A Political Risk Management Function?

Insight paper by Harmattan Risk

April 2014

_____

A three part paper exploring the concept of a political risk management function in companies with significant exposure to complex emerging markets – is there one, does there need to be one, and if so what are the options in establishing an explicit political risk management capacity?

- *Part 1: Introduction, and Lessons from a Bygone Era*
- *Part 2: The Situation Now – Considerable Tacit Activity*
- *Part 3: Considerations and Options*

Part 1 – Introduction, and Lessons from a Bygone Era

Introduction to the Three-Part Paper

For organisations working in complex emerging markets, political risk is often the most acute challenge they face. Political dynamics such as weak governance, instability and conflict can create severe uncertainties. In an atmosphere of low institutionalisation and political tension, the web of stakeholder interests surrounding a foreign operation can also pose challenges, as different interests activate their political networks to act on their own attitude towards the foreign presence, whether supportive, hostile or predatory. The organisation's people, reputation, and operational performance can be exposed not only to a tense or volatile general operating environment, but to highly sensitive or tenuous relationships with politically-connected stakeholder interests.

As this is a significant source of risk in complex or "frontier" environments, we might expect that there is something akin to a political risk management function to help handle it. In fact this is seldom the case. Even the most adventurous upstream energy or mining companies seldom have a "political risk management department", even though they routinely operate in complex terrain.

For an organisation with routine exposure to complex emerging markets, this looks like a gap. Is there no one in the company handling this role? In fact there is, but we need to look behind the scenes and titles a bit to discover who they are, and what they bring to the table. We might find both more and less than we would have expected.

This paper does not directly hunt for the elusive "Political Risk Management Department". Instead, we try to see how the capacity has manifested and evolved, not as a particular office, but as the various strands of activities which have in fact comprised it, with increasing specialisation over time. We also consider whether or not it is worth having an explicit political risk management function, and if so, what the options might be.

The paper is divided into three parts.

Here in Part 1, we look at a classic political risk case from the late 1970s (the Iranian Revolution) and how different business functions were involved in addressing the issues that arose. Because the very concept of political risk was nascent at the time, this affords interesting insights into how an organisation adapted even without a clear definition of the type of risk that became the preeminent concern, or any prior blueprint for how it should be addressed. We get a glimpse into a situation

where political risk manifested in a significant way, but with almost no specialist capacity whose remit involved assessing or dealing with it.

Part 2 moves from the Iran situation to recent times, when a clearer concept based on decades of further experience and theorisation have at least put political risk more firmly on the corporate radar, even if tacitly and seldom as a single business specialisation.

Part 3 then considers if an explicit political risk management function actually makes sense, if so to what extent, and if not then what the options might be in at least making it a more explicit and shared focus of the functions that already tacitly address it.

Old Standby Case – US Constructor in Revolutionary Iran

The company had a track record of successful infrastructure projects in Iran dating back to the early days of the Shah's regime, but there had been a slump in activity until prospects were reenergised by the regime's commitment to connect the oil hubs with key ports and with Tehran, via modern highways capable of accommodating both passenger and equipment transfer. The company won a tender for a sizeable element of this network, a highway from Tehran to Ahvaz.

Things got off to a flying start in 1977, with the company beefing up the Tehran and sub-regional offices with expat staff with engineering and management skills, and Iranian administrative and local liaison staff. Unfortunately this was just in time for the first marked stirrings of revolution.

In hind sight the impending revolution might have been clear, but in an era of considerable hype over the Iranian modernisation miracle, 1977 brought scant warnings of what was to come. There were indications should anyone have thought to look for them: Increasing student dissent with consequent intensification of state repression leading to alienation of democratic activists; inflation of the ranks of the more intellectual opposition among the leftist Fedayeen and Mujahedin Al-Halq, which became increasingly radical; strikes and bazaar shutdowns in protest against modernisation reforms that alienated traditional channels of commerce; and hyper activity among the SAVAK in trying to keep tabs on and thwart democratic aspirations; all the while with the well known and respected (and exiled) Khomeini's rhetoric getting increasingly intransigent, and appealing to a wider cross-section of resistance groups looking for a credible and cross-class figurehead.

Indications in this period manifested in general unease, but it was still hard to believe or even play with the idea that this was a harbinger of a revolution. 1978, though, saw a steady increase in these

indications as well as greater cooperation between disgruntled urban lower classes, traditional interests and intellectual opposition. By mid-year there was a sense among company managers and expat dependents that there was something stirring, however ill-defined. This “something” might lead nowhere in the end, but even if it did not, it suggested that life for a foreign company was going to get harder before it got better.

In the second half of 1978, huge demonstrations and violent regime reactions were becoming routine. There was still enough ambiguity to think that this might just be bump in the road, but unease was heightening. By late 1978, expat kids could no longer go to school, company execs could not get to work every day because of unrest, protests, and gasoline shortages, and some Iranian liaisons and staff began to show hesitancy in being affiliated with a US company. Demonstrations became huge, with coordinated chants of hundreds of thousands rattling windows in the suburbs where expat workers lived. There were power cuts and with the declaration of martial law a curfew. There was even the odd bullet going down the street and grazing apartment blocks, driving families into windowless hide-out rooms where they would play cards by a gas lamp and sneak along the floor to the kitchen in darkness for the odd snack. Parents began home schooling. There was still some hope, but the prospect of things returning to normal in Tehran was quickly dwindling.

A trickling evacuation had been on-going since late 1978, but by early 1979 this had become a scramble, though most people made it out on commercial flights. Some expat staff stayed on or returned after the Shah left to try to work out getting property back to the US, and some Iranian staff hung on, in spite of the risks, to support their old friends in the company as they tried to tie up loose ends.

This case would result in full withdrawal, much trauma for people involved (but perhaps miraculously no physical harm; it was initially feared that some Iranian staff might have had a hard time under the revolutionary Komitehs because of their prior employment with a US firm, but subsequent contact indicated that this was largely avoided). It also led to lingering international court cases as Iran tried to press for a finding of non-completion and the company sought overdue payment and repatriation of assets left in Iran. The biggest impact was simply that the jewel in the crown of the international division fell away – realisation of strategic ambition in what had been the most spendthrift market in the region if not the developing world had been thwarted.

This was a very stark case of political risk manifesting, and also an illustration of how it can be a creeping process, first slowly building in the direction of a negative scenario, then spiralling. When it gets to this point, the company can either cling to hope that the situation reverses, or it can make a

solid decision to leave in an orderly fashion before the worst case scenario fully manifests. The latter is itself a very risky decision because premature withdrawal can signify a lack of market commitment and become a major project delay if the situation re-stabilises and the project is resumed. Those in the Iran case acutely faced this dilemma.

What functions were involved? Things were pretty crude back then, but it is still instructive to look at the way it was handled, as the company quickly adapted to new contingencies even without being able to rely on an established body of learning about political risk.

