



“Politically Exposed Person”

Refining the PEP Definition

Edition II

White paper produced by World-Check, the market pioneer and industry standard for PEP screening and customer due diligence. World-Check provides risk intelligence to more than 2,700 financial institutions and government agencies in 153 countries.

Refining the PEP definition

Edition II

April 2008

Statement of Intent

The following paper intends to refine the existing accepted definition of what constitutes a Politically Exposed Person (PEP) within the increasingly complex regulatory compliance sphere.

It expounds on the “exposed persons” definition, *beyond* its primary regulatory context, and aims to serve as a reference framework for implementing an effective PEP risk mitigation strategy within the banking, legal, asset management, accounting and broader regulated industries.

Harnessing World-Check’s operational knowledge and PEP expertise, this paper highlights the origins of PEP compliance, as well as some of its key principles. It explores some of the key due diligence and risk mitigation processes involved, and examines areas of PEP regulation that pose present and future challenges for regulated businesses.

The role of research and technological innovation in meeting the future PEP compliance challenge is highlighted as well.

Contents	Page
“REFINING THE PEP DEFINITION”	1
1. Executive Overview	4
2. Refining and Expanding the PEP Concept	6
3. Key PEP Compliance Challenges	17
About World-Check	23

1. Executive Overview

The aim of this paper is to make a meaningful contribution to the existing body of knowledge about Politically Exposed Persons, or **PEPs**, for short. In refining and expanding the scope of the existing PEP definition, this paper will explore the operational implications of dealing with this heightened-risk category.

World-Check aims to provide an easily comprehensible yet authoritative definition that can serve as a benchmark for all industries having to comply with a PEP definition; most notably for service providers within the banking, legal, asset management, institutionalised lending and accounting sectors.

In terms of the implementation of an effective PEP risk mitigation strategy, this paper will equip institutions with valuable insight and a solid conceptual overview, whilst at the same time serving as a framework for a PEP risk mitigation strategy.

The Politically Exposed Person and your institution

During the last couple of decades, PEPs have become a profoundly misunderstood clientele of the broader financial community. Yet in principle, there is nothing wrong with doing business with a Politically Exposed Person, provided that a number of due diligence criteria are met on an ongoing basis. PEPs are by no means necessarily money launderers or embezzlers, nor automatically involved in corrupt financial practices.

What differentiates PEPs from other categories of financial clients is their position within a country or similar public structure, or their association with a political officeholder. It is not that PEPs are predisposed to committing financial crimes, but rather that their position, in relation to state funds and other 'cookie jar' opportunities, significantly heightens the risk that they may do something corrupt, fraudulent or otherwise illegal. Statistically and historically speaking, PEPs therefore pose an increased reputational risk to service providers in industries where a good name can be the difference between profitability and closure. A PEP's relative heightened-risk status, stemming from their position of influence within specific state structures (or their relationship to someone in such a position), is also largely influenced by the operational, financial, geopolitical and governance risks associated with their country of origin.

Against this backdrop, characterised by state-specific structural and governance nuances, effective risk mitigation and its underlying Client Due Diligence practices become a key consideration for service providers wishing to do business with this category of highly influential and often wealthy individuals.

This paper expounds on the "exposed persons" definition, beyond its primarily regulatory context, as it is seldom the primary officeholder that brings increased reputational risk; instead, it is with their associates, businesses partners and potentially shadowy middlemen that the real risk lies. As such, it must be noted up-front that an effective PEP risk mitigation solution should not merely provide a long list of officeholders' names and positions – in order to identify risk critically and methodically, it must also provide the identities of all those "exposed persons" that surround the PEP, and also qualify the exact nature and level of the risk involved.

If implemented correctly, the advantages of using this refined PEP definition in an institutional risk assessment framework are two-fold: It will assist your institution in mitigating its operational and reputational risk, based on internationally accepted best practice standards, whilst simultaneously meeting regulatory compliance standards routinely and cost-effectively.

The allure of the “Politically Exposed” client

PEPs are often high net-worth and prestigious individuals, and thus highly sought after as private clients. A “clean” PEP’s source of wealth, their position (or exposure to someone in a high position) and income-generating activities are transparent and able to withstand scrutiny. A “dirty” PEP, on the other hand, is a problem.

Dirty PEPs will go out of their way to conceal not only their identity, but the source of their wealth as well. It therefore comes as no surprise that PEPs often look to bank their money in countries other than their own. The most common forms of PEP concealment entails the use of a family member or associate through whom access to the banking system is gained, or alternatively, the formation of a company, trust, charity or similar financial or fiduciary vehicle to facilitate legitimate transactions.

As the financial community has become better at identifying PEPs and keeping the corrupt ones from accessing the financial system, so the trust and legal communities in particular have come to face an increased risk stemming from illicit PEP concealment practices.

What needs to be understood, however, is that PEPs are not automatically to be treated as “high risk”, but rather that they may potentially constitute a reputational risk.

At the heart of the PEP issue lies risk

PEPs constitute a reputational risk, rather than mere regulatory or non-compliance risk, as the scandal that sunk American bank Riggs illustrated. Once one of the United States’ financial flagship institutions, the bank paid the ultimate price for its inadequate due diligence processes.

Although regulation prescribing Enhanced Due Diligence (EDD) has been in place in industries such as the Swiss banking and financial sectors for many years, bankers were learning the hard and rather public way that bad guys with dirty money have lots to hide - namely not only their illicit funds, but their identities as well.

In many recent high-profile cases, it has been non-family members, including highly respected “advisors” and lawyers, accountants and diplomats who have, in most cases unwittingly, assisted in camouflaging and laundering dirty money. One of the most prominent examples of this trend is the case of former Zambian President Frederick Chiluba, where Meer Care & Desai, the law firm representing him, was implicated as well.

