Deloitte.

Electronic Trading Risk Management

Minimise risks to maximise profit

Deloitte Risk Advisory – November 2021

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Introduction

The risk management of electronic trading (e-trading) has rapidly matured over the past decade as the understanding and impact of e-trading risks intensifies and attracts more concentrated regulatory focus. However, risk frameworks are often disconnected, siloed and inefficient across the lines of defence. Without dedicated attention, e-trading businesses remain open to the risk of operational incidents, disorderly markets, and regulatory scrutiny – with the potential to eradicate profitability attributed to technological advances.

Context

In this paper, we explore the challenges firms have faced in managing their e-trading risks, and the ways in which they can strengthen their frameworks, focusing on best practices and areas for improvement. We explain why committing resource to stepping back and reviewing their entire front to back framework, can protect the firm from risks materialising in increasingly uncertain and volatile markets.

Regulatory expectations

The automation of trading in financial markets has developed over the past decades from basic pricing calculations and order routing to more complex investment decision and machine learning techniques for seeking alpha. Firms now have large inventories of trading algorithms across all asset classes but have struggled to standardize the implementation of risk management techniques across their e-trading businesses.

Initial regulatory scrutiny and internal risk management was light touch, with the general treatment across the industry focusing on e-trading as 'just another method of execution'. However, as techniques began to be comprehensively adopted by regulated firms and events caused instances of significant market disruption, regulators across the globe began responding – setting expectations as to how firms should manage the risks inherent in electronic trading activity.

As the algorithmic capabilities of firms have developed swiftly during the recent surge of automation efforts, regulators recognised that prescriptive rules would quickly become outdated and therefore set 'expectations' around how firms should approach the challenges. This has left requirements open to interpretation – resulting in a wide degree of implementation maturity across the industry.

Risks posed to e-trading firms

Regulatory expectations only exist because firms are exposed to tangible risks through engaging in e-trading. The onus now is on firms to assess the level of risk being taken as part of an embedded process, specifically for their e-trading businesses, and to develop a commensurate framework in order to control risk.

Any good risk management framework needs clear ownership and responsibilities – documented and managed through an effective Target Operating Model. E-trading is no different, though it has been a difficult area for many firms to tackle. Expertise has typically sat within the business and first line of defence (1LoD). However, the need for independent oversight has been a challenging path for firms who lack the expertise to effectively oversee and provide adequate challenge from the second and third lines of defence (2LoD and 3LoD).

E-trading therefore requires a collaborative approach to develop an effective risk management framework. We will explore later how a robust first line controls framework can be leveraged by the second line to monitor the risks being run. Furthermore, adapting their existing risk management frameworks, firms have been able to look forward towards what a future-proof, nimble framework might look like – one that maintains the core principles of risk ownership and independent oversight, but that also does not slow down the trade order flow and allows e-trading businesses to remain competitive in a crowded market.

We have broadly broken down the approach into the following key constituent parts of the front-to-back risk management framework:

- **RISK GOVERNANCE**
- **RISK TAXONOMY**
- **RISK MANAGEMENT**

Risk Taxonomy

E-trading not only adds to the risks captured within existing risk management frameworks; it also generates new and emerging risks requiring a fresh approach. Firms need to figure out how best to integrate 'e-trading risk' into their existing risk taxonomy: usually a decision between separating out risks, or a cross-cutting 'horizontal' approach.

Definition and identification of e-trading and algo risks

Throughout this paper, we refer to 'Electronic Trading Risk' (e-trading risk) and 'Algorithmic Trading Risk' (algo risk) to cover risks associated with automated trading activity where there is limited or no human intervention; or where a computer algorithm automatically defines individual parameters of orders (i.e., price, quantity etc.). While definitions are enshrined in regulatory expectations globally, firms need to understand the practical application of this definition for their own taxonomy.

Writing a three-line definition is easy: implementing this into risk management practices is a lot more challenging. Firms often struggle with how they identify e-trading activity as they attempt to ensure risks are subject to appropriate controls. Identification can come at the trade, strategy, system, or business level: each has its own challenges. We have observed some firms that carve out e-trading activity in each risk class, allowing for specific treatment and risk management approaches. Whilst other firms do not separately set standards for e-trading and attempt to apply their existing risk management frameworks to the activity.

