

Building an AI-Ready FCC Program

A Practical Roadmap
for AML Leaders



This eBook explains why financial crime compliance (FCC) leaders must make a concerted effort in 2026 to develop and pursue a strategy for deploying AI agents within their FCC programs. It will detail the typical timeline for planning and deploying AI agents—based on observations and data gleaned from financial institutions representing early adopters (2022-2023), fast followers (2024), and the mainstream (2025 to present).

AI Agents: from reticence to widespread acceptance

The market perception regarding the use of AI in banking and financial services (BFS) has evolved dramatically since 2022, when WorkFusion, a UiPath company first introduced AI agents for financial crime compliance (FCC). Named “Digital Workers” at the time, these AI agents faced an uphill battle in gaining acceptance in FCC operations—not over doubt about the cost and accuracy improvements they could provide, but more for the necessarily cautious nature of compliance leaders when faced with transformational and disruptive technologies.

Fast forward to today, and you would be hard pressed to find executives at major banks, FinTechs, or payment providers who have yet to test or fully adopt at least one AI agent in their AML/BSA compliance operations. The C-suite and Financial Crime Compliance (FCC) leaders recognize that AI and AI agents are here to stay. They also recognize that their leading peers are advancing the use of AI and, even among the most cautious, developing strategies centered around people plus AI and AI agents.

Why AI agent adoption has gone mainstream

FCC leaders know they must arm themselves with AI agents to battle financial crime for four main reasons:

- 1. To manage the ever-increasing alert volumes and costs** to accurately and properly adjudicate alerts in line with evolving regulatory requirements
- 2. To keep pace with competing institutions** that already use AI agents to streamline and improve financial crime compliance
- 3. To thwart criminals and other bad actors** who are using sophisticated AI against financial institutions
- 4. To demonstrate technical advancement** that ensures current and prospective customers that their institution has modernized to reduce risk while speeding and optimizing customer experiences

RAYMOND JAMES



Deutsche Bank 



The urgency to adopt AI agents *NOW*

Notice that the AI agents from WorkFusion are called “AI Agents,” with both words appearing in upper case. When we speak of AI agents generically, the word “agents” begins with a lower case “a.”

Looking across mid-sized and large financial institutions within the WorkFusion customer base, we see that a typical FCC operations team requires six months to develop a robust strategy for incorporating AI Agents into their program. Another three months are needed, on average, to deploy the agents. So, it is imperative to start now to ensure your organization gets up to speed by 2027.

Months 1–6

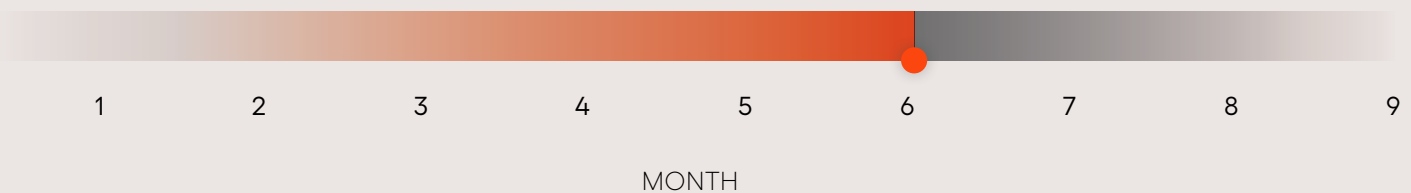
Following are the major elements of 6-month strategy development:

- Strategy definition
- Resource alignment
- Vendor/partner selection
- Proof of concept
- Statement of anticipated benefits

Months 6–9

The next three months represent the deployment stage and include the following actions:

- Ensure all data is complete and ready for AI agent use in full production
- Run trials
- Perform system testing and user acceptance (UA) testing
- Make adjustments
- Advance into full production



Gage your AI agent deployment maturity relative to industry peers

Consider this: If your organization were to start today, you can expect to be up and running with your first effective AI Agent nine months from now. That brings your organization into early 2027. That is 3 years behind early movers, 2 years behind fast followers, and a year behind mainstream financial institutions.

| AI Agent Maturity Stage | Your FCC Program | Early Adopters | Fast Followers | Mainstream Adopters |
|----------------------------------|------------------|----------------|----------------|---------------------|
| Defined AI Agent strategy | No | Completed | Completed | Completed |
| Aligned resources | No | Completed | Completed | Completed |
| Selected vendor/partner | No | Completed | Completed | Completed |
| Completed POC | No | Completed | Completed | Completed |
| Defined benefits from POC | No | Completed | Completed | In Progress |
| Prepared data for production | No | Completed | Completed | In Progress |
| Ran trials | No | Completed | Completed | In Progress |
| Tested systems & user acceptance | No | Completed | Completed | In Progress |
| Optimized with adjustments | No | Completed | Completed | No |
| 1 AI Agent in production | No | Completed | Completed | No |
| 2+ AI Agents adopted | No | In Progress | No | No |

Nevertheless, there is no need to panic. While your organization may have fallen behind, there is good news: WorkFusion has perfected solutions for an AI Agent “quick start” that enable late adopters to ‘check the box faster’ and show progress to both stakeholders and regulators. And there’s more good news for late-adopting organizations detailed on the next page.