As regulation becomes more effective in closing the net on fraudsters, money launderers and other white-collar criminals, so the importance of those “exposed” to the political officeholder is becoming the subject of increased regulatory scrutiny. Without any doubt there have been bankers who have weighed the risk, considered the reward and decided to take a chance. Yet in many such cases, it is not simply that the “bad guy” is so clever, but rather that his banker is either so greedy, or under such pressure to meet targets, that leads to dubious accounts being opened.

Other lesser-known cases either affected fewer institutions, or did not quite capture the media’s attention in quite the same way a corrupt dictator or thieving strongman may have – but the risks involved are no less grave, and the dangers of PEP-related exposure remain high.

What we need to ask ourselves is: who will feature in the next front-page exposé? Whose hidden accounts will governments spend decades fighting over? Will it be Dos Santos of Angola or perhaps Fidel Castro of Cuba? Which institution will find its name and reputation tarnished; see its shares plummet or indeed have to find a buyer, as Riggs Bank did?

Have you truly understood your PEP screening requirements, identified your PEP risk, and set out to implement a PEP policy that will protect your institution, its reputation and indeed, your job?

This paper will help you gain a sound understanding of what PEPs are, why PEP screening is required and how to go about protecting your organisation’s reputation.

2. Refining and expanding the PEP concept

International consensus as to what constitutes a “Politically Exposed Person”, or PEP, is to a large extent informed by the Financial Action Task Force* (FATF) definition. Significantly, it has also been adopted by the International Monetary Fund (IMF), the World Bank and most other official regulatory authorities around the world.

As the key policy-making body in the sphere of Anti Money Laundering (AML) and Anti Terrorist Financing, FATF’s **40+9 Recommendations** are also widely accepted as the blueprint for most national legislation on these topics:

The FATF PEP definition:

“Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.”

FATF recommendation 6:

“Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

- a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.*
- b) Obtain senior management approval for establishing business relationships with such customers.”*

The accompanying interpretive Note to FATF Recommendation 6 states that: “Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.” Many different definitions and slight variations of the above are in use, yet a recent trend shows that certain national and regional definitions have become broader in their interpretation of what a PEP is.

In Mexico, for example, regulators go as far as to explicitly name specific governmental departments and public offices – including the titles of the respective officeholders – in their PEP definition and regulatory compliance requirements. In addition to earmarking shareholders, legal representatives, investors and executives of large institutions, the country’s PEP legislation includes officials holding relatively low-ranking positions, such as public office secretaries and departmental heads, circuit magistrates, magistrates and judges of the Community Forum and Federal Districts, and even agricultural attorneys.

But what exactly is PEP risk?

PEP risk is the very real possibility that over breakfast tomorrow morning, you will read that your bank holds the accounts of one of the world’s most corrupt leaders – and you had no idea, and you are being held responsible. It’s the risk of the bank’s shares dropping because of this news. It’s the risk of a court case filed by the major shareholders against the bank’s management for incompetence and failure to comply with legislation. It’s the risk of losing clients, losing millions of dollars, paying crippling fines and having all your correspondent banking relationships terminated.



In terms of board memberships and corporations, the following Mexican entities are also subject to PEP-related regulatory scrutiny.

Dialogue Coordination for negotiation with the Chiapas	Federal Mortgage Society
Housing National Commission	Rural Financial Society
Women's National Institute	National Commission of Water
National System for Families Growth & Development	National Fund for the Development of Tourism
National Council for the Arts & Culture	Forestry National Commission
Mexican Institute for Social Security	National Council for Science & Technology
Civil Servants' Institute for Social Services & Security	National Housing Funds Institute for Workers
Mexican Petroleum	National Institute for Statistics, Geography & IT
Federal Commission for Electricity	National Commission for the Development of Indigenous Populations
Central Light & Energy	National Commission for Sports
The National Bank for Foreign Commerce	National Lottery
National Financing	National Council for Life & Work Education
The National Bank for Construction & Public Services	Airports & Auxiliary Services
National Savings Bank & Financial Services	Federal Toll Roads and Bridges and related services
National Bank for the Armed Forces (Air & Ground)	Consumers Federal Attorney
Office for the Representation, Promotion and Social Integration of Incapacitated Persons.	

Financial institutions are required to identify and risk-screen "Politically Exposed" clients on account of their politically exposed relations or activities, whether they hold or previously held prominent social community positions, both within Mexico or outside the country's borders.

Why the need to refine the PEP definition?

From an operational perspective, the FATF definition lacks refinement in some areas, and is very much open to interpretation in others. We recognise that jurisdictions such as Mexico have introduced legislation which defines PEPs to a greater degree, and in some cases requires scrutiny of a far wider group of persons. In order to ensure effective risk mitigation for such jurisdictions, localised PEP risk considerations need to be taken into account.

The ever-changing nature of risk warrants ongoing review and refinement of risk-related definitions, and of risk mitigation thinking in itself. Although the FATF PEP definition remains the key point of reference, both in terms of meeting international regulatory standards, and in broadly defining internal PEP due diligence requirements, it should realistically be treated as a work in progress.

Until very recently, adhering to this definition was generally considered a solid foundation when structuring an internal framework for meeting regulatory obligations, but given the complex nuances that arise from state-specific legislation and the ever-changing face of financial crime, the FATF PEP definition is no longer enough to protect your organisation against reputation damage.

Consider, for example, the need for a UK law firm to act on behalf of a Mexican PEP-affiliated firm. Whilst such a dealing would fall outside of the UK definition, it is certainly subject to PEP regulation under Mexican law. What are the implications of this? What are the issues faced, and what specific risk mitigation measures should be taken by such a law firm?

The Financial Action Task Force was established by the G7 Summit held in Paris in 1989. It was set up in recognition of the threat posed to financial institutions and the banking system. Its primary areas of concern are combating money laundering and since 2001, terrorist financing. It currently has thirty-one member countries and two regional organisations.

Origins of PEP legislation

The PEP concept originated in the Swiss banking community, and has been relevant within this sphere for almost three decades, due to the high profile of many Swiss banking clients. The case of Ferdinand and Imelda Marcos – the infamous **“Steel Butterfly” and the Dictator**, and the millions in illicit funds they hid in Swiss bank accounts – highlighted the need for enhanced Client Due Diligence and ongoing transactional screening when dealing with senior politicians, their associates and families as clients.

