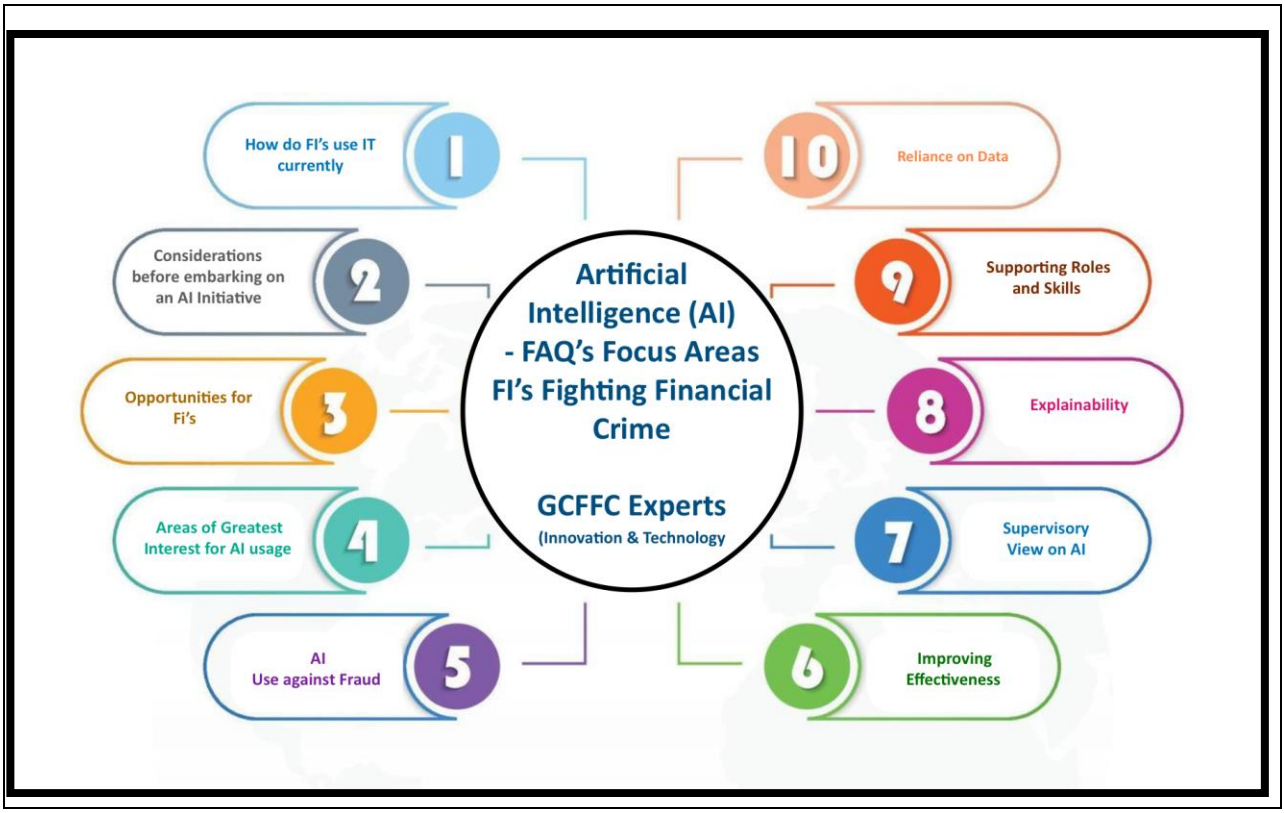
Frequently Asked Questions on the use of AI as a tool to accelerate effectiveness in fighting financial crime in the private sector for Financial Institutions

Introduction

The Global Coalition to Fight Financial Crime[1] established a Technology and Innovation Experts Working Group in 2022[2], inviting leading experts and practitioners to consider amongst other things, "*the use of Artificial Intelligence*[3] *(AI) as a tool to accelerate effectiveness in fighting financial crime*". In this paper the experts group have focussed on Financial Institutions and have formulated and answered 10 important questions (FAQ's) which reveal the state of thinking which should overall encourage further support in the years to come.