Throughout the time in Iran, **HR** regularly dealt with different ministries for expat work permits, employment permits and social security, and along with Health and Safety for the fulfilment of workplace safety regulations. It also handled the hiring of Iranian staff, partly through state employment agencies, and had Iranians on its team. Thus HR was very familiar with its corner of the Iranian bureaucratic scene, and later was able to use its contacts, as well as its own Iranian administrative personnel, to help understand the unfolding situation and to continue to support staff wellbeing once unrest became widespread.

As the situation declined, HR was concerned about the wellbeing of expat staff from an ethical standpoint. Equally, they were gauging their obligations and liabilities against all relevant national duty of care regulations, including Iranian. HR wanted to step up withdrawal planning and contingencies to support Iranian staff who would be left behind, but this urge was tempered by a commitment to the operation, and in some ways by subtle pressure from corporate management that the company should try "ride things out" or it would lose out if this wave of instability passed over. While HR could not act on its preference for withdrawal, it did support crisis management efforts as the revolution ensued, trying to ensure that people were prepared for an evacuation contingency and that the company knew where everyone was and how to get in touch with them.

Towards the end of the company's stay, **Legal** was having more severe headaches than usual over how to plan for potential withdrawal, struggling to create a legal argument for payment and for possible asset repatriation. It had been bad enough dealing with the Shah's byzantine bureaucracy to resolve complex red tape issues over the last couple of years, but now they might have to deal with a new government (no one really suspected a total change of system) who might see denigration of past international agreements signed under the Shah as a point of pride, and there was no telling if any new power-holders would adhere to international commercial law. Indeed as the regime's power eroded, there seemed to be no one clearly in charge of such questions. Legal arguments had to be mixed with incentives (i.e. we might come back to finish the job) to make any

sense to potential new officials, who themselves would be in an awkward and tenuous situation. There was much contingency planning going on in the Legal department, but the situation was often too fluid and the more pressure the regime came under, the less interested in legal details it became.

Security advisory did not consist of any permanent expert staff on-site. The security network consisted mainly of ex-US intelligence (based in the US) with some good contacts in the country, with some support from company board advisors still plugged into the US national security scene. Earlier these contacts had provided introductions to senior officials in the police, who in turn acted as a point of call and liaison for security related concerns. But as instability increased, the old country hands in the US saw their contacts wane or lapse into awkward silence in anticipation of potential regime change.

These remote advisors tried but failed to anticipate the direction and strength of change (in common with most intelligence services). They were left with advising on how expat staff should plan for volatility and how to conduct themselves when unrest was acute. They also advised on evacuation planning and liaison with current (tenuous) national security authorities to try to ensure that staff evacuation would be streamlined if it had to occur. But circumstances went far more quickly than their well intended suggestions, and there never was an evacuation per se, just an initial trickle of commercial departures, and then a scramble trying to get out on the last available flights, using local, not expert US-based, networks to help facilitate timing and arrangements.

Supply and Purchase (effectively handling local content, which was the only real manifestation of community engagement planning): This was well before the days of regulations or widespread ethical standards on corporate social responsibility in developing country projects, and the company manifested its recognition of the need for a degree integration with the host community mainly through hiring of national staff where there was any degree of fit with business needs, and by use of local suppliers where it made business sense. Construction operations had in fact not yet commenced, so the issue of directly hired local manual labour remained moot and engagement with unions untested. In fact Iranian sub-contractors never got a chance to fully apply themselves, but contacts and provisional contracts were maintained in anticipation of project execution (we should note that while the revolution was the show-stopper, before that the red tape and unpredictable approval processes had been a serious impediment to progress – operations should have been occurring by 1978).

When the revolution struck, Supply had to contend with the issue of how to recompense local suppliers for the time and assets they had accumulated in stand-by mode, in addition to quickly paying for the few provisions that had been rendered. This became a hassle as the banking system began to shut down, and cash payments became necessary.

A more critical point about Supply and Purchase is that because of their direct interaction with prospective sub-contractors, they had relationships which gave them an insider view on what was happening at the socio-political level. In the course of building local supplier relationships, the company had made some friends, some of whom were very forthright about their estimations of the political direction, and this afforded the company a source of local information and intelligence which was more nuanced and easier to read in some ways (or at least more aligned with the experience on the ground) than the grist coming out of the US Embassy and US intelligence contacts via Corporate. While the company "machine" might have been pressing for preparedness for the best case scenario, i.e. business resumption, these quiet local sources helped to plan for the worst case, which did indeed manifest in the end. Supply management thus was transmuted into a sort of intelligence capacity, making use of its contacts in local business networks.

Front-line Management, consisting of engineering and administrative executives who had cultivated relationships with Iranian counterparts and who managed Iranian personnel, quickly transitioned from their line responsibilities into a trouble-shooting and intelligence gathering role as the situation worsened. Starting with their liaisons in government, local businesses and the extended personal networks of their key Iranian staff members, they handled difficult day to day negotiations and facilitation of such things as ensuring that company cars had gasoline reserves, that families had heating fuel and emergency food supplies, that the team knew what hospitals and emergency services were open on a given day, and that everyone's status and contact details were up to date. HR played a critical role, but job descriptions soon became irrelevant as anyone with any contacts in the socio-political scene chipped in with the full extent of the information and personal networks that they had built up in Tehran over the last couple of years.

Front-line management also had the most direct relationship with the **individual Iranian staff** on their teams, directly hired or sub-contracted from would-be local suppliers. Some Iranian personnel were very open and helpful in providing their estimations of what was going on – many were also university students who knew the ins and outs of the revolutionary movement, and some were actually already members of the leftist groups who in the end helped Khomeini's people to position his "comeback", yet they still wanted to help the company which had originally given them their first serious job. When the situation worsened towards the end of 1978, some support and liaison staff

played a key role in helping to keep the company informed and supplied. Local drivers were especially critical, helping to keep the team mobile, using their knowledge the situation on the ground (and the habitually dangerous traffic conditions) to avoid protests and hazard zones once the revolution was in full swing.

Country Management, including the project managers (several people on one small executive team, with the Iran Country Manager as lead), was rightfully the main and foremost worrywart about how to manage the situation. Towards the last few months, they read the dispatches coming from the US Embassy and their national security contacts every day and tried to align this with the corporate line coming from their US HQ. They drove contingency planning and evacuation planning, and ensured open communication with people in the sub-regional outposts, and their pull-back to Tehran. They devised often rapidly revised contingency plans, and tried to keep the whole expat team and the company's joint venture partners abreast of their planning. When push came to shove, they were last out and the first to come back to pursue asset recovery, even well before the dust had settled. They had the ultimate responsibility for staff, and secondarily but importantly for the fulfilment of any last minute payments and in trying to retain a legal standing in the country in case operations ever resumed.

Aftermath

Political upheaval and a hasty departure clearly hurt. First and foremost, the company had to terminate and withdraw from a major strategic gamble. The subsequent arbitration yielded partial and ambiguous results, and losses were, to put it mildly, substantial. The company had been so closely affiliated with the Shah's old bureaucracy that it was impossible to forge new relationships with the survivors of the revolutionary purges, or ardent members of the new regime. Iran became a no-go zone, even had subsequent US sanctions not been applied to the country.