During the Marcos family’s 20-year political reign in the Philippines, this government was robbed of hundreds of millions of dollars. In late 1997, Switzerland’s highest court ordered that more than \$500 million held in Swiss bank accounts should be returned to the Philippines.

The successive international press headlines and negative publicity severely tarnished the reputations of the Swiss banks involved, and compelled the community as a whole to critically reconsider the way they approach Client Due Diligence; a process that gave rise to what today is referred to as **PEP Due Diligence**.

Some recent PEP cases

We have in the last few years publicly witnessed the damage a badly managed PEP relationship or policy (or indeed lack thereof) can cause. The highest profile PEP case was **Riggs Bank**, which banked both General Augusta Pinochet (and tried to conceal this relationship), and Equatorial Guinea’s long-term president, Brigadier General Teodoro Obiang Nguema Mbasogo.

Prior to its fall from grace, Riggs boasted a near-exclusive franchise on private banking with Washington DC’s Diplomatic Community, and a significant percentage of London’s diplomats. After more than 160 years as the most prestigious private bank in the United States of America, Riggs saw things fall apart in the last three years of its existence. The cost of non-compliance at Riggs can be set in the region of \$200 million. This included fines and shareholder settlements of approximately \$59 million, and legal and consulting fees of approximately \$35 million.

Yet ultimately, the clearest indicator of lost reputation was arguably the loss in Riggs’ share value. On 15 June 2004, Riggs accepted an offer by PNC of \$24.25 per share. On 10 February 2005, the bank accepted a renegotiated price of \$20 per share – a drop of 20% in just of 8 months.

Indeed this disastrous end to what was a highly respected institution cannot solely be put down to a bad PEP relationship or two, but is rather attributable to the lack of a sound compliance culture. The bank was at no time unaware of whom they were dealing with, but rather paid the price for how they chose to deal with such matters and Politically Exposed clients in general.

Trusts and PEP risk

Trusts and PEP identity concealment is another high-risk area. It must be stressed that it is not exclusively offshore vehicles that are used to conceal the identities and questionable wealth of PEPs. Further to this, there is a false sense of security when carrying out due diligence on or dealing with an onshore company, trust, foundation or charity, in comparison to the equivalent offshore vehicles.

The registration of a company in most *onshore* jurisdictions carries little or no KYC requirements on the beneficiaries, owners or company directors. The knowledge that a company is registered in the United Kingdom, the United States or in the EU, as opposed to some small tax haven island nation, for some reason would appear to make us think it must be above board.

Many trusts are formed for legitimate personal or business purposes. They are formed for everyday legitimate purposes such as inheritance management, succession planning and the education of minors. Trusts also play a major role in commercial transactions such as securitisations, and in socially beneficial areas such as pension schemes, employee benefit schemes and legitimate charities.

Generally speaking, such legitimate uses of trusts pose little risk of money laundering. It should, however, be noted that in 2001 the FATF typologies report stated that: "Trusts, along with other forms of corporate entities are increasingly perceived as an important element of large-scale or complex money laundering schemes."

Whether onshore or offshore, trusts can provide a valuable tool for the money launderer and corrupt PEP alike. The establishment of a trust will always increase the challenge for the authorities of identifying the beneficial owner of the funds or assets settled into trust. If the trust is established in a poorly regulated jurisdiction, which has strict confidentiality laws, anonymity can be virtually assured. Where there is such a lack of transparency within a trust, this will provide a significant advantage to the money launderer.

PEPs and Corruption

The Jersey Financial Services Commission's newly published AML handbook (published February 4th 2008) includes the following statement:

"Corruption inevitably involves serious crime, such as theft or fraud, and is of global concern. The proceeds of such corruption are often transferred to other jurisdictions and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates.

By their very nature, money laundering investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both businesses and jurisdictions concerned. This is in addition to the possibility of criminal charges.

Indications that an applicant or customer may be connected with corruption include excessive revenue from "commissions" or "consultancy fees" or involvement in contracts at inflated prices, where unexplained "commissions" or other charges are paid to third parties.

The risk of handling the proceeds of corruption, or becoming engaged in an arrangement that is designed to facilitate corruption, is greatly increased where the arrangement involves a PEP. Where the PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

PEP status itself does not, of course, incriminate individuals or entities. It will, however put an applicant for business or customer into a higher risk category."

The PEP phenomenon actually poses two groups of risk from the viewpoint of corruption.

Firstly, Exposed Person A, possibly a very senior executive of a very prominent company, is an “EP” paying bribes or making corrupt payments. Such payments are laundered through company and trust structures.

Secondly, the PEP receiving such payments has to launder them into bank accounts, investments, etc., a process which again takes place through company/trust structures which disguise beneficial ownership.

The following hypothetical example illustrates this structural vulnerability: Funds were used to buy political influence and win contracts from foreign governments. Funds were transferred to this Vice President on behalf of the company via an offshore trust structure. Activities across the bank accounts controlled by the VP included frequent and often unusually large cash withdrawals. In one six-week period, more than \$35 million had been withdrawn in cash.

The beneficial recipients of payments from the VP were several PEPs and their associate.

PEPs and false invoicing

What are the legal consequences of the following scenario?

A person is employed as your agent. The agent's duties include the arrangement of services to be performed for you by a third party. The agent induces the third party to pay him a bribe so that he awards the third party the contract for services. The bribe is paid from the inflated price that you are charged by the third party.

This scenario is, in essence, what happened in Daraydan Holdings & Ors vs. Solland International Limited & Ors. The case was concerned with an allegation of bribes or secret commissions.