[1] See: https://www.gcffc.org

[2] See: https://www.gcffc.org/the-global-coalition-to-fight-financial-crime-announces-a-new-experts-working-group-focused-on-technology/. In particular the main contributors included: The GCFFC wishes to thank all the experts, with particular thanks to Laura Hutton and Felix Hoddinott Quantexa, Dan Margetts & Joceyln Norval ING, Wolgang Berner & Felix Berkham Hawk AI, Phale McMillan, NatWest & Karim Rajwani – Advisor. Special thanks also goes to the Co Chairs of the Experts Working Group David Wilson of LSEG & Markus Schulz of ING.

[3] See: Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, particularly computer systems. It involves creating systems that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, language translation, problem-solving, and learning from experience. AI systems aim to imitate and replicate human cognitive functions, enabling them to analyse and interpret data, make informed decisions, and adapt to different situations. Key characteristics of various artificial intelligence systems include:1) **Learning:** AI systems which can learn from data and improve their performance over time. Machine learning and deep learning are subfields of AI that focus on developing algorithms that can automatically learn and improve from experience.2) **Reasoning:** AI systems which can use logical rules and reasoning to make decisions and draw conclusions based on available information. 3) **Problem-Solving:** AI systems which can analyse complex problems, break them down into smaller components, and find solutions through various algorithms and heuristics. 4) **Perception:** AI systems which can interpret and understand data from the environment, such as visual input from cameras, audio input from microphones, and text input from documents. 5) **Natural Language Processing (NLP):** AI systems which can understand, generate, and interact with human language. This includes tasks like language translation, sentiment analysis, and chatbot interactions. 6) **Adaptation:** AI systems which can adapt to new situations and changing environments. They can adjust their behaviour based on new data and experiences. 7) **Autonomy:** Some advanced AI systems can operate autonomously, making decisions and performing tasks without human intervention.

The opportunity to use AI to fight financial crime including money laundering is potentially far reaching. We are already seeing successfully deployed use cases and expect to see more as the opportunities become available to more and the challenges inherent in this area are addressed. The use of AI in fighting financial crime including money laundering, will benefit from a broader acceptance and use of AI in other areas, where public and private sector leaders see significant benefits and introduce other successful programs, such that the anti financial crime space is not an outlier.

Whilst we are convinced that AI will play a major role in the future, fighting financial crime, including across the money laundering landscape, questions around success will lie just as much in the partnerships that are formed, data pools that can be accessed, the selection of AI types used, the activity being transformed, the implementation of the solution and the feedback and control environments put in place to track progress and minimise bias and unintended consequences.

Question 1: How do FI's use technology today in fighting Financial Crime?

Most Financial Institutions utilise machine learning and are starting to develop generative AI solutions to materially enhance detection and disruption capability, with a programme of key and additional controls to mitigate the risks that come from being exposed to financial crime related risks. These include as a minimum controls designed to mitigate regulatory risks by ensuring compliance with both regulatory requirements and evolving regulatory expectations. Many Financial Institutions also go further and seek to mitigate the actual financial crime risks, beyond those that generate regulatory risks, which can also include reputation risks. Mitigating these risks is achieved largely through high volume repetitive tasks, carrying out customer identification and due diligence and monitoring customer behaviour and transactions to prevent and detect unusual, or potentially suspicious activity. "Preventative" and "Detective" controls are mostly automated through the use of technology, as the numbers of customers and transactions undertaken through many FI's far exceeds the capability for manual controls. Increasingly the escalation of events detected by automated controls also exceed manual capabilities and technology is deployed to triage these events before escalation for manual investigation. Technology is also used to adapt targeted rule sets to enable a more proportionate calibration of resources towards higher risk activity.

"Technology has therefore been used to date to essentially manage the volume of activity and to ensure consistency of approach, which is also fully auditable and reliable. It relies on human programming which in turn generates predictable results. Artificial Intelligence takes the benefits from technology to a new level".

Technology has therefore been used to date to essentially manage the volume of activity and to ensure consistency of approach, which is also fully auditable and reliable. It relies on human programming which in turn generates predictable results. Artificial Intelligence takes the benefits from technology to a new level. Whilst it relies on human programming initially, including being programmed to self learn, it's ability to self learn means that whilst it still carries out human instruction it has the potential to produce more than just pure predictable results. With enormous levels of computing power available and huge amounts of data to process and to learn from, technology that can teach itself to effectively be "smarter", and can do what individual humans can't at least at these scales, presents a compelling proposition for adoption, provided it is well managed.

