters.
2. **Input of risk factors:** Show how key variables (for example, geography, product type, and customer type) are entered into the risk rating engine and contribute to the customer's risk rating.
3. **Weighting adjustments**: Illustrate how users or administrators can configure or adjust the weighting of different risk factors and observe their impact on customer risk rating.
4. **Data capture for scoring:** Present how the system captures and utilizes both structured and unstructured data points for customer risk evaluation.
5. **Execution of risk rating:** Demonstrate the end-to-end process of generating a customer risk rating, highlighting transparency in scoring logic and underlying calculations.
6. **Dashboards and reporting:** Provide examples of dashboards or reports that display risk ratings across the customer base, including segmentation by risk level.
7. **Manual overrides:** Demonstrate how users can override system-generated risk ratings and how such overrides are recorded, audited, and managed.
8. **Enhanced due diligence (EDD triggers):** Show how the system automatically initiates an EDD review or alert based on predefined criteria.
9. **Scoring of related parties:** Explain how the system incorporates risk ratings of related parties or associated entities when determining a customer's overall risk profile.

Source: Original for this publication.

7.4.1.3 Considerations for Evaluating Vendor Proposals

Scoring converts qualitative insights from vendor submissions and demonstrations into a structured, quantitative evaluation. The scoring process can be systematic, based on predefined criteria and transparent weightings, and ideally involve evaluators from multiple business areas that have received guidance or training.

A scoring framework can outline the evaluation item, description, scoring metric, responsible evaluator(s), and data source. Weightings can reflect institutional priorities, giving highest importance to critical requirements and nonnegotiable items that could disqualify a proposal. Risk factors, such as potential disruptions in service, can also be considered to ensure both functionality and resilience expectations are met.

Table 7.9 provides an illustrative vendor scoring sheet (including key components, criticality, and source for scoring).

TABLE 7.9 • Illustrative Vendor Scoring Sheet

Area	Criticality	Main Source	Measurement
Functional Fit Evaluates how well the solution supports key business processes, meets compliance needs, and addresses all specified use cases.	Critical	RFP Questionnaire	Assessed against 85 required functionalities for completeness.
Technical Fit Assesses solution architecture, scalability, integration, security protocols, performance, mobile platform support, and data management.	Important	RFP and Technical Demo	Evaluated based on 14 technical aspects discussed during IT and demo sessions.
Experience and Support Checks references for vendor's track record in technology delivery, ongoing support, maintenance quality, local or regional presence, and relationship management.	Critical	Reference Calls	Feedback solicited from two references to verify reliability and service quality.
Regulatory and Statutory Fit Reviews how well the vendor's solution aligns with applicable regulatory and statutory requirements.	Critical	RFP Questionnaire	Considered across four categories to assess regulatory and statutory fit.
Cultural Fit and Responsiveness Reviews company profile, engagement history, communication style, and ability to meet partnership and collaboration expectations.	Important	RFP and Feedback	Considered across six categories to assess responsiveness and compatibility.
Product and Roadmap Evaluates innovation, roadmap alignment with organizational goals, and any demonstrated deficiencies during proposal preparation or follow-up.	Important	Vendor Response	Includes review of future developments, vendor timeliness, and miscellaneous factors.
Demo Performance Measures core functionality, user experience, flexibility, and overall fit as shown in stakeholder-driven scenarios during demos.	Important	Demo Sessions	A total of 131 demo items were scored, with detailed stakeholder feedback on usability.
Total Cost Estimates overall cost, including licensing, training, ongoing maintenance, and total cost of ownership for the proposed solution.	Critical	Vendor Proposal	Point-in-time cost analysis covers all relevant financial considerations.

Source: Original for this publication.

FIs are encouraged to define factors that are critical (or "make-or-break" to the procurement process) to mitigate the risk of selecting the highest-scoring vendor based on pricing and other factors whose solution is not a functional fit and fails to meet regulatory requirements or provide adequate support during and after implementation.

7.4.1.4 Managing the Total Cost of Ownership

Managing the total cost of ownership is a key consideration when selecting and deploying systems. The total cost of ownership encompasses not only the upfront cost provided by the vendor in the response to the RFP but also considers incidental and ongoing costs, such as licensing, infrastructure, and integration. Less obvious expenses like model tuning, data provider fees, audit requirements, and change management costs can also be considered.

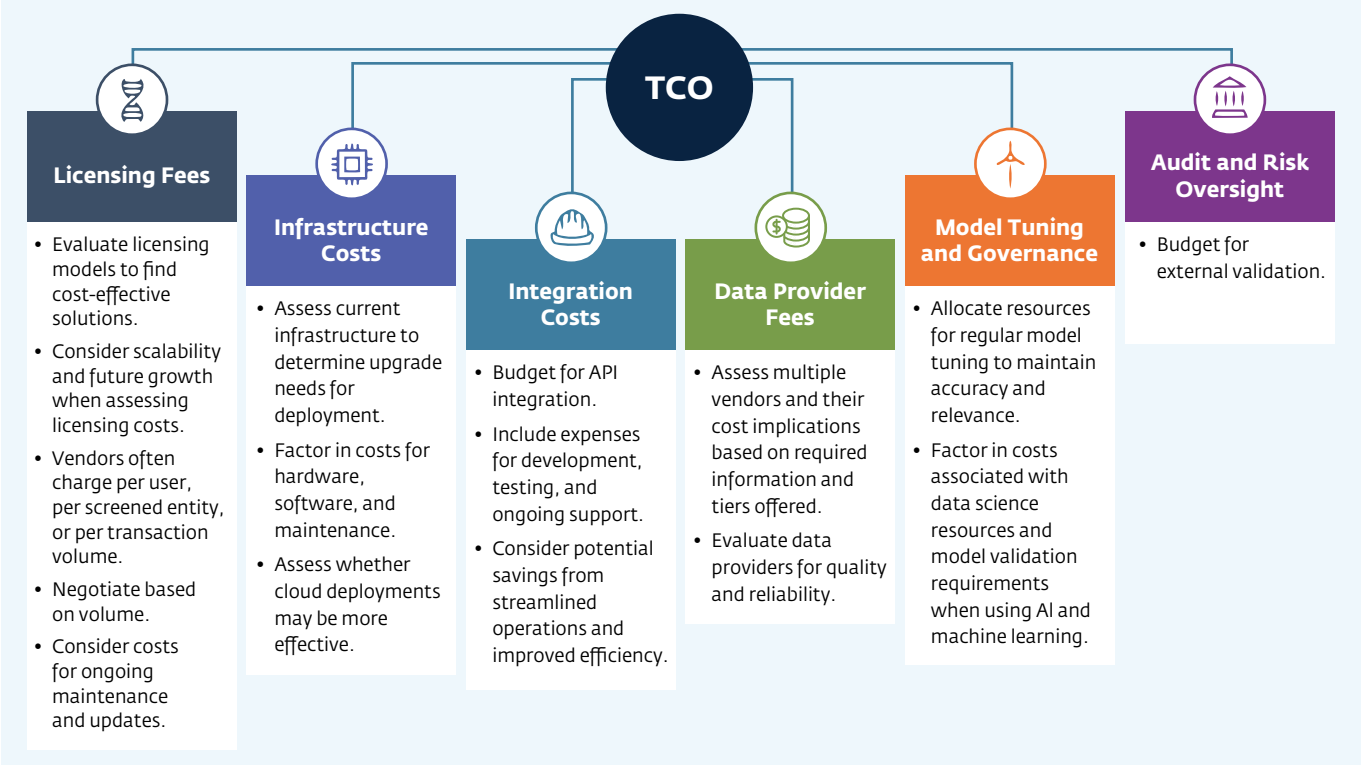
These include the following:

- **Licensing fees** that could be based on company revenue rather than usage, resulting in unpredictable pricing
- **Infrastructure investments** for hardware, cloud services, and ongoing IT support, which can vary
- **Integration complexity and customization** needed to connect vendor systems with existing platforms and data sources
- **Data provider fees for access** to external databases, watchlists, and regular updates
- **Ongoing model tuning and governance** to maintain accuracy, respond to emerging risks, and meet evolving standards
- **Audit and oversight costs**, such as the fee for periodic external validation, if required.

FIs can manage the total cost of ownership by adopting strategies like phased implementation, rigorous data testing, KPI monitoring, targeted staff training, customized detection rules, and allocating future budgets. However, without careful planning, hidden costs can arise (for example, through pricing tied to company revenue, overlooked complexity of a system integration, reliance on default system rules, and neglecting ongoing tuning or upgrades). These issues can lead to inefficient output and increase long-term expenses.

Figure 7.5 highlight six common costs and best practices for evaluating costs early.

FIGURE 7.5 • Common Costs and Best Practices for Early Cost Evaluation



Source: Original for this publication.

7.4.2. Considerations for Contracting Vendors

Establishing strong contract terms with AML/CFT technology vendors is critical for building secure, compliant, and resilient long-term partnerships. Vendors also offer additional protections to FIs, help mitigate regulatory risks, and maintain system integrity. To support sustainable technology implementation and operation, contracts can address performance, data management, ongoing support, and transparency.

Best practices for contracting AML/CFT vendors include the following:

- **Define SLAs for compliance and detection:** Set clear expectations around system accuracy and reliability, issue resolution times, and support for regulatory audits or requests
- **Specify data ownership, privacy, and auditing:** Ensure customer control over sensitive transaction data, clear audit capabilities, and robust data protection aligned with AML/CFT requirements
- **Include continuous support and regulatory update provisions:** Require timely software updates, model tuning, and support in response to evolving regulations and new typologies
- **Establish transparent cost structures and renewal terms:** Detail licensing fees, data provider charges, and renewal conditions to avoid hidden expenses and unexpected price increases
- **Address termination, transition, and data handover:** Implement exit clauses and require vendor cooperation in transitioning systems and data during contract termination or change of provider, preserving compliance and operational continuity.

By including these types of terms, FIs can set relationships with vendors up for success and avoid future hidden costs and/or lack of support when calibrating or upgrading systems. When negotiating and drafting AML/CFT technology contracts, FIs can seek legal advice from counsel familiar with both local regulations and industry practices.

8

Practices for System Deployment and Maintenance

Building on the selection and strategy challenges outlined in Chapter 7, Chapter 8 focuses on the risks and pitfalls that arise during system deployment and ongoing maintenance, as well as the measures FIs can take to ensure technology remains effective over time. Section 8.1 identifies both key outcomes that signal problems and the root causes behind them. Sections 8.2 and 8.3 present practical guidance—from planning and stakeholder engagement to go-live execution, governance, monitoring, and model validation—to help FIs avoid these issues and sustain performance.

Among other topics, Chapter 8 will address the following:

- What are the key challenges and common pitfalls when implementing technology solutions?
- What are key considerations and milestones for deployment?
- How can FIs ensure that relevant stakeholders are involved?
- How should FIs maintain and periodically test those systems and models?

