BUILDING AN EFFECTIVE FINANCIAL CRIME RISK MATRIX

WITH PARTICULAR REFERENCE TO UNDERSTANDING THE

NATURE AND FUNCTION OF KYC AND MONITORING TECHNOLOGY (REGTECH)

A TWO DAYS’ INTENSIVE SEMINAR AND WORKSHOP

IN HOUSE, IN PERSON
ON SITE or OFF SITE

Introduction

Many people talk about a financial crime risk matrix. For me, it all started decades ago when assessing risk for money laundering and terrorist financing when the UK introduced its Money Laundering Regulations 1993. They came into force in April 1994.

In those days, there were two quite equal aspects: risk and compliance. The risk came from "applicants for business" and existing customers or clients. Compliance came from some but not all regulators.

In the UK, there was a body of opinion that the Regulations applied only to banks. That was the first indication that different sectors would work in silos, looking at the Regulations in isolation. In fact the Financial Services Act, which had been in force since 1986, was relevant. By reading the two things together, it was clear that a wide range of businesses were covered. That included solicitors providing most services involving property and business, something that even several years later some large law firms continued to deny.

This was the genesis of my journey into the question of building a risk matrix – and I've been doing it ever since.

This course was first held in 2011 and it's the best selling course we have run. It's been run in many countries across Asia, the Middle East and in the British Isles.

> **NOW IT'S BEING OFFERED AS AN IN HOUSE COURSE. OUR DEFINITION OF "IN-HOUSE" IS A BIT FLEXIBLE.**
>
> **OF COURSE, IT MEANS ORGANISED BY A SINGLE COMPANY, OR A GROUP, FOR ITS OWN EMPLOYEES.**
>
> **BUT WE EXTEND IT SO THAT A FINANCIAL SERVICES COMPANY CAN ORGANISE IT AND ALLOW COLLEAGUES FROM OTHER COMPANIES TO ATTEND.**
>
> **AND WE EXTEND IT FURTHER TO ALLOW REGULATORS OR INDUSTRY GROUPS TO ORGANISE IT FOR THEIR REGULATED ENTITIES OR MEMBERS.**

The concept is simple: indeed some people think they can tell you about it in a one-thousand word article with a couple of graphics.

Hint: I can do what they do in a single sentence. Here it is: identify your risk points, if they apply to the customer assign a value and if the total of those values exceeds your risk appetite, don't proceed. I won't bother showing an image of a spreadsheet which is what they usually include.

If you want to know more and to find out why it's worth two days' of your time, continue reading.

What’s in and what out.

The starting point for any risk assessment is always the same whether your company is a mega-bank, a start-up challenger, a fintech or a non-bank financial services business. It is the law and regulation that defines what your obligations are and, even more fundamentally, what those obligations apply to.

But it is not you, the risk and compliance officer, that has to make those decisions on a minute by minute basis: it’s your staff and, increasingly, your technology.

This, you will understand, is not a matter of suspicion. It’s a matter of data collection, of yes and no answers, with the occasional ″maybe″ thrown in.

The course is highly targeted at one topic. We don't discuss the nature of financial crime, we don't look at compliance and we don't even look at law. Or at least, not much.

In this course, I will not be talking about your local law and regulation in detail. In fact, I’m going to leave that to you during the workshops.

Nor am I going to talk about how RegTech works. I will talk about how it works, or should work. And how it fails. And what you need to know to help you identify failures before they become a problem.

And while the nature of financial crime is a highly detailed subject, we only need a relatively superficial explanation for the purposes of this course.

In this course, we look at the factors that increase or decrease the risk score that attaches to a person (be that a natural or a legal person).

The course deals with sensitive issues and explains that nothing can be taboo but that risk assessment should not be judgemental or, worse, prejudiced. Delegates must expect to find that there are no no-go areas but that does not mean there is no room for courtesy and respect.

A properly designed risk matrix reduces the risk of the equivalent of "driving while black" and militates against the use of blanket de-risking.

The Premise

Every financial crime risk assessment is made up of a series of algorithms. Algorithms are everywhere in everyday life but they have been accorded an almost mythical status, increasingly seen as the exclusive preserve of artificial intelligence. But there really is nothing special about the concept of algorithms. In fact, you have used algorithms since the day you were born and you use them pretty much every minute of every day. Some are simple, some are complex.