Question 2: Considerations before embarking on an AI initiative?

For Financial Institutions, the motivation for considering embarking on an AI initiative will vary, including seeking improvements in effectiveness and/or efficiency and/or sustainability. Whilst a business case will need to be made, partners identified and the project managed well, their are additional considerations that come with this being an AI initiative that requires a level of sophistication and resource that many will find challenging, both in delivering the initiative and maintaining it. Even where a Financial Institution is confident in it's own ability to so deliver and maintain, those that audit and regulate the financial institution may be less able and as a result less supportive. For some future industry platforms or utilities may offer a short cut to accessing AI successfully, socialising the benefits and managing the risks, in ways individual financial institutions, or countries are unable.

A fundamental question to ask before embarking on transformational technological change is whether the existing, to be transformed activity ought, is one that is to be improved, rather than instead retired, adjusted, or replaced with an alternative process that better achieves the desired outcome. An example of such thinking came from Henry Ford the US Automaker, who was asked what people wanted, when he embarked on making affordable automobiles and he responded, the people thought they wanted faster horses. For Financial Institutions, their is flexibility to adapt, though their are also limitations due to regulatory requirements and expectations.

Also an FI should examine its readiness in terms of intellectual capability to design; and manage AI solutions, underlying data quality it will be built around, whether their is an ethics framework in which to assess use case necessity, and the capacity to adequately design and resource effective oversight through quality assurance of outcomes and establishing model feedback loops.

Embarking on an AI initiative at this time may not be for everyone. It's not about the size of the FI as many fintechs have advantages over many large incumbents in this respect. It's mostly about the technical sophistication and understanding of the FI. For some FI's, it may make sense to wait and continue to focus on ensuring controls effectiveness with existing tools.

Question 3: Opportunities for Financial Institutions:

Financial Institutions have been deputised to stand on the front line in combatting money laundering helping law enforcement fight financial crime, as well as combatting terrorism finance, proliferation finance, fighting fraud and compliance with financial, economic and trade sanctions. These many activities whilst distinct often coalesce into control programmes that have many uses and in aggregate mitigate many of these risks. Whilst the threats vary by financial institution: by customer, geography, product, service and channel usage, the key controls don't and remain the focus of collective risk mitigation, with key controls for customer identification, due diligence, name screening, transaction (sanction) screening, transaction monitoring, investigation and reporting.

As requirements and expectations on Financial Institutions have grown, so have teams of financial crime fighters, such that the total number of financial crime fighters in a large global financial institution outnumber, according to the Egmont Group, the aggregate number of staff employed in all 40 FATF Member Financial Intelligence Units.

These armies of financial crime fighters, whilst in most cases highly motivated, perform often repetitive tasks, are less than expert or lack significant experience, and as a result, additional more expert support and quality

controls are required to be performed to maintain standards. Technology and business process re engineering have long been compelling answers to improve effectiveness, efficiency and sustainability in this situation, but replacing human judgement so far has been at the boundary of how far this approach has dared to go. With Artificial Intelligence, automating human judgement is also now in scope, and with the ability to learn, more difficult judgements will come into scope in the future.

"Armies of financial crime fighters, often perform repetitive tasks, and they have to be supported by additional more expert support and quality controls to maintain standards. Whilst IT & BPR have been the answer to improving effectiveness, efficiency and sustainability they haven't been able to substitute for human judgement, but with Artificial Intelligence, automating human judgement is also now in scope, and with the ability to learn, more difficult judgements will come into scope in the future".

Question 4: Areas of greatest Interest to deploy AI Technology?

Whilst technology and business process re engineering has delivered improvements for Financial Institutions (effectiveness, efficiency and sustainability), AI offers the prospect of additional improvements, including for example 3 generic improvement types:

- Making mass data collection and relevance of data collected for use in key processes such as customer identification and due diligence, initial and periodic reviews smarter. Introducing AI into this activity reduces false positives and can highlight likely true positives to focus attention and support better and more successful investigations.

- Replacing so called level 1 manual investigations of customers, transactions, payments etc, where human judgement and parameters for decision making is already limited and prescribed and can be replicated with AI technology that is likely to be able to outperform existing level 1 analysts, resulting in significant cost savings and providing additional levels of consistency, accountability and sustainability.

