



complinet

www.complinet.com

Expert White Paper Series: Integrated Global Screening Solutions

Harnessing Technology to Meet Burgeoning KYC Requirements

June 2007

This paper examines the increasingly complex terrain of Customer Due Diligence (CDD), Know Your Customer (KYC) and Customer Identification Program (CIP) requirements. It discusses the regulatory obligations of reporting entities, the underlying principles, procedures and processes involved, and the ways in which technology can help firms meet their obligations and provide the appropriate foundation for anticipated future developments.

By Vincent White: KYC Specialist

Industry Braces Itself Against Mounting Regulatory Demands

The extent and rigor of customer screening has advanced rapidly in recent years, caused directly by regulatory requirements but indirectly due to political and economic change. It is only fifteen years since the EU brought into force the first Money Laundering Directive which obliged financial institutions to verify customer identity and report suspicions of money laundering. Since then the development of anti-money laundering legislation has become linked inextricably to an assault on terrorist financing, relatively trivial in scale, yet a prominent element of financial crime with grave consequences to global political stability.

Although the 'due diligence' process has been long established in some areas of business, e.g. in the legal profession, more and more industries are now obliged to carry out some form of customer identity verification, screening, or background checking. Customer Due Diligence (CDD) requirements themselves have been 'enhanced', with major developments in transaction monitoring, risk-based assessment and management, and the scrutiny of business counterparties. Some firms and sectors have systems and controls already in place, but even here the new requirements may be seen as daunting.

Where before customer investigation was specific to business sector, product and transaction type, there is now a trend towards unifying the disparate strands of due diligence, from identity verification to credit and criminal record checks, to company investigation, into a single integrated process. It is the unprecedented accessibility of information coupled with market demand that heralds a convergence of these streams, such that businesses can meet the ever changing regulatory requirements without being overwhelmed by ever-more demanding compliance obligations and attendant costs.

Where Are the International Standards?

UK Legislative and Regulatory Environment

In the UK there is a myriad of primary and secondary legislation that have a bearing on due diligence and customer screening obligations: the Money Laundering Regulations 2003 (implementing the EU Second Money Laundering Directive) and 2007 (implementing the EU Third Money Laundering Directive), the Financial Services and Markets Acts (FSMA) 2000, and the Proceeds of Crime Act (PoCA) 2002. Additionally, the Terrorism Act 2000 forms the basis of legislation surrounding terrorist financing, targeting it alongside money laundering, although the two need not be related.

The Joint Money Laundering Steering Group (JMLSG), an organisation formed from UK Trade Associations in the financial sector, publishes guidance notes to help reporting entities interpret UK Money Laundering Regulations, and sets standards and expectations of good industry practice for relevant firms. Adherence to JMLSG guidance is now mandatory for this sector, with approval by HM Treasury, and there are enforcement provisions for money laundering rule breaches in the FSA

Handbook. Likewise, similar guidance is issued by designated professional bodies in other sectors, for example, The Law Society Money Laundering Task Force.

European Union - Third Money Laundering Directive

The 2nd ML Directive, adopted in December 2001, included a provision for the European Commission to produce a third Directive within three years. This incorporated the revised FATF recommendations on anti-money laundering and combating terrorist financing, issued in June 2003, bringing this guidance into law. The 3rd Directive was formally adopted in December 2005, allowing Member States two years for implementation which is now looming large in firms' increased compliance responsibilities.

Changes to CDD largely involve transcribing previous guidance into the regulatory regime. This includes:

- ▶ enshrining the risk-based approach within KYC processes;
- ▶ situations requiring enhanced due diligence (EDD), most notably for Politically Exposed Persons (PEPs), and exceptions for simplified due diligence (SDD);
- ▶ ongoing screening to ensure continued protection of the firm and integrity of the clients;
- ▶ establishing beneficial ownership and subsequent identity verification.

United States' AML Regime

The Bank Secrecy Act (BSA) was enacted by United States Congress in 1970 to help prevent financial institutions from being used as intermediaries, or being used to hide the transfer or deposit of the proceeds of crime. It created regulatory reporting standards and requirements for financial institutions (Suspicious Activity Reports, SARs, and Currency Transaction Reports, CTRs). Subsequent amendments have strengthened anti-money laundering and terrorist financing requirements.