Clearly defining and identifying the risks subject to an ET Risk Management Framework (ET RMF) may be a challenging and laborious initial effort, but will allow all risk owners, oversight functions and senior management to identify exactly what they are responsible for managing. A well-documented framework enables risk functions to fully understand the scope of activity around which they need to set standards. For example, the ability to identify where additional controls are required to ensure ET activity remains within approved limits and is subject to adequate pre-deal checks.

Additionally, there are important distinctions to be made to ensure the correct risks are being captured, including specific regulatory expectations around the management of certain risks within e-trading. These include requirements for pre-deal credit checks, adequate surveillance of algorithms to identify unusually activity (including market abuse), and the monitoring of the e-trading environment for system runaway risks and unintended market impacts.

At a more granular level, firms benefit from being able to identify different types of activity that would be subject to the framework such as market making, automated trading decisions, order routing, execution and auto-hedging (trying to marry high and low velocity trades). Each of these activities will have subtly different inherent risks that will need to be controlled and managed as part of the firm's risk framework. Finally, frameworks should be nimble enough to adapt risk requirements for different elements of trading activity including trading algorithms, strategies, trading flows, applications, and platforms.

Firms that have established e-trading risk taxonomies have recognised the need to capture additional risks and nuances associated with a wider range of activities. These may introduce their owns risks or create a new dimension which has not previously been consider by the firm. Examples include:

- **Agent-versus-principal trading activity;**
- **Review, testing and approval of internal or third-party algorithms/applications prior to deployment;**
- **Direct electronic access;**
- **Cash-only and other margin considerations for client trading activity;**
- **Technology risk including the risk of being at the 'back of the queue' without keeping pace with the speed of change for both hardware and software;**
- **Human capital risk led by war for talent across industries;**
- **Data risk – volume, variety, velocity, and veracity.**

Finally, much of the challenge in risk managing e-trading stems from the resource impact of investigating control breaches and incidents. Identifying the source of the issue, can help mitigate the resource impact of the investigation process. A robust identification process – including a granular taxonomy – will allow businesses to design control environments that are directly linked to the risk framework. Ensuring controls requirements are consistent with the taxonomy is an imperative final step and will require strong expertise in the second line of defence, or a collaborative front to back approach across all stakeholders.

Standalone vs integrated taxonomies

Most firms have recognized that e-trading is not simply a digitization of an existing process but is an entirely new execution method that needs to be separately captured to ensure nuances of such activity are appropriately considered and managed.

Approaches vary across the industry, but broadly fall into two camps:

- **Standalone risk class; or**
- **Specific consideration of requirements within risk classes as part of the existing risk taxonomy**

Deciding which approach to take, depends on how e-trading risks are captured with the firm's risk taxonomy and risk management framework (RMF).

Standalone e-trading risk taxonomy

Specifically identifying the risks inherent in e-trading activity will inevitably lead to 'new' risks that firms have not had to consider before, such as system runaway risk [i.e., a lot more process risk requiring more risk measures at different parts of the process]. Many of these tend to be technology or operational risks in nature but can materialise through other risk classes (in the form of contingent market risk for example) that will need to be adequately controlled. Using the stalwart operational risk example of the fat finger trade incident in the front office, potentially giving rise to a significant loss: e-trading increases the possibility of lots of trades you didn't want to do intersecting with the market moving against you – heightening many risk factors and magnifying the potential losses to the firm.

A dedicated e-trading risk identification process will also lead to greater focus on risks that may have been identified previously but not considered material in a high-touch trading environment. For example, the risk that intraday financial risk limit excesses are not adequately captured. In legacy risk systems limit breaches are often only spotted once overnight processes are run (typically trade reconciliation or risk aggregation). However, in a fast-paced e-trading environment, such controls are clearly inadequate, leading to a requirement for the identified risks to be captured and controlled on an intraday basis.

Model Risk is an area that several firms have struggled to shoehorn e-trading into their existing framework. Whilst the risks are undoubtedly similar – Model Error risk or risks associated with Release/Change Management – the ability to monitor and control risks becomes heightened in a much faster and data intensive environment.

Firms should look at how they capture and respond to model risks in the e-trading context, in particular how issues are captured, and how controls are implemented to halt or limit trading whilst issues are resolved. Firms historically relied on testing, review, and validation requirements as controls to mitigate model risk. But in real trading conditions, in the review and approval of trading algorithms, models are difficult to replicate and test within the existing environment. In other words, the model can be shown to be working as anticipated in the test environment but may not work as designed in the live environment. This may be driven by data latency being too great or model execution is too slow, leading to market, pricing, and best execution risks.