Sheikh Mohammed, the third claimant, was the equivalent to the Deputy Prime Minister of Qatar and was Special Adviser to his brother, the Emir of Qatar. The other claimants were corporate vehicles for the holding of his property interests in England. Khalid, the fifth defendant, extracted approximately £1.8 million from Mr and Mrs Solland and their companies (the first to fourth defendants) between 1997 and 2001. This amount represented a 10% commission on receipts from contracts with the claimants for the luxurious refurbishment of properties in London and Qatar. The sixth and seventh defendants were Khalid's sister and nephew respectively.

The claimants comprise Sheikh Mohammed, the deputy prime minister of Qatar, and his companies hired Mr Khalid to look after their property interests in this country. The Solland's ran a design and refurbishment company and, through Mr Khalid, won the contracts on the basis that they added 10% to their prices and then paid this additional sum to Mr Khalid.

Needless to say, the Sheikh knew nothing of these arrangements and only became aware of them in 2002 when they were disclosed by another party. The sheikh immediately terminated existing relations with the Solland's and Mr Khalid, and issued proceedings to recover all the overpayments.

An employee or agent who accepts a bribe is liable, if caught, to account to his employer for everything he has received. In addition, the payer of the bribe is liable to the employer for the same sums and, as it is to be assumed that the true price of the goods or services supplied has increased by the amount of the bribe, it is no defence to claim that the employer has suffered no loss or there was no corrupt intention.

The claim against the Sollands was settled following the trial, presumably on onerous terms for the Sollands. The judgment deals with the case against Mr Khalid, and concludes that Mr Khalid was fraudulently misappropriating 10% of the sums paid and, most importantly, that the claimants had a right of priority over any other creditor of Mr Khalid in relation to recovering these payments. Worldwide orders had been obtained freezing various bank accounts into which these payments had been diverted and the claimants can now recover all these monies ahead of any other creditor.

This case illustrates how seriously English law treats all those involved in corruption, and it should serve as a deterrent to anyone seeking to use secret payments to obtain business.

PEPs and Money Laundering

The vulnerability of trusts and similar financial vehicles cannot be examined without the focus also shifting to money laundering. The term is itself a bit of a misnomer; but in order to accurately describe money laundering, it is important to initially examine what it is *not*:

Money laundering is not an activity that exclusively involves actual money; any form of asset or property that is derived in whole or in part from criminal activities, whether directly or indirectly. The term “laundering” encourages the perception that it is a form of process by which criminals seek to wash or clean their criminal property, so as to alter its form or appearance. The common perception is that money launderers seek to achieve this by utilising a number of different types of products, services, currency and jurisdictions, yet this is not always the case.

Consider the following hypothetical example: In 1999 a lawyer acting on behalf of a corrupt PEP settled a luxury penthouse apartment, previously purchased with the proceeds of crime, into a trust. This trust is administered by a trust company service provider. The property has remained in the trust for nearly a decade.

Is the trust company laundering the property? The answer is yes, despite the fact that the trust company has not changed or converted the property or disguised it in any way.

The common perception is that criminals, including corrupt PEPs, have as their money laundering objectives the avoidance of detection, prosecution and the confiscation of their criminal proceeds. Whilst this is often the case, there have also been numerous cases where PEPs and criminals have sought not to convert their properties, but rather to disguise the fact that they own these assets.

To achieve this objective, such criminals PEPs or the entities acting on their behalf attempt to camouflage or sever the connection between themselves and any property that could link them to criminal activities. Money laundering is therefore as much about disguising ownership of property as it is about converting or “washing” criminally obtained or funded property.

Jack Abramoff, former Republican “superlobbyist” and now-convicted felon, collected tens of millions extorted from Indian tribal gambling operations. Abramoff allegedly used auspiciously named non-profit, 501(c) (4) lobbying organisations such as Americans for Tax Reform and Citizens Against Government Waste as a front group for corporate interests.

These fronts were used as a conduit for receiving large fees and donations, much of which was use to buy influence from Washington Republican figures, but a considerable amount was also used for self-enrichment and personal projects. He pleaded guilty to conspiracy to corrupt public officials, defrauding clients and tax evasion charges, and was sentenced to 5 years and 10 months in prison.

Another paradigmatic case of **PEP concealment** centered on Paulo Maluf, a Brazilian Federal Deputy Member of the Chamber of Deputies representing São Paulo State (1982 -1986; 2007 – 2011).

During 2001 authorities requested the freezing of Maluf's account with Citibank, after \$200m, allegedly looted from Brazil, turned up in the Brazilian congressman's account at Citibank's Jersey branch. Although there was no suggestion of dishonesty on Citibank's part, the scandal nonetheless tarnished the institution's reputation.

Records of frozen bank accounts obtained from Swiss authorities suggested that 30 company Swiss bank accounts were linked to his family members. It also came to light that Blue Diamond, one of his companies, had opened an account in July 1985 in the Cayman Islands, before changing its name to Red Ruby in June 1994. The company account was then transferred to Jersey in Jan 1997, effectively camouflaging its connection with Maluf.

In 2005, Maluf and his son Flavio spent 40 days in prison on charges of tax evasion and money laundering, but local court decided to release the politician, who is in his seventies, because of his fragile health. Despite having been indicted for crimes ranging from tax evasion and embezzlement to passive corruption and money laundering, he had still not been prosecuted by January 2007, as his position entitles him to political immunity.

PEP risk and trusts

As far as trusts are concerned, we have an array of examples of well-known PEPs registering and indeed using such vehicles to manage their wealth:

Diepreye Solomon Peter, former governor of Bayelsa State, Nigeria, is a UK-based PEP associated with approximately 18 financial vehicles and other legal entities. He pleaded guilty to six counts of corruption during July 2007, and was also convicted of six counts of fraud and false declaration of assets. Peter also admitted to establishing the Salo Trust (also known as Falcon Flight) in the Bahamas – in the names of his spouse and children. He was subsequently ordered to forfeit €5.76m properties and cash worth several million euro, and served six two-year sentences concurrently. He has subsequently been released.

