NAPIER

FINTRAIL

The optimal path to AI implementation for financial crime compliance

The applications of artificial intelligence for financial crime compliance are game-changing and can facilitate unparalleled operational efficiencies and transform your organisation's compliance function.

This 12-step path guides you through our experts' recommended process for AI implementation, addresses some of the most common pitfalls and challenges financial institutions face in this journey, and assesses the current regulatory landscape around the use of AI.

I'm James Nurse and I'm the Managing Director at FINTRAIL, a consultancy business that specialises in anti-financial crime support. I'm delighted to have Dr. Janet Bastiman join me as my partner in FinCrime on this journey.

JAMES

I'm Janet Bastiman and I'm the Chief Data Scientist at Napier, a new breed of specialist financial crime compliance tech providers. We work with some of the world's leading financial institutions to transform compliance from legal obligations to competitive edge, and a significant part of how we achieve this is with AI.

JANET

WHY AI?

There are many reasons your organisation may have decided that AI will solve all your problems:

- ✓ Desire for automation and digitalisation
- ✓ For business and cost efficiency
- ✓ To keep up with rapid increases in regulations
- ✓ Senior leadership don't want to risk fines or reputational damage from not detecting criminal activity

There's huge pressure on financial crime teams to ensure they do a diligent and thorough job.

If you're considering AI, it is likely because you are aware that your processes may not be up to scratch and may have limitations either in the processes themselves or the tools you have in place.

JANET

THE COMMON USE CASE FOR AI IMPLEMENTATION

Your company has had a conversation internally and decided to adopt AI into a wider AML framework, or perhaps into one particular function such as transaction monitoring.

There initially appear to be three phases in the process of AI implementation:

1. You decide that adopting AI resolves all your transaction monitoring needs
2. You skip straight to implementation
3. Then you go live

It sounds simple, but there are more steps needed to ensure a successful outcome.

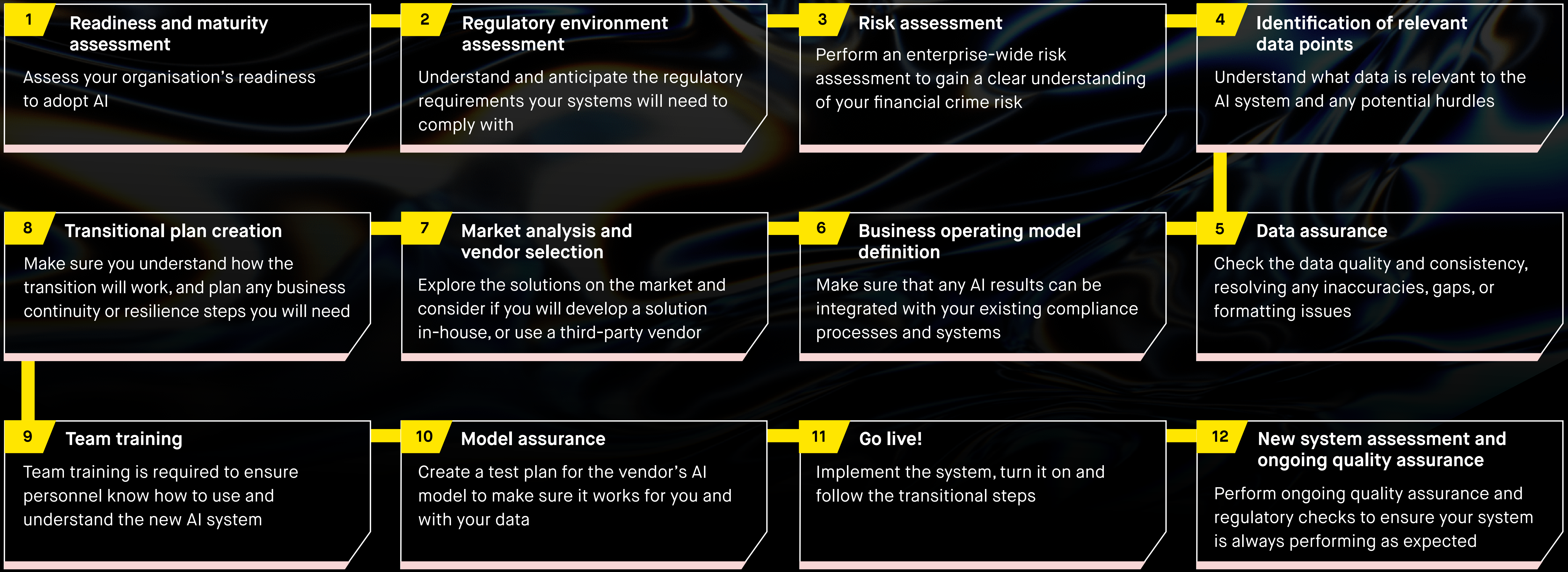
In this guide, we are going to take you through those steps that we believe will get you from ideation to successful implementation.