This example demonstrates why firms need to identify algo models separately and consider additional risk monitoring and controlled by a dedicated and experience e-trading model risk team. This shouldn't be limited to performance metrics but should expand to review and validations cycles and any further aspects that may require additional considerations within the model risk management framework.

Integrating e-trading into existing Risk taxonomy

A completely standalone e-trading taxonomy has not always been appropriate for all firms. A better approach may be to integrate e-trading risks into the existing risk taxonomy and risk management framework (RMF).

An integrated taxonomy may be particularly effective for financial risk classes, where legacy approaches can be tailored to e-trading (for example through bolstering intraday capabilities). Some firms have seen benefits of this approach for both electronic and non-electronic trading activity. The industry has historically struggled to adequately capture intraday risks despite significant resource being dedicated to finding solutions. However, structuring an intraday approach to cope with the intensity of e-trading can be a good starting point for institutions to further develop their intraday capabilities across the board.

Similarly, significant effort has been focused on enhancing compliance supervisory activities, which could remain appropriate for e-trading if adapted for the faster paced nature and with additional behavioural considerations incorporated into the oversight framework.

Risk Governance

Principles of clear ownership, governance and independent challenge across the framework are vital to ensure accountability and completeness of the oversight of e-trading risks across all lines of defence. Challenges in hiring sufficiently experienced risk managers should not give rise to a blurring of the lines of defence. Before addressing how risks are managed, firms should ensure that roles and responsibilities as part of any framework design are clearly outlined and understood, and an effective, formal governance structure has been put in place.

Ownership

All businesses should be responsible for the risks they are running – this is as true for e-trading as it is for any other activity a firm carries out. Furthermore, this principle is equally applicable for all types of risk, whether financial or non-financial in nature, and extends the responsibility for managing these risks across the respective business as the first line of defence. In order to ensure that all businesses are employing a consistent approach and standard of risk management, it is important that firms define a framework for the management of these risks.

Businesses should not typically set their own minimum standards of risks and controls without being challenged on their appropriateness. Therefore, in setting consistent standards across businesses, the key principle for consideration is the independence of the responsible function for setting those standards. Ownership of a risk management framework has been approached in several ways across the industry. Some firms have aligned responsibility with expertise, maintaining ownership within the first line of defence but ensuring independence through distinct reporting lines of a business risk function – the so-called “1.5 Line of Defence” function. However, a more typical approach has been one which follows historic risk management practices – framework ownership sitting clearly within a second line of defence function. This independent function will then own the responsibility for oversight of risks through businesses compliance with the proposed minimum standards, including how they are implemented.

Ultimately, a decision around ownership of the framework should be definitive and should be consistent with the wider approach to risk management at the firm. Whilst nuances for e-trading should be picked up, as we will cover later in the paper, it is also important not to completely reinvent governance approaches, which could cause confusion when compared to other risk-taking activity.

Target operating model

Once ownership has been defined and responsibilities accepted, it is vital that the structure is clearly documented and implemented. The target operating model should filter down from high level ownership of risk versus oversight, to individual framework elements. Some firms have expressed difficulty in taking high level ownership principles, and applying them to identification, measurement, monitoring and control elements of their e-trading Risk Management Framework (herein referred to as “ET RMF”).

Granular agreement and documentation of ownership creates clarity and can allow each respective function to focus on the effectiveness of control activities. Moreover, in an e-trading environment, it is even more critical that ownership of each element of the risk management lifecycle is transparent due to the fast-moving nature of risks, there will be no time to discuss responsibilities during an active risk event.

The most effective Target Operating Models have empowered dedicated resource within the first and second lines of defence, for e-trading Risk Management. These dedicated functions have proved invaluable in joining the dots across the traditional risk stripes across the lines of defence. For example, within the second line of defence, one team overseeing e-trading can coordinate risk management efforts by leveraging Credit, Market and Operational risk expertise, whilst ensuring consistent control standards are implemented across each of the risk classes. Equally, a dedicated ET Risk Management team can ensure new and emerging risks do not fall between the gaps of historic responsibility.