On a positive note, the company was never implicated in bribery, despite being relatively naive about the use of agents in the ambiguous governance situation at the time (a bane of many companies in Iran in that period). Miraculously, looking back on it, people got out without being harmed, aside from the nearly war-zone stress they endured for a while. Expats in contact with old Iranian staff learned that most had been able to melt back into the albeit tumultuous social scene without retribution for their American affiliation, although a few ended up in the Iran-Iraq War. And at least the subsequent arbitration cases did not implicate the company. The only reputational fallout was having lost a gamble, along with dozens of other Western companies who had been attracted by the Shah's modernisation spending.

In addition, the company learned some important lessons, namely to be better prepared for the downsides in terms of contingency planning and allocating specific responsibilities for risk mitigation when in volatile environments. Regrettably this learning did not have much impact on corporate policy; it was mainly driven at ground level by staff with experience or knowledge of the Iran project, who brought their learning to subsequent postings.

Case Learning – Who Handled Political Risk?

It is quite clear that there was no political risk management team (indeed the very label for such events was nascent at best). Perhaps in the spirit of the 1970s, international business was regarded as a gambler's art, and companies either played it safe or jumped into new environments hoping their people would adapt and learn along the way.

The US-based advisors turned out to be quite ineffective. They could not keep abreast of the situation from afar, and despite their previous involvement with Iran, they had no clear idea of the severity or even identity of the forces working against the Shah in this final stage of his reign ("communists" was the stock or fallback explanation among the less observant advisors, who were conditioned to Cold War stereotypes and believed that the leftist groups, who were only one faction in the revolution, were steered from Moscow to be the principal engineers of unrest). Based on their own experience in unstable environments, they did provide some potentially useful guidelines on how to handle the emerging crisis, but quite often the management team on the ground was well ahead of the experts in catching up to the situation.

HR and Legal both worried about how and when to pull out and how to cover regulatory obligations and reduce potential liability. Supply and Purchase became a window on the Iranian scene via their local supplier networks. Front line operational management quickly transitioned into a risk management role. Country management transitioned from being a commercial strategy and project management team into a crisis management desk. And Iranian personnel helped with the nuts and bolts negotiations over the resources to help keep the company and its people supplied and mobile, and informed their management contacts about how things were really going from a street-level perspective.

From modern day standards, the institutional response was very ad hoc, but it does illustrate some important points:

- Security and political advisors remote from the scene and shouldering long years of their own preconceptions could have limitations. Not only is their intelligence hindered by the archetypes and anchoring of the agencies which once employed them, but when their longstanding contacts are most needed, i.e. during a potential regime change, they might scatter and become incommunicable. It would be much better to have a full-time security manager on site, working routine local contacts and directly observing the scene, than to rely on remote, albeit very senior, advisors. In this case, an experienced and well networked security person or team on the ground could have been a major contributor to local intelligence, and to guiding the company in how to deal with the situation.
- Local networks helped. Those business functions with front line interaction with Iran partners and staff were able to adapt their more trusted and "plugged in" contacts into intelligence sources and facilitators of company sustenance. In this respect the company might have been lucky, because it did not carefully vet its relationships and there could have been predatory or opportunistic elements in the mix (there were some small scale scams here and there, but by and large local contacts acted on a genuine concern for their expat friends).
- In the final months and especially the last few weeks in Iran, the Tehran office was essentially a crisis management machine, and it actually performed quite well using just common sense and managerial professionalism. There was no specialist expert on site who had a standard operating procedure for the situation or any crisis response consultant (all sub-fields of political advisory were at best nascent in that era). People adapted, and quickly put their accumulated Iran experience and local networks into the foreground, well ahead of the functional specialisations for which they had been brought there in the first place.
- Corporate was anxious yet could provide little solid advice. It had approved the gamble and knew the amounts involved but also the stake in terms of people. Its messages were somewhat contradictory – hang in there in case we can resume operations versus look after yourselves and do not incur undue liability. In the end it deferred to and supported the country team in its efforts to depart with whatever grace it could muster, and no one involved in the operation faced repercussions or reprimand afterwards. If Corporate had at least had relevant policies and a pre-planned concept of how to guide such a situation, not to mention a direct line between specialist departments at HQ and their counterparts on the ground, it would have been able to do more than just watch nervously from the sidelines.

Revisiting the Question: A Political Risk Management Function?

In the Iran case there clearly was no such explicit function. Those most directly addressing the issue were the US-based advisors, by dint of their past involvement in foreign intelligence. But even if they had been more effective, their government experience was actually quite far from a political risk capacity, in which macro or strategic questions are only a part of the equation for those managing complex operations on the ground.

A political risk management function, whether one small expert team or a task force drawn from relevant specialist departments, clearly would have helped in the Iran case. On the other hand, the case also indicates the store of latent adaptability and planning capacity that can exist within experienced international business operational teams. A combination of this inherent raw capability with expert guidance would have made a much better organisational foundation for dealing with the situation.

The next part turns to where the political risk function stands in recent times. This is in counterpoint to the Iran case – here we saw that people can respond to the issue even without any concept of political risk. Now, there seems to be a much greater awareness of the issue and range of specialisation, yet perhaps like in the 1970s the function is still hard to identify with a clearly defined organisational seat.

Part 2: The Situation Now – Considerable Tacit Activity

With the end of the Cold War and a rapid increase in global communications capacity, international business is hyperactive compared to the 1970s. And governments and transnational organisations have kept pace, stipulating and proffering a range of regulations and ethical standards aimed at safeguarding both international companies and their host communities from the negative effects of foreign operations in volatile environments.

There is now a much more explicit awareness of political risk in developing region terrain, and more expertise in how to deal with it. However, in common with the 1970s, there is still seldom such a thing as a political risk management function. And just as in the Iran case above, international operators and planners still need to rely on their own judgement and networks to play their role in mitigating political risk (a role that is seldom made explicit but which nonetheless has been an increasing tacit element of many mainstream business functions).

We have pointed to some general functions involved in political risk management from the Iran case, but nowadays this range has on the one hand narrowed as specialised departments have developed, but broadened in the sense that more business is conducted at the "frontier" and more managers have experience in complex terrain. With the caveat that most business functions on the ground will be somehow involved in political risk management where the situation warrants, we can outline some trends in how this tacit function has been allocated. There will of course be many variations, depending on individual company structures, size, and international activity.

Governance Level, including Corporate Boards, Executive Committees (Excos) and Advisory Committees: In companies with a strong international footprint, political risk management is at least tacitly represented at the top. The Board and Exco, along with advisors, will be wary of the liabilities and repercussions of over extension into hazardous terrain and beyond risk appetite, and cognisant of the standards and guidelines which the company needs to adhere to in order to sustain its legal and reputational standing.

Sustainability is one driver of senior corporate awareness. Sustainability can be an ambiguous concept, but if we take it to mean awareness of and action on the risks and opportunities inherent in the relationship between a business and its socio-political environment, then it at least partly aligns with political risk management. Once a company publicises a commitment to sustainability, it becomes a promise to corporate stakeholders and hence a corporate governance concern.