8.1 Key Challenges in System Deployment and Maintenance

Expanding upon key challenges in Chapter 7, FIs often encounter multiple risks and challenges with technology deployment that can undermine transformation objectives.

Potential adverse outcomes experienced by FIs include:

- **Transformation initiatives are delayed or fail to deliver value:** Large-scale projects lose momentum or direction, causing missed deadlines and preventing expected benefits
- **New solutions fail to improve effectiveness and efficiency:** Systems produce poor detection results or operational gains due to unresolved data or process issues
- **Go-live and cutover phases introduce operational and compliance gaps:** Poor execution leads to missed alerts, onboarding errors, or unstable monitoring
- **Low user adoption and resistance to change:** Operational teams are reluctant or unable to use the system effectively, resulting in misuse or workarounds
- **Lack of ongoing calibration and validation:** Models and rules remain static after deployment, reducing relevance and missing emerging typologies.

These challenges are often attributed to one or more of the following root causes:

- **Migration of legacy issues:** Inefficient processes, outdated detection rules, and poor-quality data are carried into the new system
- **Insufficient change management planning:** Stakeholders are not engaged early, training is inadequate, and communication is limited, leading to resistance and misuse
- **Inadequate transition planning and testing:** Go-live is not supported by thorough scenario testing, contingency planning, or readiness checks
- **Weak project governance:** Scope is unclear, milestones are not tracked, and phases are poorly managed, causing delays and misalignment.

The following sections outline practical steps FIs can take to address these outcomes and root causes from effective.

8.2 Practices for System Deployment

8.2.1 Planning for System Deployment

Successful deployment extends beyond core functionality and project delivery to include critical factors such as data quality, stakeholder engagement, training, and ongoing validation. Addressing these factors can mitigate several of the root causes identified in section 8.1—particularly related to migration of legacy issues, inadequate transition planning and testing, and weak project governance—which can lead to delayed initiatives, compliance gaps, and unstable operations if left unresolved. Oversights in these areas can also result in the replication of legacy issues, poor user adoption, and compliance gaps.

Key elements for successful implementation include:

- **Comprehensive planning and strategy** to define migration objectives, project scope, and resource allocation
- **Prioritizing data integrity and quality assurance** through thorough data cleansing, validation, and integration activities
- **Engaging stakeholders and maintaining open communication** to ensure alignment, buy-in, and smooth execution

- **Rigorous testing and validation** in a preproduction environment to simulate rules, thresholds, and operational scenarios and resolve issues before go-live
- **Effective change management and user training** to support adoption, minimize disruption, and optimize ongoing performance.

FIs can enhance implementation outcomes by adopting a phased rollout, conducting real-world scenario testing, providing tailored training, and setting clear performance benchmarks. Continuous feedback and monitoring further support system adaptation and ensure legacy issues are addressed. Without structured planning, hidden challenges such as poor data quality, weak stakeholder engagement, or lack of ongoing training may emerge, increasing risk and operational costs.

8.2.2 Involving Relevant Stakeholders

Active involvement of users and operational units is essential to ensure appropriate buy-in throughout a system deployment. Table 8.1 offers guiding principles for involving and liaising with operational units and system users.

TABLE 8.1 • Principles for Involving Relevant Stakeholders

Step and Purpose	Common Pitfalls	Best Practice
Determine Business Needs Ensure the system addresses actual business challenges and meets user requirements.	Overlooking input from end-users and frontline staff; failing to identify pain points.	Engage a broad cross-section of users; conduct interviews and workshops; document needs, inefficiencies, and priorities.
Assess Current Processes Identify inefficiencies and opportunities for streamlining or automation.	Automating inefficient or outdated processes without careful evaluation of workflows.	Obtain input from end users to map and assess current workflows; separate tradition from necessity; target reduction of manual work and customer friction.
Identify Business Rules Only migrate current, relevant, and risk-based rules to ensure effectiveness and compliance.	Migrating outdated or redundant legacy rules; neglecting risk alignment or documentation.	Consult with end users to develop a detailed rule inventory and review; rationalize and update rules; document changes and ensure direct linkage to FI risk.
Testing and Feedback Validate system functionality, process fit, and usability with real business scenarios and operational users.	Treating testing as a checkbox activity or failing to capture actionable feedback.	Involve end users in UAT and pilots; set up clear, accessible feedback channels; dedicate resources to resolve issues promptly.
Contingency Planning Prepare for unexpected issues and go-live risks and ensure business continuity during migration.	Not planning for failures or rollbacks; underestimating risks at transition.	Develop and communicate robust contingency and rollback plans; conduct scenario planning and establish monitoring and escalation protocols.

Source: Original for this publication.

Refer to section 7.3.2, "Change Management," for additional information on change management considerations when designing a technology implementation and use strategy.

8.2.3 Designing a Go-Live Checklist

The period leading up to deployment and the day of go-live itself can be one of heightened anticipation and risk. Even with rigorous planning, thorough testing, robust governance, and diligent data preparation, the final stages of implementation are critical, as unforeseen issues may still arise. FIs are encouraged to adopt a structured and documented "go-live checklist" to guide the process. While the components and timing of a go-live checklist may differ based on the size, sophistication, and profile of the FI, as well as the system implemented, Table 8.2 serves as an indicative guide of the key activities and controls that can be considered in the weeks, days, and hours leading up to deployment, as well as immediately after go-live.

TABLE 8.2 • Deployment Readiness or "Go-Live" Checklist[55]

Timing	Key Activities	Best Practices and Controls
Complete at Least One Month Before Deployment: Preparation	Build and configure system; load reference data; set detection rules and workflows; implement audit logging; validate and profile input data; run backfill and historical tests; define data quality gates; complete needed testing (such as unit, integration, UAT, regression testing); archive results and documentation; obtain stakeholder sign-off; prepare and dry-run rollback plan.	Engage IT, operations, and compliance in testing; use production-like data; assign data stewards; maintain audit trails and documentation; separate validation roles; freeze nonessential system changes (both upstream and downstream); back up configurations; test rollback triggers and procedures; retain test evidence for audit; conduct a formal go or no-go review for checklist deviation.
Complete at Least One Week Before Deployment: Readiness and Dry Run	Perform platform, data, security, and governance checks; perform dry run with realistic data; rehearse backup and restore procedures; confirm freeze windows (that is, periods when change to a system or application are prohibited or strictly limited); communicate cut-over plans; archive UAT exit reports and readiness evidence; validate monitoring and alerting mechanisms.	Conduct stakeholder readiness review; communicate freeze periods and support channels; archive and document evidence and sign-offs; run and confirm rollback dry run; check data quality gates; confirm support channels for teams.
Complete One Day Before Deployment: Final Dry Run or Freeze	Execute final dry run in a preproduction environment; establish a temporary command center (with representatives from vendor, IT, users, and so on); record snapshot of database and configurations; confirm freeze window; perform precutover checkpoint; archive dry run results and approvals.	Confirm backups and rollback readiness; communicate and verify freeze window; maintain audit trail; ensure clear go or no-go criteria; archive latest configurations and test results.

55 Refer to Appendix A, "Glossary of Key Technology Terms," for definitions and use cases of terms utilized within this table.

Timing	Key Activities	Best Practices and Controls
Deployment Day	Execute release and data migration into live environments; enable ingestion of data flows and output; run smoke, ATL, and regression tests; validate alert volumes, data quality, and KPIs; hold a go or no-go huddle; record stakeholder sign-offs; archive deployment actions and results; activate hypercare monitoring.	Use detailed deployment checklists; document all actions and decisions; record final sign-off and change control; activate rollback of existing software if needed; deploy hypercare team; archive deployment evidence.
Complete 1–30 Days After Deployment: Hypercare	Monitor system health, data flows, and outputs; generate daily dashboards and reports; hold weekly review meetings among internal staff; track SLAs, backlogs, and issues; log corrective actions; archive monitoring outputs; transition to BAU support.	Maintain dedicated monitoring and escalation channels; archive evidence and logs; close change advisory board with evidence pack; record lessons learned for process improvement; prepare for audit and regulatory review.
Complete 30–90 Days After Deployment: Stabilization	Conduct weekly monitoring of KPIs, output quality, and performance; perform root cause analysis; perform preliminary validation and calibration to confirm system is working as intended and to address unforeseen performance issues; optimize rules, thresholds, workflows, as needed; gather user feedback; archive records and documentation; update training and support materials	Incorporate lessons learned; optimize post-go-live settings; prepare audit packs; keep BAU runbooks and guides updated.

Source: Original for this publication.

8.3 Practices for System Maintenance

Once deployed, AML/CFT technology solutions require continuous oversight, calibration, and validation to ensure that they remain effective, explainable, and aligned with regulatory expectations. Automated systems rely on models and data that must evolve with the FI's risk profile and the external threat landscape.

8.3.1 Model Governance

Model governance refers to the framework of policies, procedures, and assigned responsibilities that guide the development, deployment, monitoring, and modification of AML/CFT models. Proper governance can enable clear accountability, transparency, and ongoing oversight and recordkeeping of model-related activities.

Key practices that support strong model governance include the following:

- **Policy framework:** Establishing clear policies for model development, usage, updates, and retirement
- **Model inventory:** Creating a centralized model inventory that tracks purpose, logic, data sources, and change history
- **Defined roles and responsibilities:** Assigning specific roles (such as model owners, validators, data stewards, and compliance officers) and ensuring segregation of duties (usually captured in policies, workflows, and job descriptions)
- **Change control:** Applying change control procedures that require systematic review and approval for

any modification (such as a change to transaction monitoring rules)

- **Auditability:** Maintaining comprehensive audit trails for all model-related decisions and activities
- **Oversight:** Establishing a governance forum that reviews and approves system or rule changes, screening lists and logic, and the results of validation and calibration exercises. Reporting generated from or by this forum enables senior management and the board of directors to be aware of significant changes and their rationale.

8.3.2 Model Explainability

FIs should be prepared to explain the design of their models and the measures taken to keep them updated. While important for managing risks as well as relationships with auditors, regulators, and third parties, transparent documentation and the ability to explain model design and performance is particularly important for advanced models incorporating AI or machine learning.

Key practices that can improve explainability include the following:

- **Ensuring thorough documentation** of model logic, decision processes, validation results, and change history
- **Ensuring the design of models can be explained and understood by stakeholders and regulators**, particularly for AI and machine learning solutions
- **Preparing a compilation of supporting materials,** such as test results, configuration screenshots, procedural documents, governance records, and approval logs, to demonstrate compliance, effectiveness, and successful completion of a process or control for future governance and validation as well as ongoing monitoring.

FIs should also consider proactive engagement with regulators and third parties when undertaking model changes. Key practices include the following:

- **Proactively notifying regulators and correspondent banks** of major model or system changes, planned validation methodologies, and any relevant findings (alongside any remediation plans)
- **Responding promptly to** regulatory feedback and findings (as applicable)
- **Maintaining evidence of improvements made** because of regulatory suggestions or testing, ideally through action plans that are periodically reported to governance committees.