Title III of the USA Patriot Act (2001) is itself an amendment to the BSA. It established new rules and responsibilities for banks, financial institutions, and non-financial commercial businesses. While the full scope of the Patriot Act has created controversy and criticism with respect to an erosion of civil liberties, the provisions relevant to KYC are consistent with the FATF recommendations, and in line with a risk-based approach to AML, despite broad differences in the regulatory regime and culture between Europe and the US.

Outside the G8 and Europe AML/CFT systems are at various stages of maturity and sophistication, but current FATF members (and to a lesser degree, observers) share greater similarities through their alignment on common international standards and objectives, however far they may be in practice from complying with all the recommendations. As with many inter- or supranational bodies, the specific functioning, remit, and mandate cannot be clinically abstracted from a larger geopolitical environment. However, when comparing AML/CFT systems between countries the US warrants special consideration

as an unusual case because of the extra-territorial nature of its regime both currently, and in anticipation of continuing development in this direction.

Customer Identification and Screening Methodologies

- ▶ Electronic Identification and Verification
- ▶ Customer Due Diligence
- ▶ Enhanced Due Diligence
- ▶ Beneficial Ownership
- ▶ Transaction Monitoring

Electronic Identification Accelerates the Customer Take-On Process

The first step in customer due diligence is to establish whether the customer is who they say they are. Proof of identity is required in all manner of transactions both within and without the financial services sector, and the acceptable forms such identification may take in turn depend on the nature of the transaction or activity. Types of identification include primary identity documents (passport, birth certificate); secondary identity documents (driving license, social security/national insurance/fiscal number); evidence of home address (civic registration documentation, electoral roll, recent utility bills); in the laxest of situations, a telephone number or address may suffice.

Increasingly an electronic process for high speed checks through electronic ID verification and validation incorporating multiple checks on several of the abovementioned identification types have taken precedence as the preferred medium for undertaking these types of checks.

The falsification or counterfeiting of identity documentation, or unlawful misrepresentation of identity ('identity theft') cause real problems in establishing authentic identity. Despite the advances in technology, the increasing sophistication involved in false identification has given new impetus to more advanced identity verification techniques, specifically through biometric means. It is now essential to have the ability to cross-reference multiple databases to validate that the name, address, NI/SS number, passport number, utility information, driving license, electoral roll, telephone number all validate each other by cross-referral. It has become all too easy to supply a valid passport with a fake picture and a valid piece of secondary identification to reference the primary source. These electronic databases are, however, able to make multiple cross-references automatically indicating any inconsistencies and providing a scoring algorithm that may be used to make a business decision or account-opening decision in a matter of seconds rather than days or weeks as was previously the case. This not only increases the validity and effectiveness of the identity verification check but also greatly increases the speed and efficiency of business decisions.



Customer Due Diligence Using A Risk-Based Approach

Regulatory and business-related information is necessary to properly know your customer. Although due diligence is a process driven by regulatory and compliance obligations, the investigation of this information is also vital for measuring the risk of a transaction or business relationship. For any firm this is particularly important as the need to understand overall dangers will determine the suitability of doing business with a given individual or company depending on the chosen appetite for risk.

Knowing more about your customer does not lead to a straightforward answer on whether you should do business with them, rather, it is a means of making a more informed decision in the context of a risk-based approach to due diligence.

Attitudes to risk vary and will depend on the size and nature of business being conducted, composition of the client base, jurisdiction of the activity, product and transaction characteristics, and ultimately, on a firm's own risk appetite.

KYC checks can provide the following information on a client or intermediary:

- ▶ company registration details and financials
- ▶ authorized or approved status of a counterparty
- ▶ regulatory enforcements or warnings
- ▶ sanctions applied
- ▶ politically exposed status
- ▶ any relevant adverse media

The screening process is not a one-off event; it should occur at account take-on, in certain cases retrospectively on existing clients, and continually for all customer types, even those subject to simplified due diligence, since both screening source data and client attributes are subject to change, as of course is the regulatory environment itself.

The frequency with which the process is revisited or repeated should rest on several considerations, and again, this involves a rational self-assessment of the relevant factors. How dynamic or subject to change are the data being screened against? How frequently are customer details liable to change? What considerations result from the company's activities, or internal policies and procedures?