On a more practical level, a senior executive political risk role is what can be called corporate diplomacy. Executive officers often usefully represent the company in senior-level talks with policy makers and regulators, and can help to kick-start ministerial-level discussions in support of specific country operations when stalled by political ambiguity or unresolved regulatory uncertainties.

Risk Management: The role and position of Risk Management varies considerably across even larger multinationals. The Finance sector has more tendency to implement high profile risk departments and a Chief Risk Officer (CRO) role, partly to help keep up with the wave of new regulations in recent years. But for many sectors, Finance included, a dedicated Risk department was also a factor of the increasing complexity of business, which is often coordinated across a matrix organisation combining regional, business segment and departmental axes. Having one corporate department tracking risk, perhaps via an enterprise risk management (ERM) system, ensures that potential fault lines in the wider operation are mapped and overall priorities identified, ideally resulting in commensurate control programmes at the relevant organisational level. Risk Management also develops expertise in general risk control processes, which can be adapted to a range of specialist needs.

Some risk departments incorporate experts from different specialist functions, such as Legal, HSE, and Internal Control, giving them a capability to advise on specific risk control initiatives at the operational level. Political risk expertise, by whatever label is used, could be included, and there are at least some recent trends to incorporate political risks into ERM risk registries.

It seems, though, that political risk management, as the expertise and processes involved with political risk intelligence and planning, is in fact seldom an explicit sub-domain of the official Risk Management department. With some exceptions, thus far Risk's focus still tends to be mainly compliance and insurance. Aon's Global Risk Management Survey of 2013 had the interesting finding that a typical corporate Risk department even in very large firms consists of about 3 to 5 people, indicating little capacity for in-depth specialisation within the department itself.

While there is some movement towards integrating political risk into corporate ERM risk registries, the actual political risk management process is more likely to be defined, led and executed within functions that have more direct experience in international planning and operations, and which are much closer to the interface with the socio-political environment.

Strategy and Business Development: Corporate planners will aim for a risk-reward balance in the global portfolio, and will examine new overseas prospects to see how they align with the target balance. Along with Business Development, which scopes new opportunities, Strategy will examine a prospect for feasibility and against corporate risk appetite. This often includes compiling or

commissioning a top-level, or macro, political risk assessment which then feeds into a wider opportunity assessment process. If approved, Strategy will likely work with the relevant business unit to develop market entry plans, taking political risk variables into account as one set of factors.

External Affairs: External Affairs (which carries a range of other labels) is among the functions most directly tasked with managing the interface between a company and its socio-political stakeholders. It handles media relations, which is a critical risk management function in that it helps to shape how a company is perceived by socio-political actors. It also leads on lobbying efforts, articulating the company's own contribution to debates on regulatory changes that could affect it. External Affairs often works closely with CSR (see later), helping to articulate a CSR programme's intentions, and, given its public relations remit, communicating positive outcomes. Along with its core activities, External Affairs managers tend to act as mid-tier diplomats, networking in different stakeholder communities, presenting the company's position, and developing information sources that can help to negotiate socio-political sensitivities around a company's presence.

Finance: Finance works with Strategy to assess an opportunity in an emerging market, incorporating political risk variables into the financial aspect of the assessment. It might be independently responsible for political risk insurance, or would work with Risk Management to source the right coverage. Finance will also be involved with formulating project finance structures that take into account and seek to reduce political risk, specifically potential government behaviour with respect to non-payment, contract abrogation or expropriation. Finally, Finance will develop hedging strategies to help cover against unexpected government economic policy changes that could affect the value of foreign investments.

Internal Control: In the wake of the financial scandals of the last decade, internal control capacity has been increasingly mandated by regulators in developed countries, and now in addition to key anti-corruption and anti-fraud standards, companies have a range of corporate due diligence standards with which they need to comply. Indeed such standards are also adopted not just because companies want to avoid regulatory non-compliance, but because corporate integrity has its own rewards in terms of loss prevention and the prevention of embarrassing scandals.

As its label suggests, Internal Control focuses mainly on internal integrity risks, but in complex environments these are often affected by or linked to weak public governance and predatory interests outside the firm. Internal Control plays a key role in identifying and managing "insider threat", i.e. staff or partners with connections to or compromised by hostile external interests, which can be politically-connected organised criminal groups or even rogue security agencies. It also

ensures that staff are aware of corruption risks and how to identify and handle corruption pressure, much of which can come from government agencies or state partners.

Legal: Legal teams in international companies and among their legal advisors have always been active in political risk management. They are involved in contract design, including with state buyers and partners, to help ensure robust legal guarantees and legitimate arbitration options. On a more operational level they also assist in negotiating and maintaining the legal approvals that effectively become the "official licence to operate" in a given country. Additionally, Legal will ensure that other risk management functions, such as Security (a more sensitive one from a legal standpoint because it can include armed deterrence), are aware of the laws affecting their activities and will review compliance. Legal generally keeps a watchful eye over an operation with a view to legal compliance, and would directly manage any litigation or arbitration that might result from disagreements, including with state customers or partners.

Corporate Social Responsibility (CSR) / Community Engagement: CSR is the function most explicitly linked to the implementation of "sustainability" policies. We previously briefly defined sustainability in a way that also made sense from a company's own risk perspective, but the concept's usual public definition focuses much more on how companies can contribute to *sustainable* development in host communities. There is a degree of "spin" in this angle, since sustainability would seldom be a company focus unless it also helped a company to *sustain* itself and its operations. Nonetheless, the aspect of contributing to the wellbeing of societies in which a company operates is at least half of the sustainability equation, and the half that CSR is tasked to address.

In a classic model, the CSR team commissions an SIA (social impact assessment, which can overlap with and sometimes be integrated within an environmental impact assessment), and in many cases also a nuanced stakeholder assessment. CSR then uses these as a baseline to guide operations towards minimal disruption and ideally some enduring local developmental benefit from the company's operations.

CSR is rarely positioned as a political risk management function, yet it is in fact a critical one. It helps to identify and mitigate the downsides of a company's presence from a host community perspective and to offset the detrimental effects of an operation through commensurate social investment. In cases where a company is heading to particularly volatile environments, CSR also manifests a conflict sensitivity role, aimed at ensuring that the company does not inadvertently exacerbate tensions between factions in the local environment, or otherwise infringe on human security. In the best of cases, CSR initiatives actually discern and address key local socio-economic development

bottlenecks, and have an enduring positive effect long after the company has left. All of this helps to reduce potential friction with the host community, thereby reducing risk, and it also shores up the company's reputation with key stakeholders including the media and influential NGOs (hence a useful relationship to External Affairs).

CSR does not yet have firm regulatory standards attached to it, unlike Internal Control (although there is an array of ethical standards on the issue - we will get into these in another paper, but suffice to say that the UN's Principles of Responsible Investment and the Global Compact are two well subscribed baselines). And performance in CSR, as well as "sustainability", are self-assessed (though often using specialist consultancies *hired* to provide an "independent" assessment). CSR and its parent concept of "sustainability" are thus open to the charge of "green wash", i.e. putting forward an overly positive interpretation of the developmental effects of the company's presence. Despite this perception, which might hold true in some instances, CSR departments are often very committed to delivering tangible net benefits.