First Line of Defence

Generally, e-trading businesses have a developed and well understood approach to managing their risks, recognising the need (not just the regulatory push) for a robust control framework. We tend to see two challenges facing the first line of defence at E-trading firms

1. How well integrated is e-trading framework with booking model controls, legal entity controls, supervision framework for example:
   a. Who is responsible for risks booked by an algo in particular where it is not trading as expected: the algo owner in one jurisdiction or the book owner in another?
   b. Are controls built to supervise trader mandates adequate as the firm moves to an increasingly low latency?
   c. Are all booking models captured including DEA (direct electronic access), trading across multiple legal entities, etc.
   d. What happens when there are different algo model standards in place across jurisdictions, or where there is a risk that trading algorithms are used in jurisdictions that the models themselves have not been approved (see below)?
2. Lack of consistency across e-trading businesses – which often have developed their own controls from the bottom up as they have expanded
   a. How are best practices across the firm and assets classes maintained?
   b. Can risks be effectively aggregated across businesses to show a true picture of the risks to which the firm is exposed?
   c. Are all the algorithms' risks understood and adequately captured?

Typically, businesses have developed controls that oversee the risk to their revenue generating capability within the business (e.g., greater focus on system outage risk than credit risk) – but which have not considered the wider requirements of their colleagues within the second line of defence – limiting the ability for the 2LoD to challenge and set minimum standards across businesses due to differing approach to implementation of control instances.

Second Line of Defence

Despite many firms' efforts to develop their e-trading expertise across the second line of defence, there still tends to be a knowledge and resource gap at many firms. There is often a trade-off between a dedicated e-trading Risk Management team and assigned representatives in each risk class. In well-developed and mature examples, we see a dedicated team located horizontally within the function, providing SME input across each risk class. Whilst more resource intensive, a dedicated team can bridge the gap between risk classes and ensure e-trading issues are covered across the risk taxonomy with centralised ownership and escalation, rather than a siloed approach in each risk class.

Some firms have opted for a siloed approach, asking risk classes to expand their frameworks (e.g. Credit or Market risk frameworks) to stretch and bend in order to encompass e-trading. Whilst it might be initially less resource intensive, this approach tends to create additional expense as risk classes independently identify and seek to address weaknesses. For example, risk classes independently setting limit and control requirements could have the potential for businesses to set multiple control instances and monitoring frameworks.

Siloing can therefore be ultimately expensive, and potentially leave the firm open to risks falling between framework, knowledge, and oversight gaps. Compare this to a centralized approach where all risk classes express minimum risk management requirements for businesses and trading algorithms, which are addressed by one set of calibrated limit and control requirements that the business can implement as part of onboarding a new e-trading strategy.

Governance and escalation

Holistic oversight of ET-related risks should be owned by an appropriate governance authority. This could be either part of an executive risk committee or a dedicated sub-committee, co-chaired by first and second lines of defence to ensure risk ownership and effective challenge.

Firms have debated the need for a dedicated e-trading risk management committee with some relying on the inclusion of e-trading as a specific topic within existing risk governance fora. Increasingly, we are seeing firms create dedicated risk committees for e-trading as they have identified the need for sufficient expertise and dedicated time to cover e-trading risk topics.

Similarly, existing escalation channels across risk classes may not adequately cover the expertise required to resolve issues that need to be escalated. Therefore, market practice now looks towards dedicated escalation structures between the lines of defence, all the way up to the dedicated oversight committee. Delegated authority and assigned senior resource are also vital given the drastically reduced timelines for escalation, approval and remediation associated with e-trading. This could include identifying senior resource with the bandwidth to make approvals on an intraday basis – or indeed creating alterative pre-approval structures.

Risk Management

The journey towards a fully mature and implemented E-Trading Risk Management Framework may require redesign, recalibration, and a fundamental rethink of how risks are identified, measured, monitored, and controlled. The Risk function should look past the technological and operational exercise of implementing an existing framework on an intraday basis. They should instead consider the opportunity to rethink how the framework quantifies risks and calibrates risk appetite. Collaborative initial effort across the lines of defence and dedication of resource can enable the firm to implement a futureproof and effective framework.

Risk identification

Above we have indicated how an ET RMF can be structured around the risks that the firm identifies as being exposed to through its risk identification processes aligned to the risk taxonomy. Another fundamental aspect to the risk identification process is in setting risk appetite.