Refer to Section 7.3.4, "Communicating with Regulators and Third Parties" for additional engagement strategies, (primarily focused on strategies in the context of a broader system change).

8.3.3 Ongoing Monitoring and Continuous Improvement of Systems

FIs should have ongoing processes to monitor AML/CFT models and to periodically test those models. These include models for conducting suspicious activity monitoring and assigning customer risk ratings.

Key practices that can improve oversight and performance of models include the following:

- **Producing and reviewing KRIs and KPIs,** such as alert volumes, conversion rates, system performance, investigation outcomes, indications of unexpected trends, high rates of false positives, or potentially missed suspicious activity. Refer to Chapter 4 and Chapter 5 for example KRIs and KPIs used in monitoring and screening
- **Establishing feedback mechanisms** so that comments from investigators, auditors, and regulators, among others, can inform model tuning and recalibration
- **Periodically engaging independent reviewers or external** auditors to perform objective assessments and benchmark performance against industry norms
- **Conducting periodic coverage analyses** and reviews of scenarios in connection with emerging risks and changes to the business model (for example, at least annually for most banks).

Correspondent banks often expect respondent banks to be able to demonstrate that automated systems have been calibrated and validated in a manner commensurate with the respondent's risk profile. Industry practice is for banks to have a set process to review, calibrate, and test models at least annually, and to periodically engage outside reviewers.

8.3.4 Model Validation

Model validation is the process of independently evaluating AML/CFT models to ensure they are fit for their intended use, operate as designed, and do not introduce unintended risk. This practice can enable FIs to maintain system relevance and accuracy over time. Validation should take place both before a model is put into production and periodically thereafter.

Key objectives incorporated in a model validation exercise include the following:

- **Data integrity assessment:** Mapping and assessing the completeness, consistency, and appropriateness of data inputs
- **Conceptual soundness review:** Assessing model assumptions, risk factors, logic, and thresholds to align with institutional policies and regulatory requirements
- **Performance testing:** Conducting back testing using historical data, performing ATL and BTL testing of false positives and negatives (for logic or parameter tuning), and reviewing alert conversion rates. Performance testing is inclusive of a sensitivity and scenario analysis (that is, testing how changes in variables, thresholds, or typologies affect model outcomes) and outcome analysis (that is, comparing model outputs to actual case outcomes, such as STR and SAR filings)
- **Documentation:** Recording validation activities, results, findings, and remediation actions.

As an example, multiple FIs have faced regulatory challenges because AML/CFT systems did not connect properly to updates made to source systems (such as a core banking system). Validating models on an ongoing basis (including testing whether data properly flows from source systems) can assist FIs in avoiding this risk. As a best practice, which additionally draws on industry expertise, FIs can consider periodically engaging external expertise to periodically test or validate systems and models.

9

Emerging Financial Crime Risk Management Accelerators

Technology continues to evolve at a rapid pace that constantly reshapes and advances the landscape of financial crimes risk management. However, criminal organizations are also adopting new methods to circumvent controls and exploit vulnerabilities (such as the use of synthetic identities and deepfakes). FIs must consider future developments and emerging risks when developing their strategies for utilizing technology within their risk management frameworks. This chapter explores the future of financial crime risk management, focusing on four key trends and the evolving role of technology.

Among other topics, Chapter 9 will answer the following questions:

- What are the key emerging trends in the future of financial crime risk management?
- What are transaction monitoring consortiums and KYC utilities, and how can they be used?
- What are the use cases for blockchain and distributed ledger technology (DLT) in AML/CFT?
- How is AML/CFT converging with other risk domains (such as fraud and cybersecurity)?
- How is AI evolving and what are the expected use cases for GenAI and agentic AI in AML/CFT?

9.1 Key Trends in the Future of Financial Crime Risk Management

The following trends are expected to notably influence the future of financial crime risk management:

- Theme 1: Collaboration via consortiums, utilities, and information sharing to improve effectiveness and efficiency
- Theme 2: Convergence of risk domains (for example, cybersecurity and fraud) to improve risk identification
- Theme 3: Harnessing blockchain and DLT to improve transparency and reduce operational costs
- Theme 4: Continued evolution of AI and its application to enhance decision-making capabilities.

The following sections provide additional insights and considerations for each theme.

9.1.1 Leveraging the Power of Information Sharing and Collaboration

Collaboration between the private and public sectors as well as within the private sector has long been recognized as a method to strengthen risk management and accelerate responses to financial crime, with a 2021 FATF publication noting that "advanced analytics applied to data shared by multiple FIs can reveal trends or potentially suspicious activities that could otherwise go undetected by a sole institution" (FATF, 2021b). Coordinated efforts through KYC utilities, consortium models, and information sharing have significant potential to enhance the efficiency and effectiveness of AML/CFT efforts.

Table 9.1 outlines several collaboration models, key benefits, and use cases.

TABLE 9.1 • Collaboration Models in Financial Crime Prevention

Purpose	Key Benefits	Example Use Cases	Examples
KYC Utilities Centralized repository of verified customer identity and beneficial ownership data	• Streamlines onboarding for customers already verified • Reduces duplication of data collection and customer friction (for new customers) • Can reduce costs to individual FIs and improve access to key systems and databases	• Customers submitting UBO data to a central authority • Can be public- or private-sector led, with several examples leveraging e-KYC and government ID systems • Aggregating multiple lists into one database for screening	Singapore's MyInfo and India's Aadhaar KYC are government-run digital identity platforms allowing FIs to access verified customer data directly from government sources with customer consent, reducing onboarding time and errors.

Purpose	Key Benefits	Example Use Cases	Examples
Consortium Models Group of FIs pooling data, resources, and expertise to improve detection and efficiency, primarily in the context of suspicious activity monitoring (although can be used for KYC and other purposes)	• Improves detection capability through collective intelligence and insight into additional transactional activity • Reduces time and financial costs to participating FIs • Enables smaller FIs to benefit from larger participants' data	• FIs with similar profiles or geographic domains forming private utilities • Sharing typology data to improve monitoring • Joint investments in technology systems and databases	Transaction Monitoring Netherlands is a joint initiative by five major banks to detect unusual patterns across institutions, enabling the identification of complex money laundering networks.
Public-to-Private Information Sharing Direct exchange of intelligence between FIs, financial intelligence units, and competent authorities, to detect crossinstitution and cross-border activity (Egmont Group 2025)[56]	• Can enable faster detection and response tied to emerging risks and typologies • Strengthens public-private cooperation on priority areas, with potential to lead to an increase in investigations	• Identifying mule accounts spanning multiple FIs • Detecting coordinated layering schemes • Spotting rapid movements across payment rails • Asset recovery	The United Kingdom's JMLIT, South Africa's SAMLIT, and the United States' FinCEN Exchange brings together banks, law enforcement, and regulators to share intelligence.
Private-to-Private Information Sharing Direct exchange of intelligence between FIs to detect crossinstitution activity (Egmont Group 2025)	• Can enable faster response to identified risks • Provides access to a broader range of transaction information • Potential to lead to an increase in the quality of SARs and STRs	• Identifying mule accounts spanning multiple FIs • Detecting coordinated layering schemes • Spotting rapid movements across payment rails	Section 314(b) of the USA PATRIOT Act of 2001 provides a legal basis for information sharing among FIs in the United States.

Source: Original for this publication.

Note: FinCEN = Financial Crimes Enforcement Network; JMLIT = Joint Money Laundering Intelligence Taskforce; SAMLIT = South African Anti-Money Laundering Integrated Task Force.

9.1.2 Convergence of Risk Domains

Convergence refers to the growing integration and overlap of traditionally separate risk functions, such as AML/CFT, fraud prevention, cybersecurity, and credit risk management. For FIs, this convergence means moving away from siloed risk management and toward a unified view of customers and transactions within an FI. It involves integrating data, tools, and investigative insights across multiple domains to detect risks that cannot be identified by a single team or a system. This convergence reflects the reality that criminals rarely operate within the single risk type. The same customer, account, or transaction can be linked to multiple types of illicit activity, ranging from identity theft and cyber-fraud to money laundering and credit exploitation.

Key drivers of convergence include:

- **Shared data needs:** All risk domains rely on similar core customer and transaction data, enriched with device, network, and behavioral information

56 There have also been advancements in public-to-public information sharing, with the Egmont Group publishing its *Principles for Information Exchange* in July 2025. (Egmont Group 2025)

- **Advances in technology:** AI, machine learning, and improved analytics now make it possible to process and connect risk signals across domains in real time
- **Blurring of attack types:** Fraud, identity theft, credit exploitation, and money laundering often occur together within the same scheme. For instance, a stolen identity might be used to open an account, secure a loan, and launder illicit proceeds. This attack type is often deployed by transnational organized crime syndicates with threat actors not limited to physical geographical locations. It has been supercharged by advancement in technology such as AI and the use of deepfakes
- **Faster payment systems:** The adoption of realtime and instant payments increases the need for immediate, multidomain verification, using signals like device location, transaction frequency, and behavioral patterns to assess risk.

The convergence offers FIs several benefits, including earlier detection of complex schemes by combining intelligence and operational efficiency through shared investigative resources, reduced duplication, and improved accuracy in transaction scoring, leading to fewer false positives. Table 9.2 highlights opportunities to manage risks by leveraging data across domains.

TABLE 9.2 • Opportunities for Leveraging Data Across Risk Domains

Risk Indicator	Cyber	Fraud	AML	Credit	Technology Utilized for Data Collection/Analysis
IP Address Anomalies	✓	✓	✓	X	Device fingerprinting tools, GeoIP services
Login from VPN or Proxy	✓	✓	✓	X	Threat intel APIs, proxy or VPN detection services
Synthetic ID Patterns	✓	✓	✓	✓	Identity resolution, machine learning on data
Velocity of Logins	✓	✓	✓	X	Behavioral analytics, real-time event streams
Geo Mismatch (IP vs. Declared Address)	✓	✓	✓	X	Geo-IP mapping, CRM and KYC system comparison
Inconsistent Declared Income vs. Operations	X	✓	✓	✓	KYC and credit app data vs. transaction analytics
Business Registered in High-Risk Jurisdiction	X	X	✓	✓	Business registry scraping, list reviews
Mismatched Employment or Employer Data	X	✓	✓	✓	Onboarding forms, third-party verifiers
Multiple Accounts with Shared Device or IP	✓	✓	✓	X	Graph analytics, device fingerprinting

Source: Original for this publication.

Note: CRM = customer relationship management; GeoIP = databases that associate locations with IP address; IP = Internet Protocol; VPN = virtual private network.

By integrating data across domains, FIs can build a holistic view of customer and transaction risk contributing to enhanced management of cybersecurity, fraud, financial crime, and credit risks. Entity resolution is expected to play a pivotal role by identifying customers across datasets to provide a comprehensive view of potential threats.

In addition, the creation of centralized data lakes can facilitate cross-domain data ingestion and analysis. While most risk functions currently operate in silos, shared data lakes and early orchestration of alerts and scoring may become a widely adopted standard practice.