The potential "green wash" charge in mind, perhaps a more pressing limitation of the de facto risk management role of CSR teams is an oft-cited disconnect between CSR and operational management. Operational managers, many of whom have long experience in developing countries and international projects, tend to make their own way, using local relationships and routine negotiation on the ground to help shape a project's socio-economic positioning for mutual benefit, and Operations does this with a constant eye to budget, timelines, and business imperatives. CSR teams can seem like an appendage from an operational point of view, especially if they are not embedded, but rather imported from HQ on a temporary basis and develop recommendations based on a fraction of the local experience developed by country project teams.

Additionally, there can be a significant difference between the functional languages of the two realms. In fact many CSR people are hired from NGOs or transnational organisations, and they can find it difficult to shed their old paradigms when operating within a commercial environment. Likewise Operations do not often understand where CSR is coming from.

These limitations sometimes inhibit the open collaboration of CSR and Operations, and can lead to inconsistencies from a host community perspective. This can certainly lead to gaps from a political risk management point of view.

A company with a well developed CSR capacity needs to be cognisant of CSR's limitations and the need to integrate it with business operations for best effect. But without CSR they might well be left without a key interface between the company and its societal stakeholders, and might end up in a

panic-driven reactive mode when faced with host community friction. If well integrated, CSR can be a very useful player in political risk management.

There is substance to the wider "sustainability" perspective. Charges of "green wash" aside, it is at least a recognition of the fact that companies do not only operate in a vacuum once known as the "competitive arena". Companies operate in a wider eco-system alongside diverse interests and values. Sustainability, and its most direct functional manifestation as CSR, at least recognises and acts on this inescapable fact.

Security: The security function has more immediate associations with political risk than several others, partly because it addresses some of the more overt or spectacular risks, such as terrorism, kidnapping or a "melt down" in terms of instability. It is in fact a very broad domain, ranging from an overlap with more routine Health and Safety issues, to strategic contingency planning and crisis response. Security mainly focuses on "threats", in other words actors with an actual or latent capability and intention to cause harm.

In a complex emerging market context, the security function will likely be primarily concerned with the well being of personnel, and secondarily assets (including information). Security will have its own specialist intelligence process to understand priority threats, and will create plans and capabilities towards avoiding and minimising risks posed by threat behaviour. Some of its functions at the country or operational level would include:

- Keeping people informed of threats and high risk areas and providing advice and guidelines for personal security deportment among staff
- Acting as a liaison with host country security forces and police, including acting as a moderating buffer if such forces are known to be corrupt or unprofessional
- Sourcing and managing local and foreign security contractors, and ensuring that their training and comportment are aligned with ethical and legal expectations (the Voluntary Principles on Security and Human Rights is a set of guidelines in this respect)
- Creating and implementing security arrangements for personnel, residences, facilities and information integrity
- Devising and testing crisis contingency plans in line with priority risks (e.g. kidnap or terrorist attack) that could affect personnel in particular
- The above often extends to evacuation planning, often phased to align with indicators of the severity of a situation

- With Internal Control, conducting confidential investigations to discern potential ill-intentions or conflicts of interest among people and partners with whom the company is considering interacting (there can be overlap with Internal Control, but Security would likely look more at uncovering security threats, Control more at corruption and fraud risks)

Security does have some affiliation with the use of force or at least deterrence, and taken to extremes it can hinder a company's acceptance by a host community who perceive a company as somehow hiding behind barbed wire, or indeed as presenting a threat through heavy-handed security measures. It needs to be carefully managed with an eye to human security for the host community, which suggests a useful relationship to CSR. It also needs to consider that operational staff value flexibility in their own roles, and Security can become a hindrance if designed in isolation of operational performance imperatives.

As these delicate balances suggest, a good security manager is far from just being a technical expert – he or she would ideally bring a strong dose of diplomacy, cultural knowhow, and strategic thinking to the equation. If Security was well versed in these imperatives, it would be an indispensible part of the political risk management equation, since part of this derives from hostile or predatory behaviour, or violent clashes in the operating environment, which no amount of legitimate persuasion or negotiation can mitigate.

Human Resources: As the Iran case illustrated, HR's remit gives it a significant concern for political risk, specifically as it affects personnel. HR tends to manage travel tracking, travel document back-up, and personnel deployment training (ideally in conjunction with Security). HR will also ensure compliance with the duty of care regulations relevant for home country, host country, and third country staff. HR's remit extends to defining travel and kidnap insurance for individual personnel. On a more bureaucratic level, HR also handles work and resident permits for transferred staff and helps people to settle into their new location. And as dull as cross-national personal taxation issues might be, they are important for employees, and HR will take these into account in settling new staff into a foreign operation. Any bureaucratic delays in getting the right people established can have operational consequences.

HR plays a critical role in local hiring, and this can extend not just to union negotiations, but also to ensuring that national staff experience a smooth cultural fit with the foreign company. Indeed sometimes a severe lack of fit can result in "insider threat", which can be escalated to Internal Control or Security. Preventing this is part of HR's value in overall risk mitigation.

Finally, if there is a crisis that affects personnel, whether mundane or from political instability or violence, HR will have a key position at the crisis table to ensure that duty of care obligations are met.

From a political risk standpoint, HR deals with the priority exposed asset of an international company, people. Rather than being a back office function, in our experience HR has quite a lot to do in political risk management, as the main owners of employee wellbeing and personnel performance even in the face of political uncertainty.

Health, Safety and Environment (HSE): HSE's safety concerns will extend to the safety implications of the socio-political environment, and to meeting local workplace regulations. Its safety remit gives it a natural relationship to Security, who is also concerned about safety but from an external threat, rather than internal accident or natural hazard, perspective. The two functions often collaborate on emergency preparedness and evacuation planning.

On the "E", or environmental side, HSE provides guidance to Operations to help ensure alignment with environmental imperatives as identified in an environmental impact assessment (EIA – nearly always mandated by the host government and usually a good idea anyway). This role can reduce social risk by helping to avoid or mitigate an operation's potential negative effects on host communities, from both an immediate noise and pollution point of view and a longer term resource degradation perspective. It also helps align with external environmentalist expectations of the firm, mitigating NGO criticism.

HSE also seeks to ensure regulatory compliance with host country environmental standards and protections. In so doing, HSE develops an understanding of the bureaucratic approvals process to try to expedite relevant permits, which in weakly governed countries can be subject to considerable red tape, and political contention because of complex land ownership rules (often a tenuous balance between official and traditional claims). HSE's expertise in facilitating environmental approvals can significantly reduce bureaucratic delays to the launch of new operational phases.

Business Continuity: Business continuity as an independent function might not be present on the ground, but there will usually be at least a task force developing programmes to help ensure redundancy and recovery of key processes and assets, perhaps with guidance from experts in HQ. This is planned against risks to continuity, which can include political risks such as unrest blocking logistical routes, infrastructure shutdowns during periods of high tension or national strikes, terrorist attacks on either company facilities or critical infrastructure, and attacks affecting information systems and company communications.