Enhanced Due Diligence for Politically Exposed Persons (PEPs)

PEP checking has become an integral part of the due diligence process and is fully embedded in the latest regulations. It is incumbent on firms to have a proper process in place for checking for PEPs within the firm's client base. The specific areas of concern surrounding PEPs must incorporate the firm's:



- ▶ definition of a PEP, involving interpretation of, or augmentation to, the letter of the regulation
- ▶ senior management approval for doing business and ongoing oversight
- ▶ ability to establish the source of wealth/funds
- ▶ the frequency of ongoing monitoring/screening

There is ever-increasing clarity around the definition of PEPs, and it is clear that checking for PEPs within client lists is an obligation that cannot be ignored. Integrating one of the various PEP databases into your technology solution is key and a major consideration should be the ability to investigate this status with a single check covering all the different data elements.

Commercially available PEP databases differ in many respects resulting from the practical interpretation of the regulations. These precede a firm's own determinations, but grapple with the same questions – where should the seniority threshold be drawn? After what period should a former PEP no longer be considered tantamount to a current PEP? What constitutes a 'close' relative, or 'known' associate? The risk-based approach cannot provide objective absolutes for these questions, and so the compliance practitioner is compelled to interpret the regulations in light of the particular PEP risk faced by the firm. The expectation of the regulator thus becomes oriented around firms' rationalization and reasoning in terms of the approach adopted.

The differences between the scope and composition of PEPs databases can be scrutinized and thoroughly understood, but their limitations must also be acknowledged, from their overall coverage to the constraints of using information in the public domain, to the potential conflicts of interest between AML requirements and data protection law.

All high-risk entities require enhanced due diligence, and thus closer monitoring on an ongoing basis; PEPs are collectively a type of higher risk customer, although not all PEPs individually pose the same risk. As such, using other tools in tandem, particularly global media, can complement conventional databases by providing information resulting from investigative journalism, such as alleged or suspected corruption that translates into risk although unproven, or the associations between politically exposed individuals and corporate entities, where beneficial ownership cannot easily be established.

Ascertaining Beneficial Ownership

This is arguably the most complex AML activity because of the nature and complexity in identifying ownership surrounding certain corporate vehicles, e.g. trusts and shell companies. Very few suspicious transaction reports (STRs) are made by company formation agents, and the identity of beneficial owners can be easily hidden behind nominee officers. It is, however, still a clear obligation that this ownership needs to be established above a certain threshold which is increasingly being accepted at the 25% ownership threshold of an organization. This figure does differ by jurisdiction and data across different geographies can be extremely difficult and expensive to collate. It is therefore key to perform an appropriate level of company due diligence to prove that ownership has been checked and verified where possible.

On and On and On-Going Transaction Monitoring

Only once a client has been fully verified using technology to cross-reference all the previous different database sources, screened for KYC purposes, is determined not to be a PEP, has no credit issues and is determined not to be a beneficial owner or director of any potentially sanctioned, corrupt, or terrorist-funded organization does the process of actually doing business commence. Here, the ongoing screening obligations begin and the ability to assign transaction type profiles to clients kicks in. This should allow both rules based on basic transaction characteristics and thresholds to be set, and rules particular to the client's 'normal' behavior with respect to volume, value and velocity of transactions. Again, technology has to play the key role or the volume of activity and time to check transactions is prohibitive. Time spent defining the risk profile of the individual client's predicted and acceptable transaction behavior will reduce the amount of exceptions or false positives thereby delivering longer term process efficiency. Increasingly, alternative methodologies employing artificial intelligence have proved to be overly complex in managing transactional activity. It can take many months before it becomes effective and starts to bring any return on the initial investment. It is recommended that firms seek simpler rules-based systems integrated into an overall technological solution to report anomalous activity in client and transaction behavior.

Game, Set and Matching Mechanisms

Knowing your customer comprises both identity verification and further due diligence, but the latter differ in regard to the mechanics of screening. Verifying the identity of an individual or corporate entity, beyond checking identity or registration data, is bolstered by the ability to cross-reference multiple attributes to corroborate a correct identification with a high degree of confidence.

Due diligence on entities in the context of checking against internal watch lists, sanctions, regulatory enforcements or PEP lists is largely oriented around matching names as the primary identifier. The absence of supplementary data with respect to customer details or within watch lists or PEP databases has traditionally lead to methods of name-based screening which are fraught with intractable problems around meeting compliance obligations and reducing business risk exposure.