JAMES

AI is growing in popularity in the AML space and is increasingly highlighted by regulatory bodies (like MAS) as a useful tool to improve compliance functions – but it's not a one-size-fits-all solution or a silver bullet, and if implemented incorrectly you're unlikely to get the most out of it.

JANET

THE 12-STEP PLAN



1 Readiness and maturity assessment

Assess your organisation’s readiness to adopt AI

2 Regulatory environment assessment

Understand and anticipate the regulatory requirements your systems will need to comply with

3 Risk assessment

Perform an enterprise-wide risk assessment to gain a clear understanding of your financial crime risk

4 Identification of relevant data points

Understand what data is relevant to the AI system and any potential hurdles

5 Data assurance

Check the data quality and consistency, resolving any inaccuracies, gaps, or formatting issues

6 Business operating model definition

Make sure that any AI results can be integrated with your existing compliance processes and systems

7 Market analysis and vendor selection

Explore the solutions on the market and consider if you will develop a solution in-house, or use a third-party vendor

8 Transitional plan creation

Make sure you understand how the transition will work, and plan any business continuity or resilience steps you will need

9 Team training

Team training is required to ensure personnel know how to use and understand the new AI system

10 Model assurance

Create a test plan for the vendor’s AI model to make sure it works for you and with your data

11 Go live!

Implement the system, turn it on and follow the transitional steps

12 New system assessment and ongoing quality assurance

Perform ongoing quality assurance and regulatory checks to ensure your system is always performing as expected

STEP 1 Readiness and maturity assessment

Before embarking on your AI journey, you must first establish if your organisation is mature enough to adopt the technology. Conducting a maturity assessment as the first stage of the process reduces the risk of wasting resources on an unfeasible implementation project at a later stage.

A comprehensive maturity assessment involves evaluating your business, namely its people, data, and processes. This will allow stakeholders to identify strengths and areas for improvement, and accordingly prioritise what needs to be done to reach AI 'readiness'.

Data maturity is the most important factor to evaluate when adopting AI solutions.

Ensuring that your organisation holds enough historical data of sufficient quality for an AI model to draw upon is key to generating meaningful results.

When detecting customer-specific anomalies or changes in customer behaviours (as transaction monitoring and other AML solutions do) having the correct volume and quality of historical data is essential.

AI solutions will flag behaviours that are unusual compared to the data used to create the model, so without mature historical data, the system is unlikely to gain an accurate picture of customer behaviour and will produce more false positives, adding to, rather than reducing the 'noise'.

TOP TIP

Your firm should aim to have historical data spanning double the recommended 'minimum' period required to successfully run an AI solution.

STEP 2 Regulatory environment assessment

Depending on where your organisation and its subsidiaries reside and the type of business you are involved in, there are rules in place to ensure your systems are compliant. These rules are particularly important when it comes to informing the use of AI.

Naturally, considerations need to be made for data protection, such as the EU's General Data Protection Regulation (GDPR). Any process designed to process personal data is subject to the GDPR regime, specifically Article 5(1)a) which requires that data controllers constantly reassess the likely impact of their use of AI on individuals to ensure it does not produce biased outputs.

Also relevant to member states of the EU is the proposed AI act, which is concerned with the risk and explainability of AI systems, and prohibits the use of AI in ways that contradict EU values.

There also exist some specific regulations to govern the use of automated decision making. While several key jurisdictions have discussed the use of AI in the financial sector, only the EU and the UK have issued guidelines so far, and the EU is alone in having introduced any legislation or regulatory measures.

Other regulations globally are maturing that require AI decision outputs to be explainable by humans. For example, in Germany, BaFin expects firms to maintain human involvement in the interpretation and use of AI outputs to promote accountability, provide legal safeguards, or perform quality control.

If your organisation decides to extend coverage beyond traditional transaction monitoring models to include AI analytics, there are considerations to be made in order to meet regulatory requirements and to mitigate the risks of adverse consequences from decisions based on incorrect or misused models.