You even started to use fuzzy logic when you were three or four years old: how strange then that the concept, so far as computers were concerned, is first documented in 1978, appeared in toasters and washing machines in the 1980s – and the USA's Financial Intelligence Unit, FinCEN, announced only in 2022 that it was to adopt fuzzy logic as part of its analysis despite the fact that it has been collecting unstructured data for at least 20 years.

As you have worked through management, you've used flow-charts or decision trees. That, right there, is the basis of your risk matrix.. It's simply algorithms run in sequence. Nothing clever about the principles.

There is no reason to be intimidated. True, some algorithms are nested. Some have to wait for one or more other algorithms to make a determination. But, again, none of this is clever. Or at least you will realise that it's not clever by the end of the course.

The clever part is deciding what data to collect, when to collect it, when to use it and what to do with the results.

So you will build, as a group, a basic risk matrix for your company. Then when it comes to considering RegTech, or even reviewing the performance of existing RegTech, you will be able to assess the inputs, analysis and outputs. This is not benchmarking. This is to see if you are getting the results you expect and want.

The fact is that only someone familiar with your business can properly define the algorithms that will protect your business. Generic algorithms are useful starting points but no system can know your customers if you don't know your customers so you can teach it.

There is a huge irony.

Regulators are increasingly taking the view that where a tech-based KYC / risk assessment system fails, that companies cannot blame the tech. **It is not a defence to say "we bought a black box and we expected it to work."** The very regulators that are pushing companies to adopt RegTech are saying that those companies must understand and control what it does.

This makes perfect sense: it has long been established that function can be outsourced but responsibility cannot. It would be to stretch common sense beyond breaking point to imagine that responsibility can be outsourced to a computer program or to those who design and/or implement it. The simple fact is this: if your business is using it, your bank is liable for its faults.

This course is not about technology . It is about what the technology is, and must be, told to do. This requires some very basic knowledge of *how* it does what it does. The course is not about maths but some very basic mathematics / statistics knowledge might be useful.

The course is also about specifying reports to ensure both value and consistency.

An effective financial crime risk management programme depends on a series of decisions.

To make those decisions, you set a series of criteria and apply those as a template to new business and to transactions as they happen.

But how do you set those criteria in a structured way, and how do they link together, to give you an effective risk assessment and control measure?

How do you maintain the criteria in order to ensure you do not get too many false positives - and don't let important issues slip through?

The answer is a risk matrix.

What is a “Risk Matrix?”

We hear a lot about “black box” analysis. A risk matrix is not a black box : it's a dynamic decision-making tool that you can apply to all of your customers to identify those who are within the "safe" zone - and which allow you to identify those that are higher but still acceptable risk as well as those that you should consider a high risk, even if not reportable. And it's part of best practice.

The risk matrix is defined by and in turn defines your company's appetite for risk. The concept is simple: the execution is complex.

Building a risk matrix involves considering a wide range of factors, including an analysis of your company, its products and services, factors relating to the customer and counterparties and external factors. An effective risk matrix does not stand still: it changes as applicable circumstances change.

That sounds like hard work – but it need not be. And properly executed a risk matrix will provide the starting point for all of your other systems to detect and deter money laundering, terrorist financing and other financial crime.

In this intensive and highly practical course, you will build a risk matrix that suits a fictitious or your own company and its products, and take away a model that you will be able to modify to take account of your own company's circumstances and changes in the environments in which you operate.

Who should attend?

- Compliance and money laundering officers
- Risk officers
- Internal audit
- Directors with compliance responsibility
- Regulators and inspectors
- Enforcement agencies

In this course you will learn how to design and use a risk matrix:

* factors that underpin risk matrix development
* economics factors that underpin the "proceeds" section of the matrix
* assessing countries risk
* assessing client types and risk
* assessing anticipated transaction profiles
*adding in external factors e.g. sanctions
* setting the weighting factors
* applying the matrix in practice
* the limitations of the matrix approach
* beyond the matrix – how it plugs into your existing systems and enhances them
* how to maintain the matrix

An effective Money Laundering Risk Matrix is:

- simple and inexpensive to set up

- simple and inexpensive to deploy

- simple to use

- simple and inexpensive to maintain

An effective Financial Crime Risk Matrix has the following outputs:

- prioritisation of risk based on factors you specify and applicable to you, your customers and your legal and commercial obligations