Similarly, Uri David, a PEP and convicted money launderer associated with the late Sani Abacha of Nigeria, is also based in London. From a compliance perspective, this effectively means that PEPs deserve meticulous scrutiny – **regardless of whether they are of foreign origin or not.**

A handful of trusts and corporations can be linked to payments made to the European bank accounts of Vladimiro Illich Lenin Montesinos Torres (known to most of us as **Vladimir Montesinos**), former Presidential Advisor and Chief of the Peruvian National Intelligence Service (SIN) under Alberto Fujimori, who himself was recently extradited to Peru from Chile and sentenced to 6 years' imprisonment on charges of usurpation of functions.

The registration of a company in most *onshore* jurisdictions carries little or no KYC requirements on the beneficiaries, owners or company directors. The knowledge that a company is registered in the United Kingdom, the United States or in the EU as opposed to some small tax haven island nation, for some reason, would appear to make us think it must be above board; *think again and be forewarned.*

PEP risk and dealing with law firms

Financial institutions such as banks face reputational risk from dealing not only with PEPs, but also from dealing with law firms and solicitors *acting on behalf of PEPs*. Classically, large law firms are exposed to PEP risk during their dealings with State-owned corporates, as these are Politically Exposed themselves.

PEP Due Diligence when dealing with corporates is not to be taken lightly. Energem's recent listing on London's Alternative Investment Market as a renewable energy business provides a classic example of the secondary PEP risk law firms face. This corporate was able to withstand regulatory scrutiny regarding its reported involvement in illegal diamond trading in Africa during the Nineties, and as such is not considered a "PEP corporate" – yet several of its directors are PEPs.

There are some who believe that dealing with lawyers insulates them from intense regulatory scrutiny because of client attorney privileges, yet client attorney privilege applies when a lawyer is defending a client in a court of law. Client attorney privilege does *not*, however, apply when a lawyer is providing advice to client. Indeed, if a law firm is establishing structures to hide and mask proceeds of crime on behalf of a client, then it can be considered a legal accomplice to criminality.

Banks beware

Should it come to light that a law firm was making their bank accounts available during the early placement stages of money laundering by accepting stolen state funds from a corrupt former dictator, for example, this could also harm the reputation of the financial institution where the law firm's account is held.

During 2007 MEER CARE & DESAI, a UK-based law firm that acted on behalf of former Zambian President Frederick Chiluba, was found guilty of playing an instrumental role in the channeling of a portion of the £23 million this former head of state stole from the Zambian Government. The High Court Judge described their actions as "classic blind-eye dishonesty." This indictment undoubtedly tarnished the firm's ethical standing.

In industries where service providers trade on their reputation, keeping a good name intact is critical. The above example illustrates why World-Check has always advocated that legal entities be given PEP status.

It is also the very reason these have consistently been included in our risk database. Given this context and the high potential cost of not staying two steps ahead of persons with unscrupulous intentions, World-Check also endeavours to identify new heightened-risk categories before they become compromised, and to approach the gathering of risk intelligence in a proactive fashion.

PEP status: visibility vs. seniority

One of the most crucial areas in the definition of the PEP concept, and one most open to local interpretation, is the extent to which low-ranking officials and public officeholders should be included. The FATF definition focuses predominantly on senior officials or officeholders – yet where does “senior” become “middle ranking” or “more junior”? *Where does “important” become “unimportant” and, indeed, to whom?*

The Wolfsberg Group, an association of 12 leading global banks, provides the following alternative definition: “The term [PEP] should be understood to include persons whose current or former position can attract publicity beyond the borders of the country concerned and whose financial circumstances may be the subject of additional public interest.” This might be interpreted to include senior, prominent and/or important figures who ‘attract publicity’ outside of their own country – regardless of their seniority.

Not just politicians.

The following points serve to clarify what World-Check undertakes to correlate, and what we consider to be a Politically Exposed Person.

All senior political and government leaders and functionaries including:

Heads of State ranging from Royals to Presidents and Prime Ministers Government Ministers and Deputy Ministers, as well as:

- **Political Party Leadership**
- **All Members of Parliament/Senate**
- **Key Senior Government Functionaries**
 - **Judiciary**
 - **Legislature**
- **Senior Military Officers**
- **Ambassadors**
- **Key leaders of state-owned enterprises**
- **Heads of government agencies**
- **Private companies, trusts or foundations owned or co-owned by PEPs, whether directly or indirectly.**

This effectively covers the *Political* aspects of the PEP definition; yet the *Exposed Persons* aspect warrants more elaborate scrutiny and more rigorous defining.

Separating the 'P' from the 'EPs'

For the purposes of illustration, individuals whose association to "Politically Exposed Persons", and whose business/political interests and transactional activities constitute a potential risk in terms of AML, AFT and other compliance requirements as prescribed to regulated financial service providers, will be referred to as "exposed persons".

Business relationships with family members or associates of public officeholders often involve reputational risks similar to or indeed higher than those associated with "primary" PEPs themselves.

A key misconception is that PEP checking involves identifying all senior political or government officeholders only. FATF, however, clearly defines the 'P' in PEPs as being 'senior' and the "definition is not intended to cover middle ranking or more junior individuals." Of course, the 'P' stands for more than politicians and government functionaries. However, databases of tens of thousands of Russian, Mexican, Indian or Chinese middle and low-ranking bureaucrats for example, can be of little or no value, go far beyond what international guidelines and common sense require, and end up becoming an administration nightmare.

It is at this point where the 'EPs' in the PEP concept gain major significance: Family members, close associates and the personal advisors of the political officeholder can all be classified as exposed, based on their relation to the primary PEP.

Experience has shown that the likelihood of a questionable politician with something to hide sending his or her close family down to stand in the account opening queue at a bank is very rare. Senior government officials robbing their country of millions will seldom put their spouse or children directly at risk. Nor would it make sense, if the goal is to hide one's identity, to send someone to the bank called Charles Taylor Jnr in the foolish hope that no one picks up on the name or questions the millions being transferred in haste from Liberia.