Operations / Country and Project Management: The Iran case illustrated a high degree of adaptability among operational managers, from country and project management to front-line engineers and administrators (there will also be a high proportion of back office staff who might have limited professional engagement with the socio-political environment). Indeed, the more that socio-political risk awareness is integrated into mainstream Operations, as opposed to being a specialist appendage, ultimately the more effective it will be, because of Operation's proximity to the host environment, strategic perspective on the business situation, and international know-how of experienced staff.

Country or project managers are the pinnacle of operational risk management planning on the ground, and in complex environments this often means considering political risk. They would also chair crisis teams and lead on operation-wide contingency preparedness. On a more routine basis they also have a role in corporate diplomacy, as the senior company representative in the host environment, capable of bringing gravitas to high-level ministerial and state partner / customer meetings to try to overcome bureaucratic obstacles.

The Iran case and indeed the experiences of many businesses successfully operating in complex terrain make it clear that Operations have a crucial role in political risk management through sound managerial thinking and international experience, plus a very direct link to the operation at stake. Operations is often very distracted by technical and commercial issues, and specialist functions can help in informing and guiding, but ultimately Operations retain ownership over the success of a foreign initiative, and over strategic decisions about how to make their project resilient. The nexus of well integrated specialist functions and experienced Operational know-how is perhaps the ideal combination for resilience in complex environments.

Individual Staff: In a high risk environment, everyone is responsible for their own part in risk awareness and management, beginning with their own self-deportment. Through their day-to-day exposure to their own corner of the socio-political terrain, people will also develop valuable insights for risk management planning. **National staff**, as demonstrated in the Iran case, can be indispensible in helping to understand socio-political and cultural dynamics, and in facilitating local interactions that might help to sustain the company in a crisis.

Revisiting the Question: A Political Risk Management Function?

The above was not intended to be exhaustive, but even within this sample it is apparent that several functions have at least a tacit hand in managing political risk, even when it might seem somewhat remote from their label or formal remit.

Indeed any function whose position enables a strategic perspective on the international portfolio or socio-political interface in a country operation can, if the individuals in question are curious, concerned or see the value in it, play a useful political risk management role. This can occur through an individual's self-education about the socio-political environment, an inclination to look for potential issues before they become problems, and personal influence in one's informal network towards inspiring more interest in and collaboration on political risk.

There are a few functions with a direct remit for managing socio-political interaction, and by extension who have considerable interface with the socio-political environment. These tend to include External Affairs, CSR and Security. Perhaps these might be the closest things to a political risk management function, at least on the tactical level: External Affairs reduces socio-political stakeholder misperception of a company's intentions, CSR reduces socio-political friction, and Security deters and protects against threats including hostile politically inspired or connected groups.

In strategic corporate terms, one could extend these three functions to their respective corporate departmental seats, but even then they would not cover the integration of political risk with strategic and market entry planning, contract design, regulatory compliance or financial hedging. These other aspects sit better with functions which have a broader overview of the international portfolio and the corporate regulatory environment.

And between the specialists and the strategic level are Operations, including management of international divisions or business units, country and project management, and front-line core business operational departments. Country or project management is where the most direct accountability for risk management at the operational level sits, even if Operations needs to rely on specialist functions for support and implementation. Other experienced operational managers on the front line in a host country would, just through their very day to day judgements and behaviour, have a very significant effect on operational resilience.

One might be able to sketch or envision at least a mental model of an operations capacity led by experienced international managers whose core remit is to scope and execute overseas operations.

One significant issue they need to contend with to fulfil their remit is political risk, and they can draw upon and integrate specialist departments in order to help make their operations more resilient. This model puts responsibility for political risk management at the core business end, and postulates the integration of specialist functions around the common aim of supporting the resilience of business operations in complex terrain ("Sustainability" remains important in this sketch, because whatever else it does, it can help reduce risk).

This mental sketch might sound almost obvious to some, but it is not necessarily how companies see the political risk management function, and in practice it can be very difficult to map an explicit company-wide rationality to it.

Theorising aside, a main point to arise from both the Iran case and Part 2 is that there is often no one official function dedicated to the issue, and that it can fall across a range of functions. That might suggest that this type of risk is well covered, at least measured in terms of overall activity across the business. However, the question then arises, how could a company even know if the issue is well addressed if there is no one explicitly tasked to ask the question? And who keeps track of all these strands of activity to ensure that they are aligned to priority political risks and stakeholders?

Part 3, the final section of this paper, will consider these questions, among others.

Part 3: Considerations and Options

It would be useful to briefly recapitulate the key findings from the previous two parts of this three-part paper.

Part 1, looking at a foreign operation in Iran during the Revolution, found that even in the absence of a concept of political risk, let alone specialist risk management, operational managers adapted quickly to a dynamic situation, with the result that the company experienced no major incidents and got its people out intact. The major shortcoming was a lack of nuanced intelligence and analysis on the situation. This led to a highly reactive response, which might have sufficed at the tactical level, but in strategic terms it delayed a decision about what to do about the whole operation (stay or go?) until it was too late for an organised withdrawal and for minimising both loss and strategic business impact. Another key finding was that while the exertions of the management team were admirable in many respects, without expertise in dealing with political volatility on the ground, it was a hair-raising experience and there was a significant degree of luck involved. This would have been much smoother and less hazardous had there been political risk crisis management and intelligence-based contingency planning integrated with the operation.

Part 2 made it clear that political risk management now, if broadly defined as identifying, assessing and managing issues that could arise in the company's interaction with its socio-political environment, is actually undertaken across a surprising array of business functions. It is seldom an explicit focus of any of these, but it is an increasing tacit focus, and there are now more specialised departments tasked to manage particular aspects of socio-political interaction. One could try to mentally organise this diverse activity with a business-first model wherein Operations takes responsibility for resilience of business initiatives and specialist departments provide support and guidance. But this is imposed from an outside perspective, and in fact there is seldom a rationalised model of political risk management. Another finding that cross-cut the discussion in Part 3 was that depending on how it is positioned, sustainability is actually quite closely related to political risk management, but it can be a vague concept and is seldom positioned as risk management.

In this final part, we will directly posit the question, is an explicit political risk management function necessary? This will lead to some insights on the positioning of such a function. Then we examine some of the structures that have been used in the rare cases where political risk (or terms that mean something very similar) has been explicitly put on the corporate radar. Finally, we examine some options that companies can consider in their own formulation of how to address a political risk management capacity.

Is a Political Risk Management Function Necessary?