MRM REGULATION IN EUROPE

The Targeted Review of Internal Models (TRIM) missions conducted by the European Central Bank requires banks to be able to identify, understand and manage model risk. Banks should have a model risk governance framework in place, consisting of a range of components (e.g. model governance, risk control function, validation function, and internal audit).

For example, TRIM requires there to be an independent validation function within the organisation, responsible for approving the quality of the data used in the model, the model methodology, and related processes, policies, and documentation. All internal models that involve risk should be subject to a thorough annual internal validation.

STEP 3 Risk assessment

1 2 3 4 5 6 7 8 9 10

The next stage should be to conduct an enterprise-wide financial crime risk assessment in line with your financial crime risk policy.

This assessment will provide an overview of the key financial crime risks to which your organisation is exposed, including information about emerging threats and any changes to the firm's financial crime risk appetite. It will also inform you of the types of data required to manage those risks and any control procedures that you might consider to mitigate them.

Conducting a risk assessment at this stage will also inform your subsequent vendor selection process.

By obtaining a thorough understanding of your company's financial crime threat landscape, you will be better informed of the issues you face from a risk perspective and which of those an AI solution could solve.

STEP 4 Identification of relevant data points

1 2 3 4 5 6 7 8 9 10

Successful AI implementation requires managers to adopt an intelligent and networked approach towards financial crime that puts data analytics at its core. The risk assessment from the previous step should inform you of the data types required to manage the primary risks, so the next stage in the process is to locate and aggregate this data to train the AI model.

Not every firm is inherently well placed to collate customer and transaction data - not to mention data from external sources - necessary to generate a holistic picture of customer behaviour.

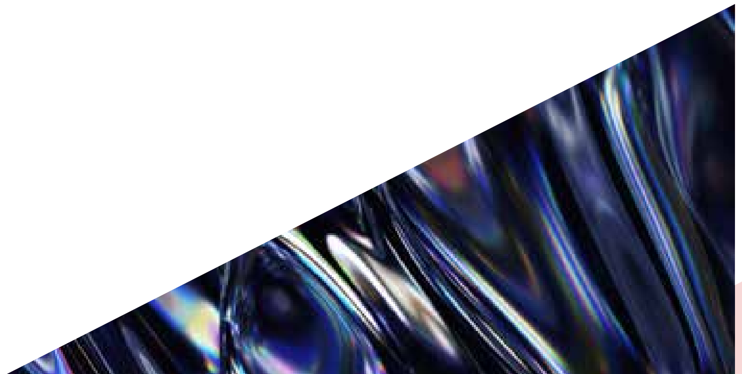
For many financial organisations, data sources are spread across the business and may be owned by teams in different divisions or geographies, or stored on different systems, causing data silos. This data can be difficult to access, particularly if the firm is burdened with inflexible legacy technology.

Data protection and data security considerations are also needed to prevent the exposure of sensitive customer data, potentially creating barriers to internal and cross-border data sharing.

You may also find that the data available to you doesn't sufficiently illuminate the behaviours you identified in your risk analysis. If this is the case, a degree of investigation is required to understand where gaps in data exist and where you can source additional information.

TOP TIP

Whether you are using an AI-driven solution or a rules-based system, always ensure you understand what the priority data points are, i.e. those that are required to fundamentally drive useful results. For example, priority data for a transaction monitoring system includes historical data on the frequency, volume, currency, and direction of customers' transactions.



STEP 5 Data assurance

Once you have identified the necessary data, the next steps are to validate it and provide assurance that this data is trustworthy and usable. Data quality and consistency must be assessed to iron out any formatting errors and fill any gaps.

Data may be stored in different formats depending on how it was collected, so cross-referencing this information to make sure it can be merged is vital. For example, restricted drop-down data fields maintain a certain pre-programmed format but may not encapsulate the nuances of the data, whereas free text inputs are subject to human error and formatting challenges which cannot be used directly into an AI model, and automated processing may introduce further issues.

Know Your Customer (KYC) data is particularly difficult to map as it is often managed externally in company registries, by regulators, or by suppliers of important information like PEPs or sanctions data.

It is also important to check the auditability of the data, which involves assessing whether the data is fit for a given purpose.

It is critical at this stage of the implementation process to ascertain:

- ✓ If your data sources are valid and reliable
- ✓ If the data has already been processed in a way that could remove information
- ✓ How old the data is
- ✓ If the data needs to be refreshed

If the quality of the data feeding the AI is poor, it is unrealistic to expect meaningful and reliable results.

DATA ASSURANCE CHECKLIST

☑ **Relevancy**
The data should meet the requirements for intended use.