- Identifying new likely insights or true positives and suppressing known likely duplicates or false positives, which would otherwise respectively remain hidden or would dominate and in so doing generate increased levels of effectiveness and reduce inefficiencies. AI technology is likely able to self learn quickly from the many experiences of what true and false positives look like and react to both these and small variations or adaptations quicker than traditional technology solutions.

"AI offers the prospect of significant additional improvements, including for example. 3 generic improvement types: 1) Mass data collection and relevance of data collected for use; 2) Replacing so called level 1 manual investigations; & 3) identifying new likely insights or true positives and suppressing known likely duplicates or false positives, non more than in Anti Fraud programmes".

Nevertheless, the promise of AI technology to deliver improvements is always dependent upon:

- data quality (the accuracy of the data itself) and data lineage (the accuracy of the source of the data)
- sufficiency of data, so that the AI technology can rely on enough data to make informed judgements
- programming capability, backed by expertise informed by evidence, credibly sourced and validated.
- specificity, such that strong evidence is not extended beyond it's natural base to other areas, or geographies where evidence is weak.

Positive results impacting these processes have a significant additional benefit beyond fighting financial crime. These include faster onboarding times, reduced friction, financial inclusion and improved overall customer experiences. As part of any business case, which will inevitably include the "cost of compliance", it should also include these elements, where competition in the market is still and something that resonates strongly in the "C Suite" and at "Board" level.

Question 5) Why is AI is already proving itself likely in combatting Fraud?

With fraud and scams at record highs and criminals using increasingly sophisticated methods, financial institutions are themselves turning towards sophisticated tools to prevent financial crime. The volume of attempted fraud means that firms are faced with a significant volume of data too large for individual human intervention or immediate analysis to be viable. However, this data can be used to the FI's advantage as machine learning can be trained to identify potential fraud scenarios using multiple data points, providing a much richer lens on potential criminality being perpetrated by or against FI customers. This in turn enables more precise customer interventions and ensures models learn faster to keep pace with criminals who continually adapt their attack methods, surfacing suspect fraud or scam activity earlier or even before it happens. AI is already helping to keep customers from falling victim to fraud and scams by identifying likely patterns of activity or customer behaviour:

Personalised Education - The use of victim propensity modelling may predict the likelihood of a customer falling victim to a scam, enabling targeted education through digital contact solutions. AI solutions can provide insights derived from trend analysis, for example a customer's lifecycle stage as a predictor of the type of scam a criminal may target them with. High Value Scams – The ability to detect a scam amidst genuine payment activity is an established challenge for Financial Institutions, particularly low value / high volume scam activity such as purchase scams. AI modelling can predict the likelihood that transactions are part of an emerging or ongoing scam as part of its real-time payment defence strategies. This gives Financial Institutions the ability to intervene early, contacting customers sooner and with richer insights to prevent harm.

Beneficiary Profiling – AI solutions may be deployed to enhance a Financial Institution's ability to identify criminal networks, including potential money mule and other first party fraud typologies, connecting with external data points through law enforcement for added insight into potential on-book criminality.

Internal Fraud – Leveraging conversational intelligence and audio transcription capability to enhance solutions to identify high risk indicators of suspect employee behaviour, increasing the insights investigators have to bolster evidence packages for criminal enforcement. FI's are just beginning to deliver the potential value that AI can bring in fraud prevention and detection, seeking to move beyond machine learning to adapt generative

AI solutions. Its necessity of use is underlined by the AI arms race that firms face, as state actors and organised crime syndicates unleash its potential for financial harm. It is therefore impossible for humans to compete with machines when it comes to optimising fraud defence mechanisms. The human input adds the most value by understanding AI's potential, where it can deliver clear improvements, sourcing the data and providing an environment for the systems to learn and adapt to an ever-changing environment.

With this also comes the opportunity for humans to leverage AI to identify, understand, and assess new, emerging and future criminal uses of AI, and the optimal strategies for addressing and mitigating these threats. In addition, an element of human agency will always be needed to ensure AI explainability.