9.1.3 Harnessing Blockchain and Distributed Ledger Technology

Blockchain and DLT are often associated with cryptocurrency, but the same features—immutability, transparency, and decentralization—can be harnessed to strengthen detection of illicit activity. Advances in blockchain analytics, smart contracts, and central bank digital currencies now enable real-time monitoring, anomaly detection, and immutable audit trails. These capabilities are already being applied in areas such as cryptocurrency transaction monitoring, beneficial ownership tracking, and cross-border payment transparency. Blockchain can help enable proactive risk detection and prevention when paired with strong governance and integration into existing transaction monitoring frameworks.

Table 9.3 outlines several potential use cases and key benefits in AML/CFT.

TABLE 9.3 • Benefits and Use Cases for Blockchain and Distributed Ledger Technology

Purpose	Key Benefits	Example Use Cases
Cryptocurrency Transaction Monitoring	• Detects illicit flows and sanctions breaches • Identifies suspicious wallet activity • Improves visibility into high-risk networks	• Flagging transactions linked to darknet markets • Detecting transfers to sanctioned addresses • Mapping wallet hops to identify layering
Digital Currency Flow Analysis	• Enables realtime detection of structuring • Distinguishes normal and suspicious behavior • Supports targeted regulatory oversight	• Visualizing wallet flows to detect smurfing • Flagging unlicensed activity • Monitoring high-risk corridors (for virtual currency)
Trade-Based Money Laundering Prevention	• Tracks goods and payments across borders • Creates immutable trade records • Reduces document fraud	• Detecting overinvoicing and underinvoicing • Verifying shipment and payment data • Identifying mismatches in trade finance
Beneficial Ownership Tracking	• Monitors changes to tokenized asset owners • Flags transfers to high-risk jurisdictions • Improves transparency in asset control	• Updating UBO records via smart contracts • Detecting hidden ownership changes • Linking UBO data to sanctions screening
Cross-Border Payment Transparency	• Provides end-to-end visibility • Detects suspicious corridors • Enhances correspondent banking oversight	• Mapping transaction chains • Identifying layering schemes • Monitoring highrisk payment routes
Corruption and Fraud Investigations	• Preserves evidence trails • Verifies transaction authenticity • Supports multiagency investigations	• Tracing bribe payments • Linking intermediaries • Auditing procurement transactions

Source: Original for this publication.

9.1.4 Evolution of Artificial Intelligence

While traditional AI models are already in use (for example, for transaction monitoring and anomaly detection), GenAI and agentic AI are now enabling more autonomous and proactive capabilities. These technologies represent a strategic shift in how FIs can prevent, detect, investigate, and report illicit activity.

The adoption of GenAI and agentic AI offers several high-impact advantages, including the following:

- **Enhanced efficiency:** Automating narrative generation, summarizing complex datasets, and producing draft reports
- **Enhanced effectiveness:** Integrating alerts from various domains (for example, AML/CFT, fraud, cyber, sanctions, and credit risk) for the purposes of assessing risk or identifying linked patterns
- **Scalability:** Handling large and/or increasing volumes of alerts and data without requiring proportional increases in headcount.

Table 9.4 defines GenAI and agentic AI and offers several uses cases in AML/CFT.

TABLE 9.4 • Definitions and Use Cases of GenAI and Agentic AI

Definition	Use Cases
Generative AI (GenAI) AI models that can create new content such as text, images, code, or synthetic data, by learning patterns from existing data. In AML/CFT, GenAI can generate case narratives, simulate transaction typologies, and summarize large volumes of intelligence.	• Automated SAR or STR narrative generation: Generating draft narratives using alert data, customer profiles, transaction histories, and typology context. • Adverse media summarization: Condensing multiple articles, regulatory filings, and intelligence reports into summaries highlighting relevant financial crime indicators • Investigator assistance and report drafting: Compiling investigation summaries from monitoring alerts, screening, and customer communications into a single case file • Typology simulation with synthetic data: Creating realistic synthetic datasets reflecting emerging ML/TF typologies to test systems and detection coverage • Training material creation: Generating tailored AML/CFT training examples, case studies, and scenario-based quizzes for staff onboarding or continuous education • Business line advisory: Automating advisory support to business units on permissible activities by policy and standards
Agentic AI AI systems designed to operate autonomously within defined parameters, capable of orchestrating tasks, integrating multiple data sources, and making decisions in real time. In AML/CFT, agentic AI can dynamically adjust monitoring rules, link alerts across domains, and trigger investigative actions.	• Autonomous alert triage and closure: Monitoring and processing incoming alerts from monitoring systems, screening systems, and adverse media, autonomously closing low-risk cases that match preapproved criteria and escalating higher-risk cases for human review • Dynamic customer risk rating: Autonomously updating customer risk ratings based on changes in behavior, transaction volumes, geographies, or external intelligence • Cross-system alert linking and network analysis: Identifying connections between alerts generated by separate systems (for example, fraud, AML, and cyber), linking patterns that suggest coordinated illicit activity • Proactive typology simulation and detection rule adjustment: Simulating emerging typologies using synthetic but realistic data, then autonomously recommending detection thresholds or adding new monitoring scenarios to improve coverage • Automated SAR and STR draft generation with contextual enrichment: Drafting SARs and STRs by incorporating alert data, customer information, transaction history, and so on, producing near-submission-ready drafts for human review and approval

Source: Original for this publication.

GenAI and agentic AI are becoming strategic enablers of modern financial crime risk management. FIs that invest in these capabilities, alongside strong governance and model validation, can be better positioned to detect complex schemes, reduce operational costs, and meet evolving regulatory expectations.

10

Key Takeaways

This Good Practice Note underscores that technology and analytics are no longer optional enablers, but rather essential components, of a modern, risk-based AML/CFT framework—provided they are deployed responsibly, proportionately, and on top of appropriate foundational controls, quality data, and sound governance.

This Good Practice Note highlights the following key insights:

- **Technology amplifies the effectiveness of a sound AML/CFT program—but cannot replace it.** Advanced tools deliver the greatest value when embedded within a well-governed AML/CFT framework that includes clear risk assessments, robust customer due diligence, effective monitoring and screening, strong governance, and ongoing testing. FIs with weak data quality, unclear risk ownership, or poorly designed processes risk automating inefficiencies or introducing new vulnerabilities. This means that FIs should prioritize foundational controls (and the data and process discipline behind them) before expecting technology to deliver measurable effectiveness gains
- **A risk-based approach should guide technology adoption decisions.** There is no single "right" solution or maturity path. FIs should align technology investments with their inherent risk profile, customer base, product mix, and regulatory environment. Low-risk or smaller institutions may rely on manual or low-tech solutions, while higher-risk or more complex institutions benefit from automation, advanced analytics, and machine learning—often through phased or hybrid approaches. FIs should match tools to their risk exposure and operational realities and build toward higher maturity incrementally as data quality and institutional capacity improve
- **Screening and monitoring technologies must prioritize quality over volume.** High false-positive rates undermine efficiency and investigator effectiveness. The Note highlights practical strategies—such as improved data quality, fuzzy matching calibration, entity resolution, alert risk scoring, and controlled auto-closure—to reduce noise without increasing false negatives. Continuous tuning, testing, and governance are critical for maintaining confidence in automated systems. It is important to measure key risk and performance metrics (for example, false positives, missed matches, conversion rates, and timeliness), tune systems periodically, and document rationale and testing to make outcomes defensible to auditors and supervisors
- **Suspicious activity monitoring has evolved beyond static rules.** While rules-based systems remain foundational, leading institutions increasingly complement them with behavioral analytics, network analysis, and machine learning to detect complex typologies and emerging risks. Successful adoption

depends on model explainability, strong model governance, robust testing, and early engagement with regulators and other stakeholders. Advanced analytics can increase detection and improve prioritization, but only when model risk is actively managed and implementation is staged, tested, and transparent

- **People, governance, and change management remain decisive success factors.** Technology alone does not improve outcomes. Skilled staff, clear roles and escalation paths, documented procedures, and strong oversight are as important as the technology itself. Institutions must invest in training, maintain audit trails, monitor performance through KPIs and KRIs, and foster a culture of continuous improvement. FIs should treat technology programs as organizational transformations (supported by governance, documentation, and internal capability building), not just IT implementations
- **Technology adoption is a journey, not an endpoint.** FIs should view AML/CFT technology as an evolving capability, progressing incrementally as data quality and institutional capacity increase. Many institutions will gain substantial benefit through staged upgrades (including low-tech improvements where appropriate), followed by increasingly advanced automation and analytics. By aligning technology with risk, governance, and strategy, FIs can strengthen financial crime defenses and improve operational efficiency. FIs should define a realistic roadmap, strengthen prerequisites (data, processes, and governance), and avoid "big bang" expectations that exceed institutional readiness
- **Emerging trends point toward greater integration, intelligence sharing, and automation.** The future direction of ML/TF risk management is toward more integrated control environments, better information sharing, and increased automation. Accelerators such as shared utilities, public-private partnerships, and the convergence of AML/CFT with adjacent risk domains (such as fraud), alongside the growing use of advanced analytics, network analysis, and agent-enabled AI, are expected to further modernize AML/CFT controls. Innovation is accelerating, and FIs should track and adopt what is proportionate to their risk and capacity while building the governance needed to use advanced capabilities responsibly.

Taken together, these insights are intended to help FIs deploy technology in ways that not only strengthen AML/CFT effectiveness, but also protect development gains by supporting financial inclusion, preserving access to correspondent banking, and safeguarding the integrity of financial systems that underpin sustainable economic growth.

Appendix A: Glossary of Key Technology Terms

This Good Practice Note utilized various technology terms that have a distinct meaning when used in the context of AML/CFT. Table A.1 is intended to enable readers to understand both the definition of commonly used terms and use cases within AML/CFT.