☑ **Accuracy**
Regardless of the area of risk and the data which is required to mitigate it, data accuracy is key.

☑ **Completeness**
The data should not have missing values.

☑ **Recency**
The data should be up to date, as data that is very old may no longer be relevant and could require a refresh, requiring input from wider team members or customers.

☑ **Consistency**
Eradicating any formatting inconsistencies is vital for the AI system to accurately interpret the inputs.

STEP 6 Business operating model definition

The next stage is to define the objective of implementing AI within the broader financial crime compliance and business operating model, to ensure that the AI results have relevance and can feasibly be integrated into existing processes.

It is important to consider the following:

- ✓ What information do financial crime teams need to mitigate risk and improve the effectiveness of the compliance programme?
- ✓ How will the AI system work with your "three lines of defence" business model?
- ✓ Where should responsibility for designing, implementing and assuring your AI model sit?

Each line of defence requires different outputs from a solution. For example, some teams will show more interest in reporting functionality, whereas others may require controls that help them to identify, assess and control the financial crime risks to the business. Not every solution will have functionality for each of these use cases.

These considerations should be used to define requirements for vendors before you go to market. Having a thorough understanding of the functionality required to fit within your operating model will narrow the list of potential AI vendors.

Ultimately, the product needs to enhance the effectiveness of the anti-financial crime function, so capturing the different teams' requirements in the broader operating model is key.

THREE LINES OF DEFENCE OPERATING MODEL

First LOD - risk owners, responsible for daily risk management and implementing corrective actions to address process or control weaknesses.

Second LOD - risk oversight and compliance functions. Ongoing monitoring of the fulfilment of AML/CFT duties by the bank.

Third LOD - internal audit. Independently evaluating the risk management and controls. Focused on policies, procedures, staff, training, quality control.

STEP 7 Market analysis and vendor selection

It is now time to think about solutions. Up until this point, you:

- ✓ Have established that your organisation is mature enough to adopt AI
- ✓ Have identified the risks you would like to manage
- ✓ Know the regulations with which you must comply
- ✓ Have reviewed your operational processes
- ✓ Have gathered the necessary data to begin AI implementation

Now, conducting market analysis involves assessing the RegTech ecosystem to identify the types of solutions that are available to you.

The first important decision to make during this stage is whether you have the existing capability, or can hire a team, to build an AI solution in-house or if a vendor, or combination of vendors, can meet your business needs.

Developing an AI solution in-house may offer benefits such as flexibility and customisation. However, this route is likely to require significantly more time and resources than a third party integration.

Finding a solution that meets your needs can feel overwhelming, particularly as differences between AI vendors are highly technical and nuanced. It's therefore vital that you understand the resources that can help in this process:

- ✓ **Make use of publicly available databases:** technology product comparison websites offer an easily searchable database of RegTech products. Sites such as these enable you to group vendors by category, risk type or technology feature, helping you to narrow down the list of software vendors quickly to those most relevant to your organisation's needs.
- ✓ **Listen to the experts:** finding a suitable partner in your AI implementation journey can be extremely beneficial. This might involve simply speaking with industry experts to help locate and assess suitable technology candidates. A more hands-on approach might involve using an implementation partner to guide you through the remaining steps in the process.

STEP 8 Transitional plan creation

Regardless of whether you are developing an AI system in-house or using a third party vendor, you must carefully consider how you will migrate from your incumbent systems to the new software. The goal is to achieve a smooth system transition, to make the new technology – the AI – available to the relevant teams as quickly as possible. You should aim to do this with the least operational disruption, at the lowest cost, and with the least amount of internal and regulatory risk incurred.

There are three main approaches to technology transition:

1 Phased implementation

In a phased system changeover, technology transition takes place incrementally. Parts of the new system are activated one at a time to allow users to get used to new processes and identify any problems before the next area is implemented. If any issues arise then they are likely to be limited in scope and any lessons learned from each phase will make each subsequent stage more efficient and reliable than the last.

2 Parallel running

This approach involves running both the new and old systems simultaneously using live data to compare the results. Once users are satisfied, the old system is taken offline, leaving the new software running. This transitional approach reduces changeover risk as, should the new system encounter obstacles, then the incumbent technology is still performing the required function, avoiding disruption to your business or compliance.

3 Direct changeover

This refers to a single fixed point where one system is switched off and the new software takes over. This is the cheapest, quickest, and simplest method of technology transition, but it carries considerable risk. If the new system needs further adjustment, the whole organisation may suffer and there may be a gap where you are not technically compliant.