The 4 Benefits to Starting Late

1 Today's AI Agents are better

For Financial Crime Compliance teams who have waited until now, there can be benefits to starting late. This is due to AI Agents and AI apps gaining in both sophistication and completeness over the last several years. Today's AI Agents do more than they could in 2023, such as optionally incorporating multiple large language models (LLMs) and offering both semi-autonomous and fully autonomous performance to manage entire processes. As such, they deliver choices to customers as well as proven governance—a matter of critical importance to internal investigators and external regulators.

3 You can speed time to production

Today's typical 9-month timeframe to progress from start to production is much faster than it was two or three years ago. For those early adopters, gaining a full production system typically took 18–24 months. You can expect much faster results at 9 months.

2 You can leapfrog into investigative AI Agents

A company's late start with AI Agents is analogous to the way many Asia-based telecom companies leapfrogged the landline companies of the West when advanced mobile communications rose to the fore. The same is happening with AI agents, with some late-starting FIs potentially leapfrogging others in their AI journey by adopting already-proven AI Agents for screening (i.e. sanctions screening alerts, transaction screening alerts, etc.) and jumping right into investigative AI Agents, such as those performing fraud-related and enhanced due diligence investigations.

4 Regulators are ready to approve your AI Agents

Regulators have made tremendous progress over the last several years in both their understanding and acceptance of AI agents. In 2022 and 2023, FIs had to explain the use of AI Agents and hope that regulators would accept it. Then, in 2024 and 2025, regulators easily accepted the use of AI Agents. Now, in 2026, not only do they accept it, but regulators expect banks to be using AI agents to improve FinCrime compliance operations.

Operating in a leapfrog manner means that your first AI deployment will likely come at a time of elevated expectations for success. After all, nearly every day, banks and other FIs publicly disclose the successes they are enjoying via AI and AI Agents. As a result, your strategy may require you to accelerate progress from initial adoption of a single screening-focused AI Agent to multiple AI Agents taking on more complexity in terms of solutions, systems involved, and processes handled. This means greater care must be taken in planning and thinking through all your system, data, and process ramifications.



Progressing from screening agents to investigative agents

Screening-focused AI Agents deliver, and will continue to deliver, critical operational improvements to FinCrime departments. But now that they have established their value and foothold, FIs are looking to deploy AI Agents that handle investigative processes, such as fraud-related investigations and high-risk reviews.

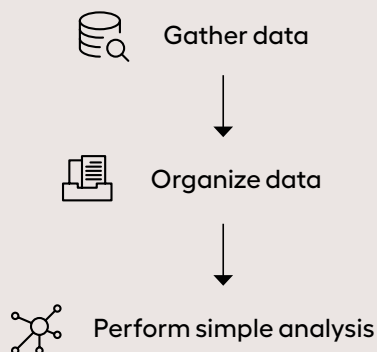
Investigations are required for instances in which an AI Agent cannot readily decide whether an alert represents true risk (a positive result) or a false positive. When an organization faces, for example, a high volume of fraud alerts or transaction monitoring (TM) alerts for things like potential structuring or other methods of obfuscation meant to hide criminal activity, it needs a way to quickly resolve the false positives and investigate the truly fraudulent and/or risky transactions. An AI Agent designed for this type of advanced data collection and analysis is needed.

How investigative agents differ from screening agents.

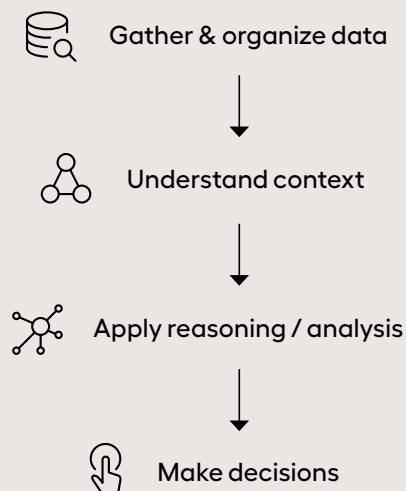
Screening agents gather and organize data, then perform simple analysis of that data. The main value delivered by screening agents arises from greater operational efficiency at the L1 analyst level.

Investigative AI Agents represent a leap forward in agentic AI by understanding data and information in context, then applying analysis and reasoning to that context to create a decision.