Since this is unlikely to happen, how do PEPs go about opening accounts?

The real risky PEPs are the suits, the middlemen and "advisors" – the men and women who stand in the shadows, broker the deals, know all the secrets, and are almost always the ones involved in account openings. The clever ones will bring a few respectable lawyers and/or diplomats along to put on a good show and create an air of legitimacy. These people are the PEPs you really need to look out for. In fact, the political figure is arguably the last person you need to watch out for.

Natwar Singh, a very senior Indian politician who was implicated in the infamous oil-for-food scandal, is a case in point. "His" assets were allegedly found to have been placed on the names of his wife's family members and his son's friends.

Over the last number of years, the pedigrees that some of these individuals hold have been nothing short of astounding. From diplomatic passports to UNESCO ambassadorships, the middlemen always cloak themselves in respectability. These PEPs can walk the walk and talk the talk. They have answered prying questions a hundred times over, and are well practiced in the process – after all, these are the kinds of individuals who negotiate billion dollar contracts. Don't believe they don't know how to handle a basic account opening procedure.

How does one define "PEP family"?

PEP family members, as Exposed Persons or EPs, can include close family members such as spouses, siblings, children, cousins and parents, and may also include other relatives and relatives by marriage. Individuals who may benefit from being associated to such "EPs" may therefore arguably also warrant scrutiny as Exposed Persons.

Defining "close association"

Close associates may include personal advisors/consultants, colleagues or the Politically Exposed Person's fellow shareholders and any persons who could potentially benefit significantly from close business associations with the PEP. In a document entitled "*Prevention of money laundering/combating terrorist financing – Guidance for the UK financial sector – Part 1*", published in December 2007 the UK's Joint Money Laundering Steering Group prescribes enhanced due diligence for "individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights, even where these interests are held indirectly.

Following the assessment of the money laundering or terrorist financing risk presented by the prospective customer, appropriate risk-based measures should be taken to verify his or her identity.

Identifying these most risky frontmen takes years of piecing together the global puzzle of relationship networks. There are no magical sources or websites that list them, yet the same names come up time and again. Each region has its handful of untouchables, and it is with these "Exposed Persons" where your real PEP risk lies.

PEPs: More than just "persons"

A major misconception regarding PEPs is that one should only be concerned about individuals when identifying PEP risk. A FATF consultation paper issued in 2002, however, indicates that "the proceeds of corruption are typically transferred to a number of foreign jurisdictions and concealed through private companies, trusts or foundations."

It is quite common for PEPs to camouflage their financial interests using legal entities, and there exists a very real possibility that you are already most likely doing business with PEPs via a legal entity.

Beyond the normal category-related indicators such as rank, position or office, many of primary **PEP risk indicators are transactional** – and these almost invariably point to entities such as the ones mentioned above. From a compliance solution perspective, it is key to be able to identify associations between legal entities such as trusts and the persons exploiting these vehicles.

Just follow the money.

By rigorously monitoring PEPs' transactions on an ongoing basis, financial institutions can ascertain whether illicit funds are being laundered, how embezzled funds are camouflaged, or what siphoned funds from state or Non Government Organisations (NGO) funds are used for. The list of purposes includes, but is not limited to, the funding of terrorism, corruption, the paying of bribes and international organised crime.

How long does a PEP remain a PEP?

At present, there is no industry-wide consensus as to how long a PEP should remain a PEP, as former PEPs can benefit from their former position for years after leaving office. The critical question is: ***How long, then, should PEP status remain effective for?***

And, if a new period is agreed upon in terms of those that hold political office, what are the implications for those "exposed" to the officeholder? The EU Third Money Laundering Directive also states that consideration should be given to the timeframe within which a person having held a public function should be considered a PEP, but makes no mention of how or even if the same is true for family, friends and business associates.

World-Check is of the view that PEPs in most countries maintain a position of influence long after leaving office and certainly for considerably longer than one year.

Corruption or the benefits of a corrupt past will become more apparent with time. As such, there should be no time limit on the scrutiny of the finances of former dictators, presidents or strongmen. It is perhaps for this reason that few definitions provide any PEP “expiry date”. The same would apply to high-level offspring of PEPs, given the negative publicity the likes of Mark Thatcher and Tommy Suharto have received.

Yet realistically, should Tony and Cherie Blair’s children Leo and Kathryn be treated as posing a heightened PEP risk?

In the interest of fairness and privacy – if nothing else – there is nonetheless a case to be made that the PEP burden should be lifted from the families and business associates of PEPs with a lower public profile. Although such PEP status indemnity could not be implemented across the board, it is certainly something that should be considered if the PEP definition is to remain focused and relevant in future. This is an evolving issue and one that needs to be addressed certainly to be ‘fair and just’ to family members and business associates who are only exposed and not officeholders *per se*.

3. Key PEP compliance challenges

If regulated service providers draw the net too widely, their compliance department and infrastructure becomes overloaded, yet if they subscribe to too “narrow” a PEP definition, the likelihood of a high-risk person or a dubious transaction going undetected is substantially increased.

In meeting regulatory compliance obligations, 21st century financial service providers face mounting challenges pertaining to the following:

- **Human resource allocation**
If conducted in-house, due diligence research places a substantial burden on key resources within an organisation. Given the sheer number of customer checks required on a routine basis, manual customer screening is simply not feasible.
- **Proliferating compliance legislation**
Staying abreast of new and emerging regulatory regulation is a full-time job. Identifying and interpreting new regulatory laws can be a cumbersome task, and one not undertaken lightly, given the stiff fines imposed for non-compliance.
- **Escalating compliance costs**
Driven by increasingly stringent regulations, initial Customer Due Diligence and Enhanced Due Diligence (EDD) requirements for PEPs, the increased burden on compliance departments inevitably lead to higher operational costs.
- **The need to provide auditable proof of due diligence**
The increasing regulatory demand for electronically verifiable proof of due diligence activities comes as a final nail in the coffin of manual account and transactional screening. As such, overcoming the technical aspects of compliance constitutes a make-or-break challenge for the future prosperity of financial service providers.