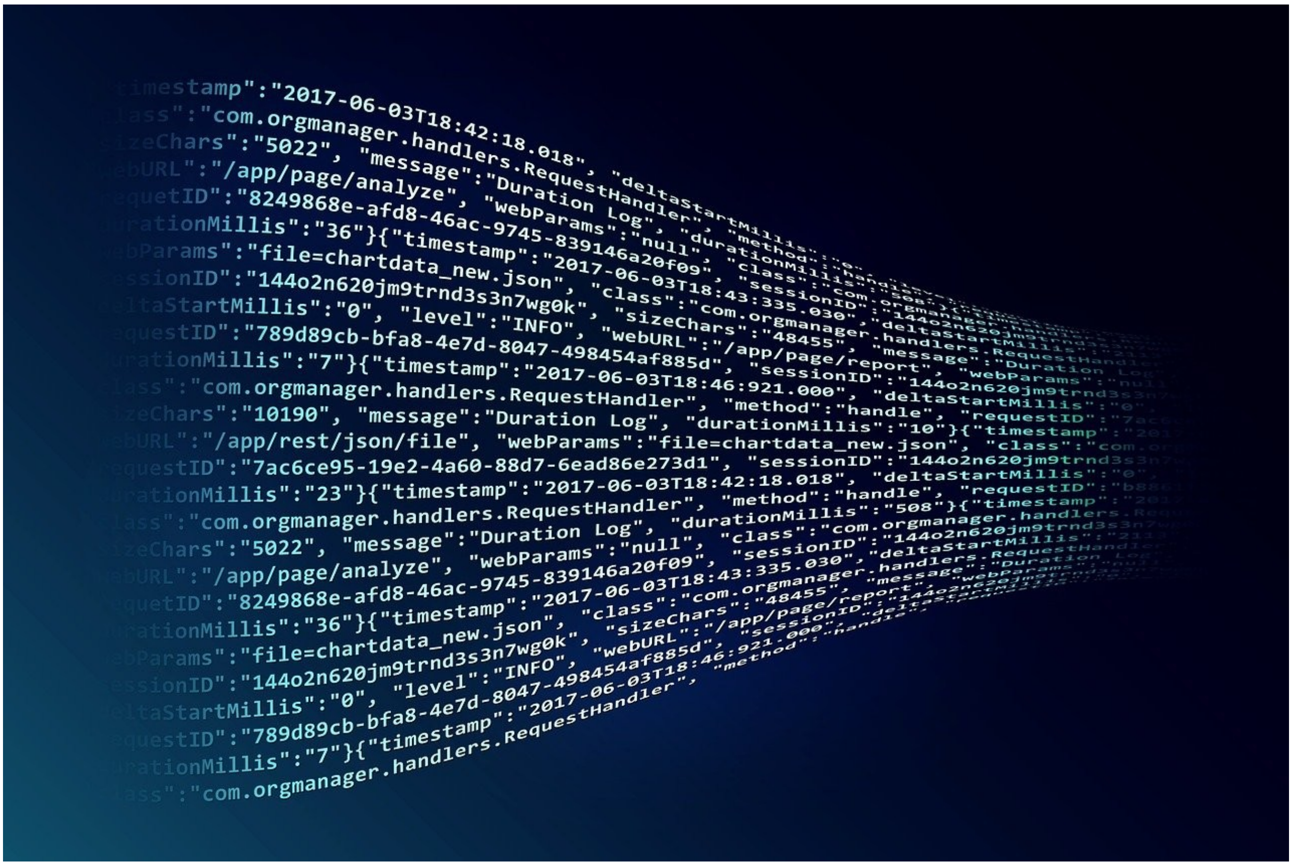
- alerts to higher risk customers and transactions based on your own assessment of risk

An effective Financial Crime Risk Matrix provides

- assessment information for you to make informed decisions for money laundering, terrorist financing and compliance purposes.

By designing your own risk matrix, you are in a much better position to assess the products and services of RegTech vendors both before you buy and as you periodically review existing implementations.

PS: regulators will find this exercise valuable so they understand the challenges facing regulated businesses. Why not book a session and create a risk matrix for a fictitious business?



Further Information

A PRACTICAL AND CHALLENGING TWO DAY WORKSHOP

ON SITE OR OFF-SITE.

LOCATION: ANYWHERE, SUBJECT TO SECURITY CONCERNS AND COVID-19 PROTOCOLS.

MAX 20 DELEGATES.

LANGUAGE: ENGLISH (EXPERIENCED AT WORKING WITH TRANSLATORS).

PRICING: DEPENDS ON LOCATION.

ENQUIRIES VIA FORM AT WWW.VORTEXCENTRUM.COM.