When we pose this question, we need a concept of what a "function" might entail. This would vary, but broadly it would have the following attributes:

- Permanent capacity with a mandate to assess and advise on political risk (whether using the "political risk" label or something with the same connotations)
- Manages and executes the political risk intelligence process, including dissemination to users across the firm
- Develops policy and good practice guidelines around political risk assessment and management
- Provides coordination mechanisms for better alignment on political risk management across the firm
- Acts as an internal consultancy to other specialist functions, and to Operations, in building and implementing political risk management initiatives
- Internal skills consist mainly of a combination of socio-political intelligence analysis, contingency planning and crisis management, with additional in-depth awareness of how the other specialist functions (CSR, External Affairs, Security, global Strategy...) operate, and strong familiarity with the business and its industry

This might be a department, or a specialist team embedded in a high-profile planning department (probably not embedded within a specialist function such as External Affairs or Security, since that would likely turn political risk management into just a manifestation of its parent department's current focus). Based on this straw man outline, is such a function necessary?

The "yes" reply might be based on the following points.

- With a greater presence in emerging markets we are finding that political dynamics are a bigger factor than ever in the success of our operations and security of people and assets. Yet as business experts we realise that we are not well versed in understanding and planning for the effects of politics. This is a very different domain and we need to develop an explicit competency in it if we are to sustain a successful global presence. A clear political risk management function would put the issue firmly on the corporate map, and its expertise could be usefully adapted to support strategic business decisions and operational resilience.
- There are a lot of activities across the firm that touch on what amounts to political risk management, but thus far they are rather disaggregated and sometimes even working at

cross-purposes. A dedicated function would help to map and align these activities for a more coordinated and strategic approach to political risk.

- Our sustainability policies and practices help us to achieve a better integration with our socio-political environment, but they do not explicitly address the risks that could arise from interaction with the socio-political domain. Sometimes it seems that sustainability is more about maintaining our standing as a good corporate citizen, and less about sustaining our operations. Political risk management would help to balance this emphasis with a more pragmatic focus on how to look after ourselves in the face of socio-political volatility and potentially hostile or predatory political interests which might not be positively influenced by our sustainability message.

Conversely, the "no" argument might consist of the following.

- We already address political risk through a variety of activities and with our sustainability practices. There is no sense in reinventing the wheel and adding yet another layer of bureaucracy.
- Besides, the presence of such a department could actually reduce a sense of ownership over the issue among other specialist departments and operations. It is better if we handle the issue organically across the firm rather than segregating it in one specialist department.
- Based on what we have seen in terms of political risk reports and advice from country intelligence consultancies, we find such expertise to be rather academic and divorced from business realities. A department would likely be just as abstract, and if so then its ideas and outputs would be difficult to act on. It is better if we just build an awareness of political risk into our operations, from a business-first perspective.
- Such a department might stand in rather stark contrast to, and even undermine, our sustainability messaging. After all, how can we say that we recognise the need to integrate and coexist with our wider stakeholder environment, and at the same time position this interaction as a source of potential harm?

This does not lead to a clear winner, and the answers would be different for different organisations. Indeed neither argument is mutually exclusive, and together they offer some potential guidelines on what a political risk management capacity might need to take into account:

- A balance of solid political risk expertise and business know-how to ensure relevance to and application by business decision makers and Operations

- A seat of political risk expertise and a channel for coordination, balanced by shared ownership of the issue across other relevant parts of the firm, Operations included
- Provide a business risk perspective on socio-political interaction without subtracting from the sustainability message in terms of the positive synergy of the business and its socio-political stakeholders

Some Current Approaches

In companies where political risk management is more explicit, a few models of a relevant function or at least general capacity have manifested. This is probably not exhaustive, but indeed it is a challenge to find many cases where political risk has been defined as an explicit focus.

1. Encompassed in the definition of sustainability

While public definitions of sustainability usually focus on business' commitment to sustainable development, some firms make it clear that sustainability does in fact refer to the company as well. The list of departments relevant to sustainability therefore extends beyond CSR to include Security, for example, which helps to sustain operational resilience and the safety of people and assets with respect to external threats. In this conceptualisation, there is no contradiction between a company's corporate citizenship role and its obligation and right to be vigilant and look after itself (Indeed if a company were lacking the means to sustain itself, it would be much weaker in fulfilling its other sustainability mandates).

This conceptualisation does not indicate or lead to a specific political risk function, but it does put risks in the relationship with the socio-political environment onto the corporate radar, thereby strengthening efforts to explicitly address such risks.

2. Political risk expertise is delegated where it is required or makes the most sense, and therefore can exist in several places

A typical model tends to be:

- Strategy and Business Development conduct tailored political risk analysis in assessing an opportunity's feasibility and risk-reward balance, and to inform global planning decisions
- The concept of the Communications / External Affairs function is expanded to mean the wider set of expertise in dealing with the external environment, including developing intelligence on socio-political trends – there would be a political risk team embedded in this

wider external-facing department (which also handles government relations and in some cases even CSR), and through the department's internal corporate networks this team can be called upon for support from across the firm

- Security goes beyond tactical considerations and is tasked with planning against potential negative political trends and threats, and therefore has an embedded political risk team focusing on risks from violent instability and hostile political interests
- Risk Management, who handles political risk insurance acquisition, regularly commissions risk intelligence reports from external experts in order to cross-check insurers' own assessments, to enable better informed purchase negotiation

This model is not very different from the more widespread "non-model" of an entirely tacit approach to political risk, but at least political risk is given explicit attention in the departments most concerned with the international and socio-political environment.

3. Political risk awareness made explicit and elevated towards the top for higher visibility

There are not many examples, but one comes from one of the companies involved in the In Amenas attack in Algeria in 2013. Its post-event review found several key gaps. One was a past tendency to see security issues as a health and safety concern (HSE traditionally does not address threats, i.e. hostile or predatory behaviour). Another, perhaps more important finding was a lack of in-house political analysis and planning capability. The company had been using external intelligence providers' reports, and while these were useful, there was no explicit task of collating and analysing these further to see what they really meant for company's operation. Political risk analysis had been conducted, but within the Communications department since political risk was regarded more as a reputational concern. This was deemed to be insufficient in light of the In Amenas tragedy, and too low in the wider corporate structure to have enough visibility across the firm.

While some political risk analysis continues to occur in other departments, the firm decided to establish a permanent political risk team within the corporate global strategy unit, a high profile department with direct links to the senior executive level. External intelligence is still used, but only as one input. The team has its own analysts who directly link analyses to operational concerns for the company. Additionally it is led by people very experienced in corporate diplomacy, contingency planning and crisis management, and therefore provides not just intelligence, but also a credible internal advisory service for operational units. The team also has explicit links with corporate Security, to ensure that Security is fully informed of issues that could affect the wellbeing of personnel on the ground.

As Part 2 of the paper clearly indicated, political risk management is actually carried out, on a tacit level, across a wide array of established functions, but these are the main organisational approaches where political risk has been given a reasonably explicit status. The above is not intended to suggest that these models are better than the more mainstream tacit approaches, but they are useful in positing some options. The third one is perhaps the closest to the archetype of a political risk management function, and it will be interesting to see how this model works and evolves over time.