Many firms are engaged in an ongoing struggle with the concept of setting risk appetite for e-trading: some have put this down to inadequate risk identification processes and challenges in aggregating e-trading Risk. Whilst other firms don't feel the need to differentiate between different types of trading activity for the purposes of appetite setting.

It is inevitable that during the journey towards a holistic front-to-back framework, e-trading firms will recognise the difficulty in not adapting their risk appetite approach for e-trading. For financial risks, setting appetite based on modelled approaches to exposure will create aggregation challenges and inevitably cause inefficiencies in latency through trying to simulate an aggregate exposure.
For non-financial risks, trigger levels for magnitude and frequency of incidents – as well as investigation thereof – tends not to be appropriate for an automated trading environment.

Therefore, when setting risk appetite, 2LoD functions should ensure they fully understand the business's capabilities in managing against an appetite – setting levels commensurate to the tangible ability to calculate and manage against. Some firms have looked towards 'decomposed' appetite setting either through the measures used or the level at which appetite is set (e.g., strategy/desk level rather than portfolio level).

Furthermore, all stakeholders need to understand the strategy and booking model of approved e-trading activity. This is pivotal in understanding exposure trends and behaviours that are being risk managed, without which an effective and commensurate appetite cannot be set. For example, are there specific times during the trading day/month where we might see spikes in exposure or more critical impact of operational incidents such as system outage. Working with desks/businesses to create a better understanding can help mitigate impact of 'noise' in the control monitoring framework – and ultimately ensure resource is focused on actual risks

The collaborative approach in setting risk appetite for e-trading is a perfect demonstration of the need to develop a standalone and nuanced framework. Understanding capabilities and limitations allows the 2LoD to independently set levels against which the 1LoD can physically risk manage.

Risk measurement

Historically, risk management often relies on a golden source risk aggregation system to calculate portfolio exposures and estimate likely losses. Responsibilities tend to be divided between supply of accurate trade data from businesses/1LoD, to 2LoD responsibility for aggregation and calculation of exposures.

Relying on a legacy approach or building an e-trading RMF based on these risk measurement concepts, will create significant challenges in capability, accuracy, and effectiveness – not to mention the significant resource required for an intraday aggregate modelled exposure. Furthermore, the latency implications of creating such a system (and controlling limits against it), such as routing an order to a calculation engine and running an exposure simulation to establish whether limit capacity exists, would not be viable for many e-trading businesses to operate as part of a pre-deal check for every trade.

Some firms have therefore started to shift the onus from 2LoD aggregation to 1LoD calculation, based on a decomposed approach to risk appetite mentioned earlier. This involves setting, measuring, and controlling risk appetite at a granular Business level for example setting algo limits by risk sensitivities rather than limits on an aggregated exposure basis. Firms will need to make the link back to their risk models (particularly where regulatory approval exists in order to pass the 'use test') – but can focus on more tangible controls and 'live' views of limit utilization that can be incorporated into pre-deal checking for ET trade flows without sacrificing latency. Firms should inherently build risk measurement capabilities into their trading architecture and ensure that all technological developments to trading capabilities include consideration for quantifying risks. This is a change in ownership and responsibility that should be baked into the ET RMF. 2LoD should oversee implementation, with appropriate skill sets and expertise to challenge and approve the solutions that are built.

On the non-financial risk side, measurement of the impact of operational events has generally adapted to capturing e-trading events, including ensuring lessons are learned from material loss (or gain) events. This is unsurprising as many e-trading risks remain categorised under the Operational Risk taxonomy (e.g., Connectivity risks, System Runaway risks, Data Integrity risks or Release/ Change Management risk).

However, it is important to recognize that the distinction between financial and non-financial risks is less defined within e-trading. Firms should recognize that multiple small operational events occurring alongside market exposure movement, will together give rise to the risk of losses to the firm. Therefore, the focus should be on monitoring through the use of early warning indicators, and mitigating losses through the use of controls and halt of trading protocols.

Risk monitoring

Monitoring e-trading risk should not be limited to monitoring the absolute level of risk being taken, but also monitoring the performance of the risk management framework and its associated controls.