TABLE A.1 • Glossary of Key AML/CFT Terms and Concepts

Term or Concept	Definition	AML/CFT Use Case(s)
Above-the-Line (ATL) and Below-the-Line (BTL) Testing	Method used to sample alerts that pass just above or just below a set threshold to determine whether the activity should generate an alert.	Calibrate transaction monitoring thresholds and fuzzy logic thresholds in name and transaction screening, reduce false positives or negatives, and improve coverage of typologies.
Agentic Artificial Intelligence (AI)	Software designed to independently make decisions and take actions to achieve specific goals, combining AI techniques with features like memory, planning, and environmental sensing.	Autonomously draft SARs and STRs, perform dynamic CRR, and detect anomalies in transaction monitoring by applying investigative logic to current transactions.
Alert Risk Scoring	Quantitative or qualitative model assigning a risk score to each alert based on severity indicators, entity profile, and contextual data.	Prioritizes workload by ranking alerts by risk and supports triage, escalation, and consistent decision-making in transaction-monitoring reviews.
API (Application Programming Interface)	A set of protocols and tools for pulling data into systems or pushing outputs to other systems and databases, allowing different systems to communicate and exchange data.	Enables real-time data integration for customer onboarding, identity verification, sanctions screening, and ongoing monitoring by connecting internal systems with external data sources.
Automated Screening Tool (AST)	Software designed to screen customer and transaction data against sanctions lists and other watchlists.	Automatically compares data against sanctions lists, consolidates multiple hits into alerts, and streamlines review and management of potential matches.
Behavioral Analytics	Analytical techniques that assess patterns of customer or transaction behavior to identify anomalies or suspicious activity.	Detects deviations from normal behavior, supports dynamic risk scoring, and enhances detection of new or evolving ML/TF typologies.
Biometrics	Automated recognition of individuals based on unique physical or behavioral characteristics (for example, fingerprints, facial features, and voice).	Provides advanced identity verification during digital onboarding, liveness detection, and fraud prevention in remote customer onboarding or during a transaction.
Case Management System	A platform to automate and regulate the life cycle of AML/CFT workflows (such as alert reviews, EDD, and ongoing due diligence) from initiation to completion.	Centralizes investigation records, enables workflows (particularly when multiple individuals are involved), supports audit trails, integrates with monitoring and CDD systems for efficient alert handling and regulatory reporting, and provides reporting of KRIs or KPIs.

Term or Concept	Definition	AML/CFT Use Case(s)
Clustering	Grouping similar data points (for example, customers or transactions) using statistical or machine learning techniques.	Identifies peer groups for risk scoring, detects outlier behavior, and supports segmentation in transaction monitoring.
Coverage Assessment	Reviewing and mapping detection rules to identified risks and typologies of illicit crime to enable appropriate monitoring coverage.	Enables suspicious activity monitoring programs and transaction monitoring systems to address relevant ML/TF risks and typologies, identify gaps in current monitoring rules, and implement improvements to enhance the quality of detection coverage.
Customer Risk Rating (CRR)	A scoring system that assesses the risk level of a customer based on defined criteria and weighted factors.	Segments customers for risk-based due diligence, triggers EDD, and informs transaction monitoring thresholds.
Data Lake	A centralized repository for storing structured and unstructured data at scale.	Aggregates and standardizes customer, transaction, and external data from multiple sources to be applied for one or more purposes (such as customer risk rating).
Digital Identity	Solutions that verify the identity of individuals or entities using digital credentials and authentication factors.	Supports secure customer onboarding, reduces manual input errors, and supports due diligence through biometric identity verification and integration with national ID systems.
Distributed Ledger Technology (DLT) or Blockchain	A protocol enabling simultaneous access, validation, and updating of an immutable ledger across multiple computers or entities.	Provides secure, tamper-proof records for customer information, transaction traceability, and detection of illicit activities in cross-border payments and trade finance.
Dual Use Goods	Products, materials, software, or technology that can be used for legitimate purposes (for example, industrial manufacturing and medical research) as well as for military, defense, or weapons-related activities. Many goods are controlled under international treaties, national export regulations, and sanctions regimes because of their potential role in PF, arms trafficking, or other activities that could threaten security.	Transactions involving dual-use goods can signal high-risk patterns that warrant EDD, especially in trade finance and cross-border payments.
Entity Resolution	Identifying and linking records across different data sources that refer to the same real-world person or entity.	Prevents duplicate customers, uncovers hidden relationships, improves detection of complex ownership structures, and creates a "golden source" of customer data.
False Positive (FP), False Negative (FN), True Positive (TP), and True Negative (TN)	Classification metrics evaluating model or rule accuracy: FP = incorrectly flagged as suspicious; FN = missed suspicious activity; TP = correctly flagged suspicious; TN = correctly dismissed normal activity.	Used to measure performance of screening and monitoring tools, calibrate thresholds, and optimize alert quality while balancing detection coverage vs. efficiency.
Freeze Window	A scheduled period during which changes to a technology system, application, or infrastructure are prohibited or strictly limited, typically to ensure stability during critical operations such as go-live deployment, end-of-year processing, or regulatory reporting cycles. Only urgent, approved changes (for example, security patches or critical bug fixes) are permitted.	During AML/CFT system go-live or hypercare phases, a freeze window prevents configuration changes that could disrupt sanctions screening, suspicious activity monitoring, or CRR processes. This ensures consistent alert generation, data integrity, and compliance reporting while the new system is stabilizing.

Term or Concept	Definition	AML/CFT Use Case(s)
Fuzzy Logic / Fuzzy Matching	Algorithms that identify potential matches through approximation, accounting for misspellings, aliases, and transliterations.	Reduces false negatives in sanctions and PEP screening by matching similar names, even with data quality issues or different alphabets.
Generative AI (GenAI)	AI models capable of creating new content (text, images, code, or data) by learning patterns from existing data. Unlike rule-based systems, GenAI generates novel outputs dynamically.	Produces draft narratives for SARs and STRs, generates synthetic training data for typology testing, and automates documentation and report summarization.
Geolocation	The process of identifying the physical location of a user, device, or transaction, based on data emanating from a device (such as IP address or GPS).	Detects location anomalies (for example, access from high-risk or inconsistent jurisdictions) and supports geobased transaction monitoring and sanctions compliance.
Global Positioning System (GPS)	A satellitebased navigation system that provides accurate location and time information to GPSenabled devices anywhere with a clear line of sight to satellites.	Verify customer location during onboarding or transactions, detect geographic anomalies indicating potential fraud or ML/TF risk, and enforces geofencing (as needed).
Graph Analytics	Analytical techniques that map and analyze relationships between entities (for example, customers, accounts, and transactions).	Uncovers hidden connections, identifies networks of suspicious activity, and supports UBO analysis.
Hypercare	A temporary, intensive support phase following the go-live deployment of a new technology system, during which issues are actively monitored, resolved, and communicated in real time to ensure stability, performance, and user adoption. Hypercare typically involves dedicated resources, heightened monitoring, and expedited escalation processes.	In AML/CFT technology deployments, hypercare can ensure that transaction monitoring, screening, and alert review systems operate as intended immediately after go-live. Dedicated support teams can rapidly address false positive spikes, data integration errors, or configuration issues, minimizing compliance risks during the critical transition from implementation to business-as-usual (BAU).
Internet Protocol (IP) Address	A unique numerical identifier assigned to each device connected to a network, enabling communication between the device and other systems over the internet.	Identifies the geographic source of online activity, detects location mismatches, flags connections from highrisk or sanctioned jurisdictions, and recognizes patterns of suspicious access behavior.
Latency	The time delay between a system input and the corresponding output or response.	Critical for real-time AML systems. Low latency enables timely interdiction of suspicious transactions before settlement.
Machine Learning	A subset of AI that enables systems to learn from data, identify patterns, and make decisions with minimal human intervention.	Transaction monitoring and sanctions screening to reduce false positives, detect patterns aligned with previously identified suspicious activity or true positives, and enable alert closure or prioritization based on historical outcomes.
Metadata	Information that describes and provides context about other data, such as its source, creation date, author, format, or classification.	Metadata supports data integrity, auditability, and efficient retrieval by recording details about when, how, and by whom customer information was collected or updated.
Model Validation	Independent assessment of an AML/CFT model to confirm it is fit for its intended purpose, operates as designed, and produces accurate, reliable, and explainable outputs without introducing unintended risks.	Verify transaction monitoring models, CRR methodologies, and screening algorithms to ensure they detect relevant illicit activity, comply with regulatory expectations, and perform effectively over time.

Term or Concept	Definition	AML/CFT Use Case(s)
Natural Language Processing (NLP)	A branch of AI that enables computers to understand, interpret, and manipulate human language.	Adverse media screening to perform sentiment analysis, extract risk factors from news articles, and reduce false positives by interpreting context.
Noise	Refers to irrelevant or false-positive alerts that do not indicate genuine risk but can obscure true suspicious activity and hinder operational efficiency.	Noise encompasses false positives, redundant matches, alerts triggered by common names, outdated information, or data errors that do not represent true risk or needed action. Noise reduces the effectiveness of systems by overwhelming investigators with unnecessary alerts, potentially causing real threats to be missed and increasing operational costs.
Optical Character Recognition (OCR)	Technology that converts different types of documents, such as scanned paper documents or images, into editable and searchable data.	Digitize and extract information from identity documents during onboarding, supporting automated verification and reducing manual errors.
Perpetual KYC (pKYC)	A continuous process for updating and monitoring customer profiles using automated data feeds and analytics.	Dynamic risk scoring, timely detection of changes in customer risk, proactive escalation to EDD or transaction monitoring.
Principal Component Analysis (PCA)	A statistical technique used to reduce the number of variables and identify key features that distinguish true positives from false positives in alert data.	Suppression of low-risk alerts in screening systems, enhances model explainability for regulatory review.
Productivity Dip	A temporary decline in performance, efficiency, and/or output that occurs when FIs transition to new systems, processes, or technologies.	An FI is unable to review the same quantity of alerts stemming from name and transaction screening and transaction monitoring in the same period.
Robotic Process Automation (RPA)	Productivity tools that automate repetitive tasks by mimicking human actions within digital systems.	Reduces manual workload in alert triage, accelerates onboarding, and supports automated data entry and verification in the CDD and transaction monitoring processes.
Rollback	A controlled process of restoring a technology system, configuration, or dataset to its earlier version or state, usually to recover from failures or mitigate risks following the introduction of new changes. Rollbacks are guided by predefined change management and contingency plans to ensure minimal disruption and maintain compliance.	If a newly implemented transaction monitoring platform begins producing excessive false positives, missing true matches, or fails to integrate properly with upstream systems, the FI can initiate a rollback to the prior system or configuration to preserve accurate alerting until fixes are applied. Rollback processes are also used if deployment causes data corruption, breaches regulatory requirements, or disrupts reporting to authorities.
Rule, Scenario, or Detection Rule	Predefined logic or parameters in transaction monitoring systems that trigger alerts when certain patterns or thresholds are met.	Detect potentially suspicious activity, such as structuring, rapid movement of funds, and transactions with high-risk jurisdictions.
Rule Calibration or Threshold Setting	Adjusting detection rule parameters to optimize alert generation, balancing false positives and negatives.	ATL and BTL testing, back-testing on historical data, or periodic review to maintain model effectiveness.
Ruleset or Detection Rule Library	A structured collection of predefined logic statements or algorithms used to identify patterns indicative of suspicious behavior.	Forms the backbone of transaction-monitoring systems; continuously tuned using ATL and BTL testing and feedback from investigators.