The importance of effective PEP Due Diligence

PEP due diligence has far less to do with PEP identification than it has to do with risk detection. A database that merely confirms that an individual is a PEP is of little value to financial institutions. What institutions require is much more than that, it's the information on the associates, middlemen, relatives, companies and trusts that often reveal the level of risk, for it is through these vehicles that a 'bad' PEP will carry out the illicit activities. Remember there are many honest PEPs that you would want to have as customers, what is key when it comes to PEP due diligence, is having precise risk-relevant information that will allow you to measure your risk exposure and help you make the right decisions.

Therefore, in order to be able to mitigate PEP risk, you require more than just PEP identification data; you require information that is risk-relevant: In simple terms, a database that confirms that Mr A and Mr B are both political officeholders, but fails to mention which of these two gentlemen is currently under investigation for bribery and corruption, is useless to you. The value of PEP due diligence lies in identifying the risk of bribery and corruption; not in confirming that an individual exists.

A true PEP solution, unlike a "Who's Who" Directory, will tell you that Mr A's brother-in-law is an arms dealer, and Mr B's wife is the arms dealer's sister. It will tell you behind which company Mr. A's brother-in-law is hiding his activities, and that Mr. B is not only a board member and trustee of this company, but also a convicted trafficker of narcotics. This amounts to relevant PEP risk intelligence, which makes for effective due diligence.

A copy of a passport and 10 ticked boxes won't suffice – *and it certainly won't get your organisation off the hook with the regulator when things go wrong*. No bank would look forward to appearing on the front page of the Financial Times or the Wall Street Journal in relation to an account that holds the ill-gotten gains of a corrupt, senior government official. In fact, banks will and do go to great lengths to ensure they stay out of the media when the news could damage their reputation. Millions of dollars are spent each year in ensuring that society, your customers and peers perceive your institution in a favourable light. Free press that comes with doing business with the 'bad guys' is not what your Directors had in mind.

"Sleeper PEPs" and elections

Between 2005 and 2007 alone, approximately 318 general and by-elections were held worldwide – that's more than 9 elections per month (source: www.electionguide.org).

There exists a very real possibility that one of your institution's existing customers will be elected – and hence become a PEP – without you even knowing it.

It is for this very reason that regular PEP screening of your entire customer base is recommended as best practice. Routine re-filtering against an up-to-date database featuring newly-elected officeholders will uncover "sleeper PEPs", and is critical for your organisation's ongoing risk mitigation. The success in avoiding risk lies as much in thoroughness and research consistency as it does in the ability to filter transactions and clients on an ongoing basis.

Addressing the compliance challenge

In order for a compliance strategy to remain sufficient, both in terms of current and future regulatory mandates and effective risk management, it needs to be risk-based, and remain ahead of the curve – on all fronts, and at all times.

In order for a regulatory compliance solution to fully address the PEP challenge, several conditions have to be met:

1. Adherence to an evolving PEP definition

Given the fact that new PEP definitions continually emerge as more and more money laundering loopholes are found and exploited, it would be realistic to assume that the existing legislation and official PEP definition is presently outdated, and becoming more so with every passing day.

Considering the fact that official definitions and legislation are not updated regularly, there exists the real possibility of dangerous PEPs slipping through the cracks and harming your institution's reputation, if it merely conforms to currently prescribed definitions. As such, using an evolving PEP definition in creating your organisation's compliance framework, is critical.

2. Robust name and PEP-related risk factor matching mechanisms

Mitigating your organisation's PEP risk requires a combination of highly structured risk-relevant data, a comprehensive PEP definition and identity matching mechanisms that connect the dots, taking linguistic, regional naming conventions, associations and aliases into account. An effective system should produce as low a percentage of false positives or inaccurate false alarm matches as possible.

3. Routine client and transactional filtering

Given the fact that persons become "politically exposed" on a daily basis, and that questionable transactions can take place at any moment, a robust technological infrastructure is required in order to conduct regular client screenings swiftly and accurately.

4. Access to authoritative global PEP database

Given the fact that PEPs are often foreign nationals, a comprehensive PEP compliance solution would require a risk intelligence database that:

- A) Is global in its scope
- B) Is updated in real-time on a 24/7 basis
- C) Allows for the automated screening of an entire client base. (Only a meticulously structured database where not a comma, letter or full stop is out of place, will allow for a seamless integration in an automated environment).

5. Electronically verifiable proof of due diligence

Whilst protecting the reputation and integrity of your institution is the most important consideration when tackling PEPs, their identification and monitoring is also a regulatory requirement and hence being able to produce proof of your best due-diligence efforts is of utmost importance. Increasingly regulatory bodies are demanding that financial institutions provide **electronically auditable proof of diligence**.

PEP compliance check-list

With all the pitfalls how does one still do business with PEPs?

- Ensure you carry out KYC and Enhanced Due Diligence on companies, foundations, charities and trusts in the way you do with individuals.
- Treat onshore and offshore vehicles in the same manner.
- Having identified a PEP, assess your risk in dealing with this person. Consider the country and its government, the person's position and their potential exposure to corruption and bribery. Understand the PEP's business requirements of your institution.
- Carry out regular reviews of all customers and even more regular reviews of all PEPs.
- Understand that it might be an 'Exposed Person' you are looking for and not an actual 'office holder'.
- Ensure you are fully aware of and have carried out KYC on all signatories on all accounts but especially PEP accounts.
- Ensure you have carried out KYC on all credit card and additional credit card holders.
- Have a well thought-out and even better executed KYC and PEP policy and culture throughout your organisation.
- No single person in your organisation should have total control over PEP customers or PEP matters. Ensure counter-signatories on everything PEP related.

And finally, plan ahead for the end of a PEP relationship. Realise that PEPs have a hidden 'expiration date' that will not be evident to you or even to themselves. A PEP can go from good guy to bad guy in a day and you don't want to be the last one standing behind the throne of a disposed leader.