The quandary that many firms have faced over recent years is how to find the optimal balance between ensuring that the risk of doing business with an 'undesirable' entity is effectively mitigated, while simultaneously ensuring that resources are not overwhelmed with an inordinate burden resulting from 'overmatching'. This is achieved only in part through acquiring appropriate tools and putting systems in place to identify potential customer risk, whether it be PEP status, or any other proxy representing greater risk – the mechanics of how customer names are screened is equally important.

Such is the potential risk of transacting business with a sanctioned entity, directly in terms of penalties, and ultimately, in terms of reputational damage, the field of name screening technologies have long employed fuzzy matching techniques in order to identify inexact, but potential true matches between a customer and a watch list. Unfortunately, relatively short shrift has been given to the relevance and effectiveness of various fuzzy matching techniques. These methods can be broadly categorized as linguistic, e.g. phonetic algorithms such as Soundex and Metaphone, or etymological algorithms based on name morphology; or as mechanistic in computational 'string comparison' algorithms, such as those employing Levenshtein distance to quantify closeness of match. To complicate matters further hybrid



algorithms may contain elements of both types, and a host of ancillary matching criteria may be additionally applied to account for other name characteristics, such as name length, initials, foreign characters, and so on. Unfortunately, the appropriateness of using a particular algorithm for name comparison and matching are not well-understood, and have in some cases inadvertently contributed to excessive volumes of spurious results.

The optimal method for name matching should combine mechanical and linguistic elements. In general terms, linguistic content, from phonology to morphology, is embedded in a system, while the mechanics governing transformation or comparison function derivatively to the linguistic rules. Where name matching algorithms depend on an underlying linguistic substrate, it is still important to provide the flexibility to tailor the mechanical parameters in accordance with the characteristics of the names being matched, for example, names in a particular format or language.

In the context of a risk-based approach, striking the balance between the use of fuzzy name matching and the attendant burden of resolving false positive matches has lead to a one-dimensional 'single lever' model, as illustrated in figure 1 below:

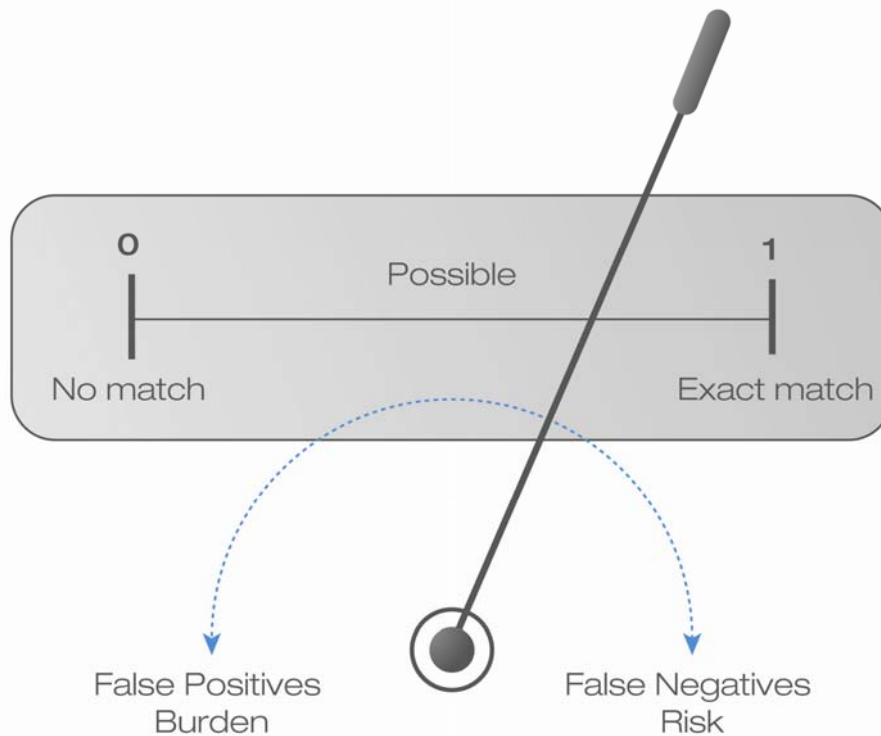


Figure 1 – Name Matching Single Lever Model



The binaries of 'no match' and 'exact match' are straightforward, but the continuum between the two poses several problems. Determining the optimal balance in this model is complicated by the need to distinguish between the quality or closeness of possible matches, and an array of other risk characteristics particular to the customer, product, transaction, or data being screened against, that discourage if not wholly undermine a one-size-fits-all configuration.