A lot of focus has been given by firms to ensuring a robust control framework is in place to ensure automated trading activity stays within appetite. Understanding the use of such controls can assist the firm in improving the framework, and to identify weaknesses. Some firms displayed significant challenge in their ability to measure the performance the control framework, such as implementing metrics to monitor the number of instances of control usage (e.g. hard blocks in order to avoid limit breaches). The concept of 'near misses' (inc. metrics around control usage), allows senior management to understand how vigorous the reliance on controls is, as well as enabling businesses and algorithm owners to identify the need to recalibrate models, risk appetite or both.

Many firms have tried to develop tactical e-trading risk metrics and dashboards – but most still struggle to concisely aggregate the risks into a digestible format, particularly for senior management. There tends to be a heavy reliance on prior knowledge and familiarity with legacy reporting formats for management and the executive to understand what they are looking at. Whilst this paper talks about the importance of dedicated resource and expertise – this does not negate the need for brevity and concise articulation of risks. Responsibility tends to sit with the 2LoD dedicated risk function, who often struggle with the tools available to them through legacy reporting by the individual risk classes. A fundamental redesign of the monitoring platform would certainly herald benefits for senior management as well as the day-to-day oversight of e-trading using risk dashboards for exposures and control performance metrics. Focus should be on context and comparability of risk between asset classes – drawing attention to the most material risks to which e-trading exposes the firm/entity.

Risk control

E-trading risk management relies heavily on preventative controls, given the automated and fast-paced nature. We often see e-trading businesses leading best practice within firms as they recognise a need to control their activity. However, challenges remain as to how consistent control instances are across businesses and asset classes, including the ability to set minimum standards by the 2LoD. Furthermore, 2LoD are heavily reliant on the expertise of the 1LoD for design, testing and implementation of e-trading controls.

As part of an effective front-to-back e-trading risk management framework, 2LoD should be skilled and tooled with the ability to challenge how controls are implemented against their minimum standards. This is often effectively done by a dedicated e-trading Risk Management team, with expertise across the trade lifecycle and architecture, including of specific risk classes. Their roles tend to be less around excess-monitoring, and more focused on ensuring algorithms and controls are appropriately tested prior to implementation.

With the aforementioned introduction of 1.5LoD risk and controls teams established within the 1LoD, 2LoD control testing takes on a more 3LoD role compared to historic activity. The Internal Audit function may subsequently have more light-touch role within the overall testing of e-trading risk controls and will focus more on ensuring an effective review of how testing has been carried out as part of the framework, only undertaking detailed work in areas of heightened risk.

Finally, when implementing a new ET RMF, firms have expressed challenges in retrospectively ensuring all existing algorithms, strategies and systems comply with the framework. Unfortunately, there are few solutions to this other than carrying out a one-off recalibration exercise. Whether this is reviewing and updating all model documentation to meet a minimum standard or implementing new preventative controls within well-establish trade architecture – the exercise is essential in order to be confident that the firm's risks are properly captured and controlled.

Conclusion

In summary, the benefits of taking a refreshed look at how your firm has set up its oversight of e-trading risks should be fundamental to ensuring the institution is adequately accounting for the risks it is running.

Ensuring your framework appropriately captures e-trading risks will require some reconsiderations of how risks have historically been managed, including some potentially fundamental redesigns of the approach to risk management. This should include the way appetite is set and control requirements are developed. Furthermore, a one-off exercise to recalibrate businesses and controls may be resource intensive but will empower the firm to be confident that they are on a good level footing upon which to operate in a future state.

There is no one set standard or requirement for e-trading Risk Management. We have seen many different approaches and continue to see appetite evolve as understanding improves both at regulators and across senior management and executives at firms. However, whatever the degree of implementation firms are comfortable with, they are clearly able to articulate the approach they have settled on, not just for supervisory bodies, but for their own day to day operational purposes. The biggest risk of all is that a framework for managing e-trading risks doesn’t exist and isn’t continuously evolving.

Contacts

Mo Abbas

Senior Manager

Tel: +44 20 7007 5497

Email: moabbas@deloitte.co.uk

Adam Clarke

Director

Tel: +44 20 7007 6550

Email: adamclarke@deloitte.co.uk

Damian Hales

Partner

Tel: +44 20 7007 7914

Email: dhales@deloitte.co.uk

Zeshan Choudhry

Partner

Tel: +44 20 7303 8572

Email: zchoudhry@deloitte.co.uk

Mark Cankett

Partner

Tel: +44 20 7007 5150

Email: mcankett@deloitte.co.uk

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.