It would be easy to prevent fraud if there were some straightforward single piece of evidence that separate fraudulent transactions from legitimate ones. Unfortunately, that is not the case. Fraudsters use the same services that are used by genuine customers when committing fraud. This leaves fraud prevention teams with the challenge of finding and accumulating multiple features, in order to predict whether fraud is being attempted. Traditionally, this has been achieved, with reasonable success, by creating very specific rules that use multiple criteria to identify patterns. The process of creating and maintaining these rules is labour intensive and is complicated by the fact that less than one in every thousand transactions is fraudulent – making false positives very likely. These rules are typically standalone and do not support each other. By using AI machine learning, and training it on mass data where fraudulent transactions and non fraudulent transactions are clearly identified, it can deploy multiple rules that can predict whether a particular transaction is likely to be fraudulent, is stopped and or is escalated for further review once a prediction becomes likely or reaches a particular threshold and as important continues to learn by being fed new data where fraudsters have evolved and used new techniques. It is impossible for humans to compete with machines when it comes to optimising thresholds over many criteria and combining these to generate a combined prediction as to fraudulent activity. The human input adds the most value by sourcing the data and providing an environment for the system.

> *"By using AI, & training it on mass data where fraudulent transactions and non fraudulent transactions can be clearly identified, it can deploy multiple rules that can predict whether a particular transaction is likely to be fraudulent, is stopped and or is escalated for further review once a prediction becomes likely or reaches a particular threshold and as important continues to learn by being fed new data where fraudsters have evolved and used new techniques. It is impossible for humans to compete with machines when it comes to optimising thresholds over many criteria and combining these to generate a combined prediction as to fraudulent activity. The human input adds the most value by sourcing the data and providing an environment for the system to learn".*

Question 6: How to improve overall AML/CTF effectiveness?

Traditional Key Controls, such as customer due diligence, monitoring and screening have always been siloed within a financial institution, and despite deploying ever wider nets, generating significant false positives, the biggest risk, in a highly regulated environment is undetected risk. Whilst Financial Institutions may be loathe to

widen the net, generating ever more false positives, a better response is to try to materially improve detection rates AND the quality of detection, without increasing or better still reducing false positive rates. This can be achieved in a number of different ways:

- by improving existing approaches, for example:
    - by pooling additional data from which new detection can be achieved
    - by collaborating with experts in order to generate new detection, from emerging relevant typologies or case studies, focused on particular crime types or on high risk counterparties
    - by increasing the confidence in relation to detection, predictability and explainability

It is possible to achieve gains without the use of AI, through better use of and/or improvements and/or combinations of people, process, data and technology. Nevertheless, by adding AI technology components, more could be achieved, with expectations that such adoption would outperform none AI usage. Examples of AI adoption to outperform existing approaches include:

- materially improving the quality of alerts generated in transaction monitoring and screening, so that the proportion of risk relevant alerts to false positive alerts is improved
- materially improving the explanation and presenting context as to why an alert has been generated to support a faster and better investigation and alert decision.
- new alerts generated targeting particular complex behaviours and transactional activity, where single algorithmic alert generation is too blunt an approach, particularly targeting complex typology types such as fraud and scams, human trafficking, trade based financial crime and sanctions circumvention and/or high risk counterparty types such as complex shell companies involved in high volume and/or recurring circular financial activity, mule and/or funnel accounts.

Question 7: How is AI adoption viewed by Regulators?

Key themes from regulators when considering AI, include the need for Financial Institutions to understand the fundamentals of this technology, and that it's underlying risks are well understood and an adequate control framework is put in place.

In France for example the ACPR has identified 4 interdependent criteria to be implemented in the design and development of an AI algorithm in the financial sector: 1). Appropriate data processing, ensuring regulatory compliance, and taking into account ethical considerations, such as fairness of processing or absence of discriminatory bias, 2) Use of a set of metrics to measure technical, and/or commercial efficiency, 3) Stability, being the robustness and resilience of the algorithm during its life cycle, that should be tested, on an ongoing basis, & 4) Explicability and Explainability, notions linked to transparency as to why and how decisions are made, so as to provide explanations of algorithm goal or operation to end users (e.g. customers), compliance and governance officers, along the 4 levels of explanation (observation, justification, approximation, replication), depending on the targeted public and the nature of the relevant risk.

As Financial Institutions scale AI solutions through supplier relationships, stringent explicability and explainability requirements could hamper their ability to derive benefits, something criminals don't have to contend with as they exploit AI solutions for illicit gain. Financial Institutions should engage actively with regulators to go on this journey together, building trust and confidence in AI derived outcomes.