Term or Concept	Definition	AML/CFT Use Case(s)
Sanctions Screening	Checking customers, transactions, and counterparties against official lists of sanctioned individuals, entities, and jurisdictions.	Detects engagement with sanctioned parties, enables regulatory compliance, and reduces exposure to financial crime risk.
Self-Organizing Maps (SOMs)	Unsupervised neural network techniques that cluster and visualize high-dimensional data to reveal patterns and anomalies.	Adverse media and PEP screening to group similar alerts, identify outliers, and prioritize high-risk cases for investigation.
Suppression (or Auto Closure)	Automated process that closes alerts or cases when predefined low-risk criteria are met (for example, duplicate alerts, low-value recurring transactions).	Frees analyst capacity by automatically clearing low-risk alerts, subject to documented governance and audit controls.
Transaction Monitoring System	Software solutions that detect potentially suspicious activity and/or transactions by analyzing them against predefined rules and behavioral patterns (in traditional systems).	Automated surveillance of customer transactions that detects activities consistent with predefined patterns or thresholds and generates alerts for review.
User Acceptance Testing (UAT)	A formal testing process in which end users validate that a new or upgraded technology system functions as intended and meets documented business requirements in a real-world or simulated environment before final deployment.	UAT allows users (such as compliance officers, investigators, and screening analysts) to verify that systems and processes perform correctly and in line with stated business needs. UAT may result in additional refinements before a system (or later changes to a system) goes live.
Utility or Consortium	Shared platform or database jointly operated by multiple FIs (and sometimes regulators) to exchange standardized data or analytical results.	Enables collaborative KYC and identity verification, shared adverse-media screening, and typology detection across institutions while reducing duplication and costs.
Vendor Partner	A third-party technology or service provider with whom an FI establishes a formal, collaborative relationship to deliver, maintain, and enhance solutions that support the FI's operations, compliance requirements, or strategic objectives. A vendor partner is not only a supplier but also a long-term collaborator, sharing responsibility for successful implementation, integration, and ongoing performance of the product or service.	A vendor partner might provide transaction monitoring platforms that detect potentially suspicious activity, sanctions, and watchlist screening tools with API integration, CDD solutions that leverage digital identity verification, data feeds for adverse media, PEP lists, and other risk intelligence.
Vendor Viability	An assessment of a vendor's financial health, operational capacity, market position, and long-term sustainability to determine whether it can reliably deliver, maintain, and enhance its products or services throughout the partnership. Vendor viability is a critical factor in technology selection to ensure ongoing support, updates, and compliance alignment.	A vendor that loses viability may stop providing updates for detection rules, sanctions lists, or screening algorithms, impacting compliance. Lack of viability can lead to service disruptions or inability to integrate with future technologies.
Whitelisting	A control mechanism that marks certain entities, accounts, or behaviors as trusted or exempt from specific monitoring rules.	Reduces false positives by excluding verified low-risk customers, counterparties, or recurring payment patterns from repetitive alerting.
Workflow Management	Systems that automate and standardize business processes, ensuring tasks are carried out consistently and efficiently.	Streamlines AML/CFT operations, minimizes delays, and supports escalation and approval processes in investigations and onboarding.

Source: Original for this publication.

Appendix B: Control Maturity Matrix

As previously noted in this Good Practice Note, particularly in Chapter 2 and Chapter 7, FIs must have foundational controls in place before technology can enable material gains in effectiveness and efficiency. This Good Practice Note referenced control maturity and provided several examples escalating maturity for elements of CDD, screening, and monitoring. Table B.1 summarizes those examples and provides additional examples organized by element or stage of CDD, screening, and monitoring, respectively. The table, which defines five stages of control maturity—ranging from "basic" to "agile"—includes examples of practices aligning with the stage of maturity. It was built based on IFC's experience (with input for contributors) and should not be considered a definitive source of control maturity; rather, its purpose is to provide readers with a tool for understanding existing control maturity and control areas that may benefit from additional automation or techniques defined within this Good Practice Note.

TABLE B.1 • Examples of Elements of Customer Due Diligence, Screening, and Monitoring

Area	Basic	Fragmented	Managed	Integrated	Agile
Customer Due Diligence (Chapter 3)					
Information Capture	Client information is captured in spreadsheets or other nonelectronic formats.	A system exists for capturing customer information, but it is not aligned to policy requirements.	The system is aligned to policy and supports document uploads with metadata tags.	Forms are partially auto- populated with information sourced from external vendors and databases.	Data is captured and integrated within a data lake, available for use in multiple applications.
Document and Data Storage and Retention	Documentation is stored in hard copy and/or not in centralized, searchable location.	Multiple systems are used by different teams, resulting in no single view of the customer record.	A centralized digital KYC platform is used for customer onboarding.	APIs connect systems and applications, providing a single view of the customer.	Document and data capture is fully automated with real-time validation, enriched from multiple sources, and instantly available through a unified customer profile.
Customer Risk Rating Methodology	The FI has no documented method, and ratings are based on simple manual judgment using a few static factors.	Criteria vary across business units, resulting in inconsistent scoring and poor data quality.	A standardized methodology applies weighted factors, with ratings updated at onboarding, periodic reviews, or trigger events, and linked to AML/CFT controls.	A centralized system uses static and dynamic factors, automatically updating ratings from internal and external data and linking them with other AML/CFT systems.	Ratings are fully automated, continuously recalibrated from alerts and evolving typologies, and integrated across risk domains for an enterprise-wide view.

Area	Basic	Fragmented	Managed	Integrated	Agile
Customer Risk Rating Frequency	Customer risk ratings are not updated after initial onboarding.	Customer risk ratings are updated but based on static data factors, so the risk remains constant after the periodic review.	Customer risk rating occurs after the periodic review, with EDD triggered if new high-risk factors are identified.	Customer risk rating is performed as factors are updated or when new information (for example, monitoring alerts) results in a change to the customer's risk profile.	Customer risk rating is perpetual, with the customer record continually updated to reflect the latest risk profile, based on internal and external factors.
Enhanced Due Diligence	There is no defined driver for when EDD should be performed or what information and/or analysis is required. EDD is performed only when there is a request for information or an alert.	EDD requirements exist but are not supported by the system or processes. EDD is performed periodically for high-risk customers but not necessarily on a set frequency.	A system flags accounts when additional information or EDD may be required. Alerts are generated when customers are due for periodic refreshes.	Monitoring, adverse media, and other alerts automatically filter into the EDD process. A trigger-based review strategy is used, with reviews performed as customer risk profiles change; outcomes impact risk ratings.	EDD processes are continuously refined to address new threats and regulatory changes. EDD may be triggered through the enrichment of data from both internal and external sources.
Ongoing Due Diligence	Reviews are performed reactively with no set frequency.	Basic event-driven reviews are conducted, typically when static customer data (such as address details) changes.	A system manages a defined refresh cycle on a periodic basis, based on customer risk. Refreshes occur periodically or from a trigger event.	Dynamic trigger events focus on ongoing updates to client information rather than solely periodic reviews.	Real-time monitoring is enabled via APIs to external data sources (for example, business registry and credit data), supported by autonomous detection of profile changes (like address).
Name and Transaction Screening (Chapter 4)					
Sanctions Screening Processes and Tools	Manual web searches are performed using online databases and official government or international organization websites.	Basic watchlists are utilized, often those that are freely available. An automated screening system may be in place.	An automated screening system is in place and employs fuzzy logic. Lists are updated through uploads of new files.	An automated screening system is in place and employs fuzzy logic. Dynamic list updates are performed, generally by the vendor.	Continuous monitoring of customer data and activity against dynamic lists is done, there is plug-in capability for new lists, and methodologies are in place to rate risk or suppress matching alerts.
Sanctions Screening Frequency	Sanctions screening of customers is only performed during onboarding.	Clients are regularly reviewed on a batch basis, with delta screening (list changes) performed periodically.	Automated name screening is integrated with core systems, with both batch screening against changes in deltas (at least daily).	Screening is performed at onboarding, as transactions occur (for example, during cross-border payments) and during maintenance activities.	Screening is continuous (typically at least daily) with cases flagged as required.

Area	Basic	Fragmented	Managed	Integrated	Agile
Name and Transaction Screening (Chapter 4) (cont.)					
Sanctions Screening Alert Reviews	Employees follow basic criteria to see if there is a name match. There may not be an audit trail or metrics maintained on hits and decisions.	There is a defined process for alert review, but the process may not be followed in practice. Some documentation is maintained and metrics are tracked.	There is a defined process for alert review that is followed in practice. Systems enable documentation of alert reviews, metrics, and quality assurance reviews.	Clear case management and workflow are in place. List suppression is performed, and relevant decisions are documented. Alerts may be filtered to improve quality.	Machine learning is used to suppress alerts, with models tested to ensure suppression remains within risk appetite.
Adverse Media Processes and Tools	Searches are conducted using web browsers or free tools, with results neither documented nor retained.	Basic news aggregator tools are employed, utilizing search engine-optimized strings to generate higher quality alerts.	A screening tool is implemented, providing feedback on searches performed and typically integrating with a list provider.	The screening tool is integrated with CDD and monitoring systems, providing a comprehensive overview of customer risk.	Screening is performed in continuously, leveraging multiple sources from global media, including the dark web, but with logic resulting in only material alerts generated for human review.
Adverse Media Screening Frequency	Adverse media screening is performed occasionally, typically when a risk is identified or upon request.	Screening occurs at onboarding or when triggered by specific events requiring further review.	Screening is performed at onboarding, during customer refresh, and periodically throughout the relationship.	News outcomes impact customer risk ratings, generating workflow items for ongoing monitoring. Alerts are generated continuously, with deduplication to ensure relevance.	Screening is continual, with dynamic updates to customer risk rating (as applicable) and workflow, but with logic resulting in only material alerts generated for human review.
Adverse Media Alert Reviews	Employees manually reviews matches to media articles and input data, leading to omissions, errors and inefficiencies. Screening and alert reviews are not documented.	Screening results are analyzed to identify concerns, with minimal relevance filtering.	Screening results in customer record. Advanced systems store and manage adverse media data, making it accessible to authorized personnel.	NLP is utilized to filter and classify relevant hits. AML functions are connected, enhancing collaboration and efficiency.	AI systems extract structured risk factors and classify news by risk type (for example, financial crime and reputational risk).

Area	Basic	Fragmented	Managed	Integrated	Agile
Suspicious Activity Monitoring and Reporting (Chapter 5)					
Monitoring Processes and Tools	There is no automated transaction monitoring system in place. Monitoring, if performed, is completed manually and on an ad-hoc basis.	There is a basic automated monitoring system utilizing rules focused primarily on regulatory reporting (such as receipt of cash).	There is an automated monitoring system in place with predefined rulesets generating alerts tied to indications of suspicious activity.	There is an automated monitoring system in place with rules that are calibrated periodically and segmented by customer types and products.	Machine learning and anomaly detection are utilized to identify risks that are not detected through static rules.
Monitoring Alert Reviews	There is no clearly defined process to complete alert reviews and no consistent evidence saved of the alert review or investigation.	Manual case management is performed, with some information maintained in the customer file.	Automated alert routing and monitoring are performed using an integrated case management tool.	Alerts are prioritized based on risk scores, and audit logs are available for each review.	Contextual case information is generated based on past alerts and the nature of transactions.
Suspicious Activity Reporting	Reporting to the financial intelligence unit is performed manually and often does not include all required information.	Reporting to the financial intelligence unit is undertaken on an as-needed basis in response to specific requirements or events.	Reporting to the financial intelligence unit are enabled by system tracking with a full audit trail to support investigations.	Reporting to the financial intelligence unit is populated with relevant information prior to human submission.	Reports can be automatically sent to the financial intelligence unit
Model Effectiveness and Rule Setting	No statistics on the number of alerts or the effectiveness of rules are maintained.	High false positives occur as rules are static in nature and lack a feedback loop for improvement.	Rules are calibrated, and ATL and BTL testing is performed annually, with feedback provided for alert tuning.	Rules are informed by typologies and the changing risk profile of the organization. Model tuning approaches such as ATL and BTL testing are utilized, and rule effectiveness is analyzed to improve models.	Ongoing learning from closed alerts is used to improve model effectiveness. Dashboards provide a real-time view of transactional activity and risk, with model governance measures in place to manage risk and ensure explainability.