TOP TIP

Your technology transition plan should include an effective IT contingency plan that includes policies, procedures, and technical measures that enable the recovery of technology operations in the event of an unexpected incident.

STEP 9 Team training

AI implementation helps streamline and optimise processes in financial crime risk management. By using machine learning models and natural language processing, much of the structured and unstructured data analysis can be automated, which inevitably causes a shift in employee roles and processes.

For example, analysing unstructured data for transaction monitoring, PEP screening, or sanctions screening is often done manually but is a process well-suited to automation.

New procedures and workflows are therefore required to facilitate this transition to automation, and employees need to be trained on new data inputs and outputs, as well as new role responsibilities.

It is not only important to train the team on the processes around AI, but also to train the AI algorithms themselves. We touched upon AI explainability in the regulatory assessment step, but it is particularly pertinent here for two reasons:

1 Regulatory compliance

Several regulators such as BaFin place the responsibility on institutions to assure the explainability and traceability of AI-based decisions. Other regulators such as the UK's Information Commission (ICO), European Banking Authority (EBA) and the Monetary Authority of Singapore (MAS) emphasise the importance of analysts understanding why a particular conclusion was reached by the AI algorithm to protect users from potential adverse outcomes caused by biased AI.

2 System usability

For financial crime compliance teams to make informed decisions based on AI-generated recommendations, they need to properly understand the outputs and the methodology followed to reach them. Ensuring the team can explain the AI and its outputs also encourages wider confidence within a company through knowledge diffusion.

TIPS FOR EMPLOYEE TRAINING

Use subject matter experts
Trainers need to know the system well, so, if possible, use internal or external experts to develop the technical training (many third party vendors will offer training with their solution).

Make training a priority
Allocate sufficient time and resources to ensure training is comprehensive and well-received to improve employee buy-in and confidence in the new system.

Set clear and realistic deadlines
Provide advanced notice of training deadlines to demonstrate consideration for employee workloads.

Use incentives where necessary
Deploy a combination of rewards to encourage employee engagement.

STEP 10 Model assurance

Before you go live with your new AI-powered solution, you must perform rigorous testing of the AI model and wider system to ensure that it functions effectively and is producing the expected results. Technology vendors provide a range of performance and data science metrics to help with testing such as accuracy, precision, recall, and deviation from the truth.

You will also need to ensure the model is interacting as expected with your data. For instance, before going live with a transaction monitoring solution you should always run testing on sample data to observe the AI outputs. Questions to be answered include:

- ✓ Is the system identifying deviances in behaviour patterns?
- ✓ Is it reporting suspicious transactions correctly, and are those reports being flagged to the correct person?
- ✓ Is it populating suspicious activity reports with the correct inputs?

DATA SCIENCE METRICS

Bias

Within Data Science, bias refers specifically to unwarranted correlations between the input data and the output, this is not the same as bias inherently in the data or bias from human interpretation, neither of which can be tested directly with the data you provide.

Recall

The ability of an AI model to find *all* of the relevant cases within a data set. This is measured by dividing the number of true positives by the number of true positives plus the number of false negatives.

Precision

The ability of an AI model to identify *only* the relevant data points. This is measured by dividing the number of true positives by the number of true positives plus the number of false positives.

Accuracy

The ability of the AI model to get the relevant data points, which is measured by combining the number of true positives and true negatives by the whole data population. Some people incorrectly use recall or precision as the quoted accuracy measure.

RMSE

The root mean squared error is used for time series prediction and is a measure of the difference of the prediction from the observed behaviour.

STEP 11 GO LIVE!

Once you are satisfied that your AI model outputs meet requirements from a regulatory and a financial crime risk appetite standpoint, it's time to go live!

"Going live" is the point at which the code and data analysis moves from a test environment to the live environment, which means that the system becomes officially available to your applicable users who can now perform their functions using the new software.

Weeks, if not months, of preparation have got you to this point, so it's important to have a plan in place to encourage an efficient transition. It is reasonable to expect some growing pains as the team become accustomed to using the new AI system to monitor real customer behaviour.

If you are using a third party vendor, ensure that you have agreed an appropriate level of ongoing support over the transition period. As we've previously mentioned, it may be worth finding an implementation partner to facilitate this process.

In any scenario, a 'go-live' checklist is a critical resource that can often be overlooked. While your vendor should have their own cutover checklist, it may not contain every necessary step to migrate your internal processes, so each organisation should aim to create their own customised checklist.

GO-LIVE CHECKLIST ESSENTIALS

☑ **Operational aids** to support employees with logging in to and navigating the new system.