Screening AI Agents:



Investigative AI Agents:



Example of screening vs investigative AI Agent

In this example, a bank's transaction monitoring (TM) system has generated an alert because one of the bank's customers, a sneaker manufacturer based in the US state of New Hampshire, has suddenly started sending wire transfers to the Philippines. The TM alert was generated, because the bank designates the Philippines as a high-risk country. For this reason, the TM system wants a review of transactions sent to the Philippines.

Following are explanations of how each AI Agent type would handle the TM alert.

Screening AI Agent

This agent gathers all the available KYC information on the customer business and shares with the human investigator that the customer is a sneaker manufacturer. The agent also gathers 90 days of prior customer transactions so that the human investigator can look at them and begin to build context. Finally, the agent provides public records and adverse media search results.

The public records, in this case, show the owners of the NH business and that they also have personal accounts at the bank. The human analyst can see from the data shared by the screening AI Agent that the owners have been registered in New Hampshire and that there is no adverse media about them or their sneaker business.

Investigative AI Agent

This agent can do everything that the screening AI Agent did, plus the following for this case:

The investigative agent applies one or more LLMs (AI large language models) to the case. As such, it knows how to dig for additional context. In this case, the agent returns with, "We also understand that the counterparty to this wire transfer is 'Company X' in the Philippines." This triggers the agent to automatically perform research on that company, and the agent discovers that the company manufactures shoelaces. The investigative AI Agent reasons that this all makes perfect sense, because it details a scenario of a sneaker manufacturer importing shoelaces. Thus, the agent then makes the decision that the alert is a false positive.

The leap forward provided by the investigative AI Agent comes from providing context, reasoning, and the decisioning. That can only be done automatically by using an LLM. It goes beyond the capabilities of models, rules, and machine learning. At WorkFusion, the investigative AI Agent to handle this entire case, from TM alert receipt to completion, is Isaac for AML Transaction Monitoring.



Investigative AI Agent for EDD

To further your understanding of the power of investigative AI Agents, let's now assume that the sneaker company is considered 'high risk' by the bank, because the company does a lot of international activity. Another investigative AI Agent (named Edward) can apply advanced intelligence and reasoning to enhanced due diligence (EDD) about this customer. Edward would review the sneaker company's account once per year to make sure the company is engaging in proper activities, even if they are complex. For example, they buy product inputs from the Philippines but make payments for shipping to a Cypriot shipping company. AI Agent Edward collects data that shows the company that ships for the sneaker business is registered in Cyprus. Edward looks at all that and puts it into context to reason that nothing nefarious is taking place with the sneaker manufacturer and its dealings with the foreign counterparties.

Investigative AI Agents save their human investigator counterparts 1 to 3 hours, on average, per case investigation. The end result is faster response times to minimize loss potential.

Spotlight on High-Risk Reviews

Banks are compelled to perform high-risk reviews to minimize their risk surrounding numerous potential financial crimes, including money laundering, terrorist financing, fraud, and tax evasion. The types of customers considered to be higher risk include those that show indications of having a PEP status, operate cash-heavy businesses, have complex ownership structures, or operate in high-risk jurisdictions.

The primary goal of performing high-risk reviews is to protect the bank's reputation and to avoid massive fines and stringent remediation measures imposed upon the bank by regulators and government agencies.

But risk reduction is not all investigative AI Agents deliver in the area of high-risk reviews. They also relieve operational stress by lowering manual effort by up to 80 percent and increasing investigator throughput by 300-500 percent.

Impact

~10%

Auto-grouped alerts avoiding duplicate effort

~50%

Auto-closed alerts avoiding analyst touch

1-3

Hours of effort saved per case investigation

Impact

80%

Reduction in Manual Effort

3-5x

Increase in investigator throughput

10+

External and Internal systems and sources automated



Now is the time, but exercise caution

A growing number of solution vendors are attempting to 'ride the wave' of popularity of AI Agents for FinCrime compliance. Your challenge is to determine which solutions are proven in the field among your FCC peers. As you evaluate solutions, consider these critical factors:

- Is the potential solution referenceable within banks of your size?
- Is success actually realized and the solution road-tested at your expected volume scenarios?
- Have the vendors' customers passed through auditor and/or regulatory review while using the solution?

To learn more about WorkFusion's AI Agents for screening and investigations, schedule a demonstration today.





WorkFusion was acquired by UiPath in 2026. WorkFusion, a UiPath Company, is a pioneer in AI agents for financial crime compliance. Its AI agents are purpose-built workers that augment financial crime compliance operations (FCC) teams in Level 1 and 2 analyst/investigator functions for anti-money laundering (AML), adverse media monitoring, sanctions screening alert review, Know Your Customer (KYC), and transaction monitoring and fraud investigations. Its AI solutions are used by top banks and leading financial institutions around the globe to mitigate risk, solve talent challenges, increase workforce capacity, reduce costs, enhance employee and customer experience, and improve compliance posture.

workfusion.com

© UiPath. All rights reserved.