It is also important to consider the dialogue occurring between regulators, Financial Institutions and AI creators, focusing on the ethical development of AI to balance technology optimism with the clear need to consider and institute controls to counter the potential for criminal exploitation of new and evolving AI solutions. Another facet to this is how regulators, Financial Institutions and other sectors come together to educate consumers. Criminal exploitation of, for example, deepfake capability has already provided for alarming use cases in how consumers are victimised. There is a continuing need to invest in public awareness campaigns to disrupt the human propensity to trust interactions, with this an important facet of any ethical development framework.

Question 8: Is Explainability essential to a successful AI deployment?

Whilst their is an emerging business case for many Financial Institutions in deploying AI (see above), an important element to any successful implementation, and to achieve support from internal Financial Institutions stakeholders as well as financial services regulators and data protection supervisors is to be able to explain how the AI is performing and whether it is operating within set parameters, which can be assured and tested.

Rules based is easy to understand – an alert being generated when a threshold is reached is not a hard concept to grasp, explain and test. AI is different. It is more complex. There are relatively few who understand, for example, random forests, clustering, and unsupervised learning and even less who can articulate how these techniques can be applied effectively in a fighting financial crime context. The temptation is to try do so using rules-based thinking and approaches but this is to force a square peg into a round hole. Or more prosaically, it is like trying to explain how to make a call on an iPhone using an instruction manual for a rotary telephone.

A useful approach to bring all this together is to establish an “Explainability Framework” up-front, which identifies all key stakeholders, their respective interests and what they need to see to be able to support the implementation. Not doing this and expecting sign off in a “ta dah” moment just before going live is likely to result in a lot of wasted time, re-work, damage to confidence and, at worst, project failure. But above all, the organisation needs to be ready and willing to take this new step. AI itself is not new, but its application in fighting financial crime is, and so monitoring performance and consequences closely will be important controls. In a financial crime use setting, outcomes may more readily point to protected consumer characteristics as indicators of criminality and so explainability becomes arguably more critical.

Question 9: Which roles and skills will support successful AI deployment?

It is self evident that smart people who understand AML and AI are important. However, there is a gap between the two: People who know how to build and apply models in an AML context are hard to find, but crucial. The key is being able to design models that identify and manage AML risk well. That is a different proposition from, say, designing credit risk models where absolute accuracy and precision is demanded.

AML lives in the grey zone where judgement and experience predominate and bank obligations stop at identifying and reporting suspicion through interpreting facts, but do not extend to establishing that money laundering has for sure taken place. The trap here is that human beings are allowed, and indeed expected, to have different opinions when interpreting a set of facts, whereas machines are expected to be right every time when looking at the same data.

Another factor is bias. Personal data that, rightly, should be excluded in one context, may indeed be relevant and even amount to a red flag in a money laundering context.

It is important therefore that people with experience in applying AI techniques in an AML context and who understand the principles of the Risk Based Approach are engaged. They need to know how to design models that can operate successfully in the AML grey zone, identifying the right risks in the right way, and then be able to explain in language that all stakeholders can understand.

Finally, it goes without saying that proper governance should be wrapped around any AI for AML project, with the right stakeholders, preferably as identified in the Explainability Framework, driving at senior level to ensure the proper balance between all interests is achieved, whilst creating an environment to allow the Financial Institution to proceed safely.

Question 10: How reliant is AI on data and on data quality?

AI feeds on data to learn and then to do it's work and so the quality of the work undertaken using AI is reliant on the quality of the data and the data infrastructure built and maintained by or used by the Financial Institution. In order to benefit from AI, the foundation is the availability of data, the right data, in the right formats and systems, and in the right quantity and quality. Any application of AI will only be as good as the quality of data collected and available for use. If previous activity being replaced has been mainly manual, and or very little data has been gathered and analysed, and/or it has a lot of variance in it, then this 'dirty data', will first need to be transformed by converting the data into a common format and importing it to a common system, where it can be used to build models. Whilst this sounds complicated, solutions are available to automatically collect the data from a variety of devices and systems, then automatically clean the data or format and ready the data for use. Starting an AI journey with a data first approach is crucial, as it avoids the implementation of AI only to find out later that outcomes are not as expected because of the unavailability or lack of quality of necessary data.