Source: Original for this publication.

Appendix C: Detection Strategies for Common Typologies

As noted in Chapter 5, FIs must have capabilities to detect potentially suspicious activity aligned with the risks they face (which may be derived from, among others, exposure to certain typologies, customer segments, or products and services). This appendix is intended to assist FIs in understanding potentially suspicious patterns linked to common typologies to be used as a tool when designing suspicious activity monitoring coverage. Table C.1, which leverages information from typology reports, industry sources, and contributors to this project, in addition to IFC's own experience, provides examples of suspicious patterns, detection strategies, and rules FIs may consider when designing suspicious activity monitoring coverage.

TABLE C.1 • Example Detection Strategies for Common Typologies

Typology	Potentially Suspicious Patterns	Considerations for Detecting Patterns
Human Trafficking Human trafficking often involves organized networks facilitating the recruitment, transportation, and exploitation of victims, with financial activity characterized by structured payments, use of intermediaries, and transactions linked to travel, accommodation, or movement of individuals.	• Payments to travel, hospitality, medical, or visa services for unrelated individuals • Payments to adult service websites or for adult clothing • Frequent funding to hostels or hotel chains • Rapid transfers between unconnected parties • Payments at off-peak times of day (after midnight and before dawn) • Multiple small deposits from diverse geographies • Transactions inconsistent with customer profile • Activity in high-risk sectors or known trafficking corridors • Repetitive small payments for atypical services • High volume of activity involving ATMs	• Lower monitoring thresholds for high-risk merchant codes (for example, hospitality, travel, and ceremonies) • Monitor frequent, low-value payments • Flag transfers to high-risk regions • Identify payments related to property rentals or purchases outside the customer's usual region • Detect payments made without matching travel bookings

Typology	Potentially Suspicious Patterns	Considerations for Detecting Patterns
Child Sexual Exploitation Online child sexual exploitation often involves offenders using online platforms to share, purchase, or commission child sexual abuse material. Financial flows may involve small, frequent payments through various payment methods, often concealed under legitimate service or content labels (FATF 2025d).[57]	• Multiple recurring low-value payments to online content platforms, streaming services, or P2P payment apps • Uncharacteristic use of individual peer-to-peer platform accounts, digital gift cards or gaming credits, and prepaid cards • Uncharacteristic purchase of virtual assets (such as frequent conversion between fiat and cryptocurrency for small amounts). • Unusual payment descriptors or vague invoice narratives (for example, transactions structured to conceal purpose) • Uncharacteristic funding linked to online video conferencing or hosting services	• Monitor corridors that present heightened geographic risk (such as transactions from advanced economies to higher risk jurisdictions) • Apply enhanced scrutiny to transactions involving high-risk merchant codes or payment processors associated with online streaming or content sharing • Flag payments made to receivers in another jurisdiction with whom the remitter has no apparent legitimate connection • Flag repeated micropayments coupled with cross-border activity. • Flag payments typically occurring between 7pm and 7am (usually as the sexual extortion is happening in real time)
Drug Trafficking Drug trafficking typically generates large volumes of illicit proceeds that are introduced into the financial system through cash-intensive deposit activity, structuring of deposits and/or payments, layering across multiple accounts, and transactions linked to high-risk regions or trade-based schemes.	• Structuring large cash proceeds into smaller deposits • Trade-based money laundering, including overinvoicing or underinvoicing (for example, of chemical or consumer goods) • High volume of cash deposits in known drug production or trafficking regions • Abrupt variations in account balances inconsistent with customer profiles • Transactions linked to high-risk regions or corridors • Use of shell companies, funnel accounts, and PSPs, for movement and layering of funds)	• Analyze trade invoices for relevant deviations from market practices and benchmarks • Identify multiple transfers through PSPs without clear customer links • Scrutinize high-volume cash deposits or patterns in known trafficking regions • Detect use of funnel accounts consolidating deposits for cross-border transactions
Terrorism Financing Terrorism financing is frequently characterized by relatively small transactions, often involving high-risk jurisdictions, abuse of charities or NGOs, and payment patterns designed to evade detection thresholds.	• Multiple small deposits from apparently unrelated parties (often disguised as donations) • Use of charity or NGO businesses for deposit and payment activity • Small, high-frequency cross-border transactions • Structuring to evade reporting thresholds • Transactions lacking a clear economic rationale • Payments to or from sanctioned or embargoed parties	• Monitor repeated small transfers to high-risk jurisdictions • Flag round-number transactions (for example, $100) • Apply lower thresholds for recipients with charity or NGO merchant codes • Track rapid outbound movements after inflows • Identify high inflow or outflow turnover within short periods

57 Refer to Annex A of the FATF's Report on Detecting, Disrupting and Investigating Online Child Sexual Exploitation for additional indicators (FATF 2025d).

Typology	Potentially Suspicious Patterns	Considerations for Detecting Patterns
Proliferation Financing Proliferation financing involves efforts to procure, transport, or finance dual-use goods or restricted materials used in the development of weapons of mass destruction, often using complex payment structures, intermediaries, and transactions linked to sanctioned parties or jurisdictions.	• International trade activity involving dual-use goods or shipments to sanctioned destinations • Rapid, circular merchant payments and fund recycling patterns • Payments lacking documented commercial justification • Use of high-risk jurisdictions and restricted industry merchant codes	• Identify payments linked to dual-use goods via merchant codes or trade documentation • Detect frequent trade payments to sanctioned or embargoed zones • Monitor repetitive counterparty and circular fund flows (for example, same funds circulating across accounts) • Track excessive use of intermediary banks • Scrutinize FX activity inconsistent with business profiles or geolocation
Environmental Crimes Environmental crimes encompass a range of illicit activities involving restricted natural resources, frequently reflected in trade flows exceeding legal limits, use of front companies, and transactions routed through jurisdictions with weak environmental controls.	• High-volume trade in commodities subject to sustainability or environmental restrictions • Transactions routed via jurisdictions with weak environmental controls • Use of freight forwarders or front companies to obscure origin of goods • Exports of timber, fish, or wildlife without required permits, or exceeding caps • Trade volumes exceeding declared capacity or inconsistent with demand	• Monitor routing of goods through high-risk transit hubs to conceal source or destination • Scrutinize large cash transactions originating from sensitive or protected areas • Detect structuring into multiple smaller wire transfers • Identify discrepancies between shipping documents and invoices • Conduct screening over counterparties (for indications of shell company or financial crime)
Illegal Mining Illegal mining generates illicit proceeds through unlicensed extraction and trade of minerals, often reflected in cash-intensive activity, exports inconsistent with declared production capacity, and transactions involving high-risk mining regions or intermediaries.	• Payments to or from mining areas without declared licenses • Export volumes inconsistent with reported production capacity • Cash-intensive activity inconsistent with stated business profile • Transactions with regions known for illegal mining • Use of intermediaries or traders in high-risk jurisdictions • Export invoices misaligned with prevailing market prices or reported shipment weights • Purchases of mining equipment inconsistent with customer profile	• Verify customer's licenses through EDD and external databases (as available) • Flag transactions involving high-risk mining zones • Monitor cash intensity relative to industry norms • Compare export invoice values to market prices or production figures • Detect trade flows to nonlicensed parties • Identify layering through multiple intermediaries prior to refining material or export • Monitor purchases of mining equipment for consistency with declared business activity
Illegal Wildlife Trafficking Illegal wildlife trafficking involves the trade of protected species, with financial activity often linked to source or transit jurisdictions, logistics providers, shell entities, and payments lacking proper documentation.	• Payments to exotic animal vendors or wildlife tourism operators • Trade in high-risk flora or fauna without valid CITES documentation • Transactions involving wildlife source or transit jurisdictions • Vague item descriptions (for example, "natural goods") • Use of shell companies or newly incorporated entities • Large or repeated cash deposits without matching business activity	• Monitor payments to logistics or freight firms with no declared trade history • Identify shell companies, newly incorporated entities (<12 months old), and e-commerce platforms trading wildlife commodities • Track cross-border wires to wildlife hotspot jurisdictions • Detect suspicious use of HS codes • Monitor payments routed via higher-risk intermediary hubs

Typology	Potentially Suspicious Patterns	Considerations for Detecting Patterns
Bribery and Corruption Bribery and corruption typically involve illicit payments, kickbacks, or asset transfers to influence decision-making, often conducted through intermediaries, relatives, or offshore structures, and commonly associated with politically exposed persons (PEPs) or public-sector transactions.	• Unusually high consulting or advisory payments • Use of third-party agents, relatives, or offshore accounts • Private asset acquisitions or refinancing of assets inconsistent with salary and wealth • Public officials transacting through associates or intermediaries • Sudden, unexplained account balances or asset acquisitions among low-salaried officials • Luxury asset purchases that are disproportionate to declared income • Account balances and amount of account activity significantly higher than salary	• Compare asset values and luxury purchases to official salary or declared income • Flag contractor-to-official transfers and frequent round-dollar payments • Map networks of family members and associates • Monitor for repeated higher-value payments to or from the same vendor or company • Track large cash withdrawals or deposits around tender awards or elections
Tax Evasion Tax evasion generally involves illegal arrangements where liability to tax is hidden or misrepresented. This may be through misrepresentation of financial information to reduce tax liabilities (often reflected in discrepancies between reported income and financial activity), the use of offshore structures, and/or abnormal cash or trade patterns.	• Underreporting of income or underinvoicing of exports • Use of double books or shadow accounts to conceal financial activity • Complex offshore arrangements • Cash-intensive businesses reporting abnormally low revenue or sales (or turnover) • Discrepancies between financial statements and tax filings	• Compare trade invoice values to customs data • Benchmark revenue or sales against peer group and industry averages • Look for use of multiple accounts to spread or disguise revenues • Identify discrepancies between tax filings and financial reporting • Monitor offshore transfers lacking declared income justification

Source: Original for this publication,

Note: CITES = Convention on International Trade in Endangered Species.