Options

Harmattan Associates and like-minded consultancies exist in part because we feel that political risk is a unique and important concern, and that as a result political risk management should be an explicit capacity in companies with regular exposure to unstable environments. We would naturally agree with the "Yes" side of the earlier argument, but we also respect some of the "No" points. For example, if a certain capability is important to the entire firm or major parts of it, then positioning this capability as an arcane specialism is inappropriate. It needs to be well connected to those parts of the company that most require its expertise, and while there can be a core of expertise on the issue, ownership for it must be shared. We also agree that whatever form it takes, political risk management should deliver to the business, and that means knowing the business and how the function's expertise can be shaped for best effect.

We certainly do not see any contradiction between even the most development-oriented sustainability position and political risk management. If a company cannot look after itself, it cannot contribute to sustainable development. Conversely, sustainability commitment has a very relevant political risk management role, in helping the company to understand and mitigate concerns about its social performance that could lead to socio-political friction, hostility, and liability, with consequent harm to core assets and strategic aspirations.

Thus we would argue that an explicit political risk management capability or function is both necessary and fits well with broader initiatives to integrate with the socio-political environment. However, this does not necessarily mean that it should become a full department. As Part 2 made clear, there is a lot of relevant capacity in the company already. It could just be a matter of aligning it, or at least making it aware of political risk to better steer activity to take it into account.

What then, are the options? The permutations could be diverse and need to be tailored for the firm's own context, but we can suggest a few reference points.

1. Policy Guidelines and Awareness

- Political risk assigned to existing high-profile department, perhaps Strategy, and one or a few executives with the requisite experience are tasked to draft political risk policy guidelines and develop an awareness-raising programme
- Policy guidelines provide:
    - A consistent definition of political risk
    - The types of issues that could affect the firm's people, reputation and performance
    - Political risk considerations for specialist departments, including External Affairs, CSR and Security
    - Political risk considerations for business planning and operations
    - Guidelines for political risk analysis and planning at the operational / country level
    - Where to seek internal support on political risk, useful contacts and networks, suggestions for coordination
    - Useful external resources
- The establishment of a political risk knowledge forum to encourage cross-learning, information-sharing and coordination across the firm, with representation on the company Intranet
- In conjunction with HR and specialist departments, the design and delivery of political risk awareness training focused at both specialist departments and operational management

This option inserts political risk into the corporate consciousness and provides top-level guidance on addressing it, but for the most part it then allows political risk management to occur tacitly and organically, albeit ideally with more focus and coordination as a result of increased awareness.

2. Coordination Mechanisms

Perhaps using the same initial resources as above, the team establishes mechanisms, for example joint planning or review meetings or joint task forces, to ensure a reasonable degree of coordination on political risk intelligence and planning between specialist functions and between them and Operations:

- Cross-functional risk intelligence sharing, and risk assessment cross-checks to ensure that different functional activities are aligned to common priorities
- Sharing lessons learned and emerging best practices
- Coordination of functions involved with risk management planning for specific operations in volatile locations

- A channel for operational managers to express their needs and preferences in terms of specialist analytical and planning support

This model is compatible with, and could even depend on Option 1, and would be a formalised extension of the knowledge forum concept. This is still quite "light touch" and does not mandate a political risk management function. But it would require that the founders of these mechanisms retain oversight over them, to ensure that they remain effective and adapt to changing requirements.

3. Political Risk Intelligence Team

- Embedded in Strategy or Corporate Services department
- Establish and manage the political risk intelligence process
    - Focus defined by geographic areas and transnational issues most relevant to company exposure
    - In addition to regular reporting and monitoring, also takes intelligence tasks from prospective end-users in Operations
    - Performs full intelligence cycle, from collection to analysis to reporting and dissemination
- Manages relationships with external intelligence suppliers, but does not rely exclusively on supplier reports – rather takes these as one input, in addition to its own research, for a company-specific integrated analysis
- Manages political risk intelligence portal and other dissemination channels
- Principally experts in political risk intelligence, including research and analysis, but also well aware of the company's business to enable user-relevant reporting
- This intelligence function would not replace more specialist information gathering among other departments (for example, Security would seek its own detailed assessments on terrorist and organised crime threats, CSR on social stakeholders, etc), but it would provide a strong baseline of shared risk awareness.

In not intruding beyond intelligence provision, this team would leave planning and execution to others. There are two assumptions behind this. One is that a shared intelligence output would tacitly increase alignment around priority political risks, in other words it would help put different risk management activities "on the same page". The other is that prospective users in specialist departments and Operations already have a workable process in place to actually make use of political risk intelligence (this might not always be the case and should be examined in order to ensure that an intelligence team's outputs could indeed be effectively applied).

This option is compatible with, and would be more effective with, Options 1 and 2, though some explicit integration would be required.

4. Political Risk Advisory Unit

This need not be a department on par with mainstream functions, but it would be a more centralised and independently resourced unit. It would actually manage and coordinate the activities indicated in the three previous options (policy and awareness, coordination mechanisms, and political risk intelligence). But in addition it would contain the expertise to advise other specialist departments and Operations in planning and executing political risk management initiatives, or in tailoring their own efforts to help ensure that political risks were addressed in the process. This *additional* expertise would include:

- Contingency planning and crisis management
- Corporate diplomacy and negotiation (especially private-public)
- An understanding of the remit and practices of other specialist functions and departments involved with risk management or socio-political interaction
- An understanding of the business: strategy, international ambitions, global portfolio, at least the basics of how operations are conducted
- Strong links into the "customer base" in international Operations

It is conceivable that such a unit would:

- Have a permanent core of intelligence, contingency planning and crisis management professionals
- Have seconded staff from other specialist departments, and Finance, Strategy and Operations to help ensure alignment with other risk management activities and business imperatives
- Deploy its own members to overseas Operations when called upon for local political risk management support
- Have a tier of non-permanent members in other departments and Operations who retain their "day jobs" but who act as the liaison and initial point of political risk guidance for their respective units

This is perhaps the full model of a political risk management function. It is short of being a department, has a small core team but is extended by secondments and liaison members, and is well integrated with other risk management functions and mainstream planning and Operations. Being

an independent entity, it retains its own identity and puts political risk well on the corporate radar, and has the flexibility to shape itself in relation to customer needs.

Going beyond this would mean the establishment of a new corporate department, which is certainly an option, but there would have to be tight control over its scope and position or there could well be redundancies given the other related activities going on around the firm.

Further thought on the issue would certainly yield more options. In assessing what makes sense, a company would clearly set forth the relevance of political risk in its context, what it would hope to achieve from a political risk management capacity, and the internal cultural and organisational factors in shaping it. A variety of options could then be tabled and assessed against a consistent set of meaningful criteria.

Summary

The full paper has illustrated that there are inherent political risk management capabilities among experienced international operational teams. It has pointed out that political risk is now handled by an array of different business functions, but tacitly and often without much coordination or alignment. And finally it tested the concept of an explicit political risk management function and what the options might be in establishing one.

It is becoming very hard to ignore the intersection of increasing foreign business in emerging markets and the challenging political dynamics in many such environments. This makes political risk a pressing concern. Addressing it tacitly can only go so far, and at some point in the evolution of a company's global presence the question of an explicit political risk management capacity, bringing shared awareness and greater organisational alignment, will likely arise. Hopefully this paper has provided some useful reference points.