Maintaining a benchmark KYC and PEP intelligence solution

What sets World-Check's PEP intelligence apart?

Flexible data scaling

In response to the market demand for an effective and comprehensive solution, World-Check set out to expand the PEP definition, beyond the accepted regulatory requirements, in order to cover a far more comprehensive range of heightened-risk persons, entities and related risk variables. World-Check's data is structured with this objective in mind.

There are many so-called "risk mitigation" solutions available on the market, most of which merely identify PEPs based on a list of high-level political positions as per the FATF definition. The obvious problem is that this identification fails to cover other critical aspects and hence does little to reveal associative risks. This leaves financial institutions with the burden of manually identifying actual risk in the form of political scandals, indictments, high-risk relationships and associations, compromising business interests, etc.

World-Check's intelligence aids institutions in meeting their regulatory requirements, and profiles are structured to support specific screening processes and applications. This ensures maximum risk mitigation, whilst minimising the administrative burden on the client organisation.

Featuring robust historical data mining capabilities and a **graphic relationship display functionality** that highlights the less-than-obvious associations a PEP may wish to conceal, World-Check doesn't merely confirm PEP status, *it identifies PEP risk*. Using the refined PEP definition as a framework, World-Check's database can be scaled and adjusted to support specific screening requirements.

Customisable risk weighting is a key requirement to closing industry-specific PEP risk loopholes. World-Check addresses this need through a combination of fields and values to cover 24 primary risk categories. The following is an example of the Primary Category variables pertinent to banks, among others:

Primary Category: Crime

- **Sub-category: All PEP-risk related entities are assigned a PEP value (not only Senior Political Figures, as per the refined definition outlined in this paper)**
- **Official Lists – OFAC, FBI, USDOJ and so forth**
- **Aliases**
- **Position**
- **Country**
- **Locations**
- **Companies Reported (linked profiles)**
- **Associates (linked profiles)**
- **Synopsis, Structural – Sanctions, Funding (terrorism related)**
- **Synopsis, keyword – World-Check uses standardised wording**
- **Information sources**
- **Updated – date of the last profile update**

The Human Research Factor

Correlating open-source intelligence on PEPs is a complex task that requires dedicated teams of multi-lingual researchers, pouring over millions of pieces of data, day in and day out. For the past seven years our teams have been methodically monitoring hundreds of thousands of individuals as well as their companies. We have spent tens of thousands of man-hours hunting for key PEP risk information and it may take years to finally be able to join several dots.

Substantial and ongoing investment in research capacity has contributed to World-Check's leading position as global risk intelligence provider. World-Checks team of expert multi-lingual researchers gather open-source information on high-risk entities around the world in 28 different languages including Arabic, Tajik, Russian, Tamil, Turkish, Korean, Polish and Chinese.

Understanding how much your chosen PEP data vendor has invested in staff and technology, not just in the creation of the database, but in its ongoing maintenance, is by far the best test for measuring the quality of the information in the database.

No PEP risk intelligence, of any real value, comes quickly or easily or can be uncovered by part-time, outsourced or untrained labour. This is not about building the biggest database; it's about uncovering the underlying risk and maintaining the quality and relevance of the data. Finding the hidden relationships and gathering the pieces of this global PEP network puzzle takes resource commitment and dedication that borders on addiction.

Real-time database updates

World-Check's database, containing hundreds of thousands of high-risk profiles, is updated on a real-time, 24/7 basis. Tens of thousands of new profiles are created each month, whilst similar numbers of profiles are updated on a monthly basis as new risk information becomes available in the public domain.

Committed to meeting risk mitigation requirements

World-Check remains committed to perpetually expanding and refining the PEP definition in support of financial institutions' risk mitigation efforts – especially with regards to local legislative requirements. We continue strengthening our efforts to educate compliance practitioners worldwide about the origins and operational implications of PEP compliance, and collaborate with regulatory and law enforcement agencies around the world to grow the body of knowledge on PEPs.

Our ultimate goal is to create a sustainable PEP compliance solution for all regulated industries, taking changes in the legislative landscape and emerging institutional risk mitigation needs in mind.

It is World-Check's belief that the greatest risk in dealing with PEPs lies not so much with politicians who readily identify themselves but more so with those that choose to use intermediaries (the EPs) and corporate structures to conceal their ill-gotten gains. Not only is this industry in constant evolution but the content we correlate and the people and entities we track are "moving targets". As such, in-house research practices are aligned to meet the standards to which our clients are held accountable, and research outputs are structured with international and country-specific PEP requirements in mind.

About World-Check

World-Check provides its global open source intelligence database to more than 2,500 institutions in 135 countries, including 47 of the world's 50 largest financial institutions, and more than 200 enforcement and regulatory agencies in over 90 countries. Widely regarded as the global leader in risk intelligence, it was originally created to meet the compliance requirements of the Swiss banking community.

Our database and tools find direct application in financial compliance, Anti Money Laundering (AML), Know Your Customer (KYC), PEP screening, enhanced due diligence (EDD), fraud prevention, government intelligence and other identity authentication, employee background screening and risk-prevention practices.

“Significantly, we serve more institutions than all other PEP data providers combined.”

The World-Check database comprises hundreds of thousands of heightened-risk profiles, including money launderers, fraudsters, terrorists and sanctioned entities, as well as individuals and businesses from more than a dozen other high-risk categories.

In addition, World-Check also tracks PEPs, their family members as well as their potentially risky associations. Leveraging highly intuitive research and data mining capabilities, World-Check highlights not only risky persons, but the companies and organisations associated with them as well.

World-Check offers a downloadable database for the automated screening of entire customer bases, as well as a simple online service for quick customer screening.

The sheer number of risk mitigation success stories bear testimony to the value of our intelligence.

As much as our sources are public, our intelligence is not.

Visit www.world-check.com for further information,
or contact World-Check at contact@world-check.com

World-Check. Reducing risk through intelligence.