References

ABS (Association of Banks in Singapore). 2024 *Industry Perspectives on Best Practices: Leveraging on Data Analytics and Machine Learning Methods for AML/CFT*. ABS, Singapore. **https://abs.org.sg/docs/library/acip-industry-perspectives-on-best-practices---leveraging-on-data-analytics-and-machine-learning-methods-for-amlcft.pdf**.

APG (Asia/Pacific Group on Money Laundering). 2024. *Asia/Pacific Group on Money Laundering's Yearly Typologies Report*. APG, Sydney. **https://apgml.org/sites/default/files/documents//2024_APG_Typologies_Report.pdf**.

BCBS (Basel Committee on Banking Supervision). 2014. *Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism*. Bank for International Settlements, Basel. **https://www.bis.org/bcbs/publ/d505.pdf**.

Egmont Group. 2024. *Best Egmont Cases III: FIU Case Studies 2021–2023*. The Egmont Group of Financial Intelligence Units, Ottawa Available at: **https://egmontgroup.org/wp-content/uploads/2024/09/EGMONT_2021-2023-BECA-III_FINAL.pdf**.

Egmont Group. 2025. *Principles for Information Exchange*. The Egmont Group of Financial Intelligence Units, Ottawa. **https://egmontgroup.org/wp-content/uploads/2022/07/EG-Principles-for-Information-Exchange-Revised-July-2025.pdf**.

ESAAMLG (Eastern and Southern Africa Anti-Money Laundering Group). 2023. *Third Follow-Up Report to Assess the Continued Existence and Impact of De-Risking in the ESAAMLG Region*. ESAAMLG, Dar es Salaam. **https://www.esaamlg.org/reports/ESAAMLG_3rd_De-risking_FUR.pdf**.

Faz, Xavier. 2013. "Mexico's Tiered KYC: Update on Market Response." CGAP Blog, Consultative Group to Assist the Poor, Washington, DC. **https://www.cgap.org/blog/mexicos-tiered-kyc-update-on-market-response**.

FATF (Financial Action Task Force). 2013. *Guidance on Politically Exposed Persons (Recommendations 12 and 22)*. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf.coredownload.pdf**.

FATF (Financial Action Task Force). 2016. Guidance on Correspondent Banking Services. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Correspondent-Banking-Services.pdf.coredownload.pdf**.

FATF (Financial Action Task Force). 2020. *Guidance on Digital Identity*. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf**.

FATF (Financial Action Task Force). 2021a. *Opportunities and Challenges of New Technologies for AML/CFT*. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf**.

FATF (Financial Action Task Force). 2021b. Stocktake on Data Pooling, Collaborative Analytics and Data Protection. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Stocktake-Datapooling-Collaborative-Analytics.pdf**.

FATF (Financial Action Task Force). 2022a. *Procedures for the FATF AML/CFT/CPF Mutual Evaluations, Follow-Up and ICRG*. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/Assessment-Follow-Up-ICRG-Procedures-2022.pdf.coredownload.inline.pdf**.

FATF (Financial Action Task Force). 2022b. *Report on the State of Effectiveness Compliance with FATF Standards*. FATF, Paris. **https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html**.

FATF (Financial Action Task Force). 2023. *Illicit Financial Flows from Cyber-Enabled Fraud*. FATF, Paris. **https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html**.

FATF (Financial Action Task Force). 2024. *FATF Ministerial Declaration 2024*. **FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/FATF/FATF-Ministerial-Declaration-2024.pdf.coredownload.inline.pdf**.

FATF (Financial Action Task Force). 2025a. *FATF Guidance: Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures*. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf**.

FATF (Financial Action Task Force). 2025b. "FATF Updates Standards and Consults on Guidance to Better Promote Financial Inclusion." February 25, 2025. **https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-standards-promote-financial-conclusion-feb-2025.html**.

FATF (Financial Action Task Force). 2025c. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. FATF, Paris. **https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf**.

FATF (Financial Action Task Force). 2025d. *Detecting, Disrupting and Investigating Online Child Sexual Exploitation*. FATF, Paris. **https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html**.

FATF (Financial Action Task Force). 2025e. "FATF Updates Standards on Recommendation 16 on Payment Transparency."

June 2025. **https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html**.

FATF (Financial Action Task Force). 2025f. Explanatory Note for Revised Recommendation 16. FATF, Paris. June 2025. **https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Explanatory%20Note%20for%20Revised%20R.16.pdf.coredownload.pdf**.

FATF (Financial Action Task Force). 2026. "High-Risk and Other Monitored Jurisdictions." February 2026. Accessed April 2026. **https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html**.

Forrester Consulting. 2023. *True Cost Of Financial Crime Compliance Study, 2023: A Forrester Consulting Thought Leadership Paper Commissioned by LexisNexis® Risk Solutions*. LexisNexis Risk Solutions, New York City. **https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-for-the-united-states-and-canada**.

GAFILAT (Financial Action Task Force of Latin America). 2025. *Informe de Tipologías Regionales de LA/FT – 2025*. GAFILAT, Buenos Aires. **https://biblioteca.gafilat.org/wp-content/uploads/2026/02/Informe-de-Tipologias-Regionales-LA-FT-25.pdf**.

Gopalakrishnan, B. 2013. "Project Managing Global Business Transformation Projects: Tips and Tricks." Paper presented at PMI® Global Congress 2013—North America, New Orleans, LA. Project Management Institute, Newtown Square, PA. **https://www.pmi.org/learning/library/managing-global-project-risk-5909**.

HKMA (Hong Kong Monetary Authority). 2023. *AML/CFT RegTech: Network Analytics*. Hong Kong Special Administrative Region of the People's Republic of China. **https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/AML_Regtech-Network_Analytics.pdf**.

IFC (International Finance Corporation). 2019. *Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks – Good Practice Note*. International Finance Corporation, Washington, DC. **https://www.ifc.org/en/insights-reports/2019/aml-cft-risk-management-emerging-market-banks-good-practice-note-062019**.

INTERPOL. 2026. *Global Financial Fraud Threat Assessment 2026*. INTERPOL, Lyon. **https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat**.

Kida, Mizuho, and Simon Paetzold. 2021. "The Impact of Gray-Listing on Capital Flows: An Analysis Using Machine Learning." IMF Working Paper WP/21/153, International Monetary Fund, Washington, DC. **https://www.imf.org/en/publications/wp/issues/2021/05/27/the-impact-of-gray-listing-on-capital-flows-an-analysis-using-machine-learning-50289**.

LexisNexis Risk Solutions. 2022. *Build vs. Buy: The Financial Crime Compliance Platform Study*. LexisNexis Risk Solutions, New York City. **https://risk.lexisnexis.com/insights-resources/research/build-vs-buy-platform-study**

MAS (Monetary Authority of Singapore). 2018. *Guidance for Effective AML/CFT Transaction Monitoring Controls*. Government of Singapore. **https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.pdf**.

NICE Actimize. 2019. "Intelligent Automation for Effective AML: Modernising AML Monitoring Programs to Ensure Compliance with Heightened Regulatory Expectations." White Paper, NICE Actimize, Hoboken. **https://resources.niceactimize.com/wp-content/uploads/2022/11/nice_actimize_intelligent_automation_for_effective_aml_white_paper.pdf**.

Reynolds, Peter. 2023. "How AI is Helping Banks Combat Human Trafficking – and Why It's Just the Beginning." ThetaRay Blog, July 30, 2025. **https://thetaray.com/how-ai-is-helping-banks-combat-human-trafficking-and-why-its-just-the-beginning/**.

Stames, Susan, Michael Kurdyla, Arun Prakash, Ariane Volk, and Shengnan Wang. 2017. *De-Risking and Other Challenges in the Emerging Market Financial Sector: Findings from IFC's Survey on Correspondent Banking*. International Finance Corporation, Washington, DC. **https://documents1.worldbank.org/curated/en/895821510730571841/pdf/121275-WP-IFC-2017-Survey-on-Correspondent-Banking-in-EMs-PUBLIC.pdf**.

The Wolfsberg Group. 2022. *Guidance on Digital Customer Lifecycle Risk Management*. The Wolfsberg Group, Basel. **https://db.wolfsberg-group.org/assets/497de382-1b84-4b6a-aed2-5e627d7c81c9/Wolfsberg%20Guidance%20on%20Digital%20Customer%20Lifecycle%20Management%20(2022).pdf**

The Wolfsberg Group. 2023a. *Wolfsberg Group's Payment Transparency Standards*. The Wolfsberg Group, Basel. **https://db.wolfsberg-group.org/assets/373dbb28-b518-4080-82cc-4be7a54aa16e/Wolfsberg%20Group%20Payment%20Transparency%20Standards%202023.pdf**.

Wolfsberg Group. 2023b. "Publication of the CBDDQ, FCCQ, Guidance, Glossary and FAQs." February 10, 2023. **https://wolfsberg-group.org/news/publication-of-the-cbddq-fccq-guidance-glossary-and-faqs**.

The Wolfsberg Group. 2024. *The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity Part I: Moving Beyond Automated Transaction Monitoring*. The Wolfsberg Group, Basel. **https://db.wolfsberg-group.org/assets/e3d83d2f-fad9-46d2-b5a9-3cf4e932f53f/Wolfsberg%20Group%20MSA%20Statement%20Part%201.pdf**.

The Wolfsberg Group. 2025. *The Wolfsberg Group - Statement on Effective Monitoring for Suspicious Activity Part II: Transitioning to Innovation*. The Wolfsberg Group, Basel. ***https://db.wolfsberg-group.org/assets/298bc488-6e47-465c-8d61-f776aa86594a/Wolfsberg_MSAP2_Transitioning%20to%20Innovation.pdf***.

UNECA (United Nations Economic Commission for Africa). "Digital ID to Unlock Africa's Economic Value If Fully Implemented, Say Experts." UNECA Stories, February 20, 2024. ***https://www.uneca.org/stories/digital-id-to-unlock-africa%E2%80%99s-economic-value-if-fully-implemented%2C-say-experts***.

UNODC (United Nations Office on Drugs and Crime). 2024. World Wildlife Crime Report 2024. UNODC, Vienna. ***https://www.unodc.org/cofrb/uploads/documents/ECOS/World_Wildlife_Crime_Report_2024.pdf***.

World Bank Group. 2015. Fact *Finding Summary from De-Risking Surveys*. World Bank Group, Washington, D.C. ***http://documents.worldbank.org/curated/en/534371468197058296***.

World Bank Group. 2018. *Identification for Development (ID4D) 2018 Annual Report*. World Bank Group, Washington, DC. ***https://documents1.worldbank.org/curated/en/967301587472879585/pdf/Identification-for-Development-ID4D-2018-Annual-Report.pdf***.

World Bank Group. 2019. *Identification for Development (ID4D) 2019 Annual Report.* World Bank Group, Washington, DC. ***https://documents1.worldbank.org/curated/en/566431581578116247/pdf/Identification-for-Development-ID4D-2019-Annual-Report.pdf***.

IFC
International
Finance Corporation
WORLD BANK GROUP