In contrast, a risk-based approach supports a departure from this formulation, and recognizes that resources should be deployed efficiently according to where risk resides. An enhanced name matching model should avoid a broad-brush methodology, either through the pre-processing or segmentation of customer data, or through the application of appropriate matching criteria in accordance with the perceived risk. This is illustrated in figure 2 below:

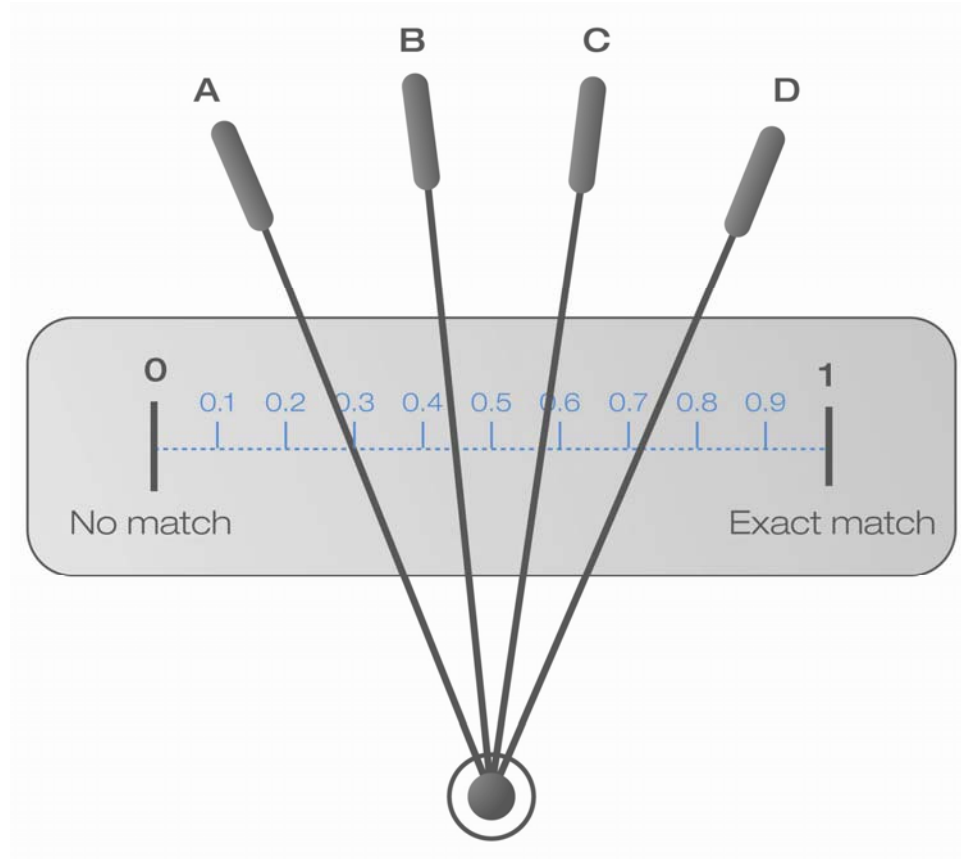


Figure 2 – Name Matching Multiple Lever Model

The range of settings from A-D addresses differences in the component characteristics of risk that may be present, a firm's own attitude to risk, or in the nature of data being screened against. Further, a discrete scale of 'possible' matches affords the opportunity to quantify the quality of match. Using a quantitative method, albeit arbitrary, to score matches brings additional definition to the process, and can reinforce the methodology applied in the subsequent handling and resolution of false-positive matches.

The presence of secondary identifiers can assist greatly in the resolution of possible matches, however, the availability of these data varies across data types. For example, date of birth is often present for individuals who are sanctioned against or wanted by law enforcement agencies, sometimes available for PEPs, and rarely present for regulatory enforcement data. Thus, the value of using secondary attributes in the matching process itself can only be realized where data are reasonably extensive. A prime example is nationality or country of residence, which by definition, is always available for PEPs.