☑ **Deadlines:** it is important to have a cut-off date for any data or implementation changes prior to going live. Stop dates for the old system that show when the new one comes online are also important, this could be one fixed date or series of dates depending on your transition strategy.

☑ **A timeline** of all tasks, such as data integrations, migration, and testing.

☑ In some cases, it is appropriate to **notify customers and vendors** about the system update, to outline if and how it will affect their interactions with your business.

STEP 12 New system assessment and ongoing quality assurance

Crucially, going live does not mark the end of your AI implementation journey.

Once your system is up and running, you must define and conduct ongoing quality assurance processes. The pace of regulatory change is only increasing, and you need to ensure that your AI solution and its outputs are not only accurate, but that they are sufficient to safeguard your organisation against the risk of breaching regulations.

The financial crime landscape is also continuously evolving, particularly in the wake of the COVID-19 pandemic. As we push forward into this new age of digital sophistication, criminals are constantly evolving and adopting new innovative tactics to bypass financial crime defences.

One key takeaway from this suggested approach is the importance of data. The effectiveness of AI-powered financial crime systems is entirely dependent on having good quality data in sufficient volumes and in the correct formats.

AML - An example of regulatory change

The EU Anti Money Laundering Directives (AMLDs) are issued periodically by the European Parliament to be implemented by its member states as part of domestic legislation. Since 2015, the AMLDs have been updated six times, providing new additions and updates to regulatory obligations for member states, the most recent being 6AMLD in December 2020.

Summary

When implementing AI into your organisation's AML function, it's important not to rush the process or sacrifice crucial steps in the pursuit of a speedy transition.

Although 12 stages may seem extensive, each serves a valuable purpose and informs subsequent stages. Following our suggested path can save you time, conserve resources, and deliver better outcomes by reducing internal and external risk. Adopting a detail-oriented approach to AI implementation will lead to a more sustainable and reliable solution in the long run.

One key takeaway from this suggested approach is the importance of data. The effectiveness of AI-powered financial crime systems is entirely dependent on having good quality data in sufficient volumes and in the correct formats.

You can approach AI implementation with the best intent, performing thorough risk assessments and regulatory checks, but your own data is what will ultimately make or break the project.

Therefore, it is imperative that you invest time and effort into the maturity assessment and data aggregation and assurance stages, using all available internal resources and liaising with relevant teams and data experts.

Finally, remember that going live does not mark the end of your AI transformation: ongoing quality assurance and regulatory monitoring are vital to maintaining the efficiency and effectiveness of your new solution.

Implementing AI software is an opportunity to partner with a technology vendor to find or create a product that fits your needs long term. Technology capabilities are not static, so it is important to provide your supplier with regular feedback to help shape and influence model enhancements moving forward. By doing so, your vendors are better able to scale the solution in line with your organisation's requirements and manage your evolving regulatory obligations.

About the authors

Janet Bastiman
Chief Data Scientist @ Napier

With over 20 years of experience, Janet has pushed the boundaries of data science in telecommunications, marketing and the financial sector, working with start-ups and established businesses to implement and improve their AI offering.

James Nurse
Managing Director Europe @ FINTRAIL

James has spent the last 10 years working in the regulated financial sector. Having held first and second line AFC roles in the gambling, challenger bank and money transfer space, James brings a wealth of experience from the fast-moving Fintech space.

About Napier

Napier is a London-based financial crime compliance technology company founded in 2015 with global offices in all the key financial hubs.

Trusted by the world's leading financial institutions, our next generation intelligent compliance platform is transforming AML and trade compliance.

We design and build compliance technology to help companies in any sector comply with AML regulations, detect suspicious transactions, screen potential customer and business partners, and help analysts predict customer behaviour.

Napier uses industry knowledge and cutting-edge technologies such as artificial intelligence and machine learning to help businesses detect suspicious behaviours and fight financial crime.

napier.ai

About FINTRAIL

FINTRAIL is a global consultancy here to help companies manage their exposure to financial crime risk and maintain regulatory compliance.

We've worked with FinTechs, RegTechs, traditional banks and other financial institutions, startups, venture capital firms and government bodies to implement industry-leading approaches to combat money laundering and other financial crimes.

Our team is deeply experienced in developing and deploying effective, innovative and inclusive risk management controls.

fintrail.com

Discover next-generation financial crime compliance technology

To find out how Napier's AI-powered platform can transform your financial crime compliance processes, visit www.napier.ai

Get in touch

Book a demo