Rather than facing the undesirable trade-off and consequences of too loose or too tight name matching, the multiple lever model in conjunction with secondary matching or filtering can have a significant impact in terms of distilling both the volume and quality of results sets. The reduction of noise is of particular importance in media searching, where the priority is to obtain manageable results of relevant content, as opposed to being inundated with undifferentiated voluminous content.

The dearth of information for some data types is in many cases the result of another key legislative consideration, that of data protection requirements. In order to overcome this constraint adjunct due diligence tools, such as media searching, can prove critical in garnering additional information that will help to resolve possible matches.

Taking a Risk-based Approach

The global regulatory climate is moving towards a more risk-based approach which is integral to a principles-based regulatory framework. This framework is one that is being reviewed by the more rules-based, prescriptive regulatory bodies as a superior way to managing risk in the financial services markets. Here, individual companies need to adopt appropriate positions on risk depending on:

- ▶ Company size and nature of business
- ▶ Composition of client base, region/jurisdiction
- ▶ Product and transaction characteristics

The effective management of risk across a broad client base is one that can only be handled by the sophistication of a technological solution embedding the capability to create a detailed workflow into the practices of KYC. Integration of additional risk data will assist in risk assessment for due diligence purposes, e.g. the use of Transparency International's Corruption Perception Index as a measure of jurisdiction risk. The adoption of the risk-based approach to screening applies the different variables identified above to the ongoing screening requirements as a way of managing sensibly the obligations inherent in the regulation. Whilst the traditional method has been to place the onus on manual checking of single names, this is no longer feasible with the extra regulatory obligations, where a firm could find itself swamped by the volume of checks that need to be performed on a continual basis. It therefore

behooves firms to use an end-to-end technological process of the various checks supported and managed by human skills. Here, technology is capable of assigning different flags for risk-rating the client base and altering the frequency, type and breadth of check that the organization determines according to its own risk appetite. Naturally, it is fanciful to think this process can be managed in a purely manual way. The cost of manual checking of this kind is prohibitive and the regulator will be looking at all times to ensure that there are demonstrably robust processes in place with the appropriate systems and controls for handling exceptions effectively.

Implementing a Connected Approach to Mitigate Risk

In order to fully integrate all the different independent checks into one solution, the firm must first make some important decisions with regard to its risk tolerance and threshold. The first objective is to understand the company's compliance and risk tolerance or, as expressed in the philosophical aphorism, to 'know thyself'. This involves identifying the specific areas of risk where the firm feels vulnerable and will be different for each organization. Secondly, the company must define the stages of company workflow, develop processes to accommodate all due diligence obligations and manage due diligence tasks with the best use of technology in order to:

- ▶ Reduce the reliance on manual intervention
- ▶ Simplify the audit process
- ▶ Improve efficiency and free up resources

Harnessing technology to bring together the different elements of KYC into a single solution avoids the risks of a disparate approach where due diligence processes may be connected within a process workflow but are performed by different individuals or roles. It further provides a platform where ongoing oversight is facilitated and any form of change can be identified and assessed in a timely fashion, and risk can be mitigated effectively.

With large volumes of dynamically changing data that must be continually monitored, screening solutions need to satisfy a number of criteria. In the first instance, in order to stay abreast of changes in watch lists, PEP status, or customer details, on an ongoing basis, screening tools need to alert users of any changes, rather than the burden lying with the user to monitor each and every change to data that could ultimately have an effect on risk exposure and meeting compliance obligations. As a by-product of a system monitoring over time, historical changes to data can be tracked rather than simply a snap shot of current status at a single point in time. This affords the opportunity to consider, for example, a sanction that has been repealed or enforcement that has expired, but which may still have a bearing on assessing the risk that a given entity may pose.

Meeting the Challenge

The challenges facing firms with respect to ever more demanding AML/CTF regimes are unprecedented; daunting as they may be they are not insurmountable nor unworkable when adopted within the context and framework of a proportionate risk-based approach.

Technology has become a key differentiator when defining and developing a workable process to meet the obligations of customer due diligence and satisfy the needs of the business. Many of the processes and checks can be integrated if you select the right provider to automate and understand the complexity of this process. It is less about the individual content and databases that are available to support the regulatory requirements and more about the connection of these data sets into a technological process providing a manageable number of exceptions that can be handled efficiently by suitably trained professionals in this area.