A Few Questions about Clear Thinking in Political Risk Analysis

Insight paper by Harmattan Risk

August 2016

_____

This is certainly not intended as a mini-manual on political risk analysis. Rather it derives from our own experience and some of the questions that we have faced in projects involving intelligence on risks in a particular country context, for a specific client initiative (i.e. not just a "country report"). Our past work with some mainstream consultancies in this space and discussion with old colleagues reinforces the notion that knowing about something (a country or a type of risk such as terrorism) does not necessarily make it easy to decide how to define and address a risk intelligence question.

Some of what follows could seem like philosophical meandering, and though it might be, it can be surprising how inattention to structured thinking in political risk analysis can lead to ambiguous or indecipherable results, or reports that are "all about X" without a clear hook for the user. There is a large range of such questions, and the logical character of risk itself is still under debate. We confine ourselves to a few questions that we have more regularly encountered.

This could be of interest to those involved in political risk analysis and consulting, but it is aimed at political risk intelligence users, whose input in terms of the question and tasking can be a significant factor in how useful and logically robust an assessment turns out to be.

The article has five main sections and a conclusion:

- How to focus an assessment when we do not really know key issues in advance (do we cover everything and then decide what is important or narrow it down first?)
- The definition of a risk in the socio-political assessment context (what is a risk versus what is a negative attribute of a situation, and how do we define a risk for actionable analysis?)
- Challenges in measuring and prioritising risks – is the commonly used likelihood-impact framework as straightforward as it seems, and how do we account for other relevant variables?
- The question of residual risk in risk assessment – in political risk, how useful or realistic is it to address residual risk in the assessment phase?
- What if we dispensed with the risk framework and just relied on logic and common sense?
- Conclusion

The problems and questions we address here have actually arisen from discerning client questions, and were common themes in our analytical work over the years. More could be said, and this was selective, but it is a start.

1. What to Focus On? The paradox of having to know enough to know what we have to know

We have seen cases in which an assessment has been tasked as a long, diverse list of predetermined factors which the analysts must consider for potential risk – the user wants to cover all bases, but the result is equal treatment between factors of widely different importance, and indeed much ground covered might not be particularly relevant to the country in question (in one such case the client company apparently had a standard checklist, and discussions towards a more focused approach did not stand up against entrenched practice).

In other cases, an analyst very familiar with the country in question has taken a cursory look at the client's operation, delved into a very detailed exposition of political dynamics in the country, then somehow, as though through the proverbial black box, derived a tiered (and often very extensive) list of risks.

Overkill in detail might be unfriendly to a decision-maker, but it is perhaps not as bad as an assessment that either broad brushes a complex picture, or takes a narrow focus but on the wrong set of issues, or issues already well understood by decision-makers. For example, security managers have been dealing with terrorism risk for years, yet assessments still often get side-tracked by this spectacular type of risk, to the detriment of much needed nuance on less newsworthy but far more prevalent challenges in the operating environment.

Some of these issues derive from a lack of analytical expertise (as opposed to subject knowledge), but these and other problems also arise from the paradox of how to focus a study for best effect when prior to it one does not really know what the important factors are. This paradox has a variety of solutions, and below we only posit a few approaches that have worked for us in the past.

a) Break the problem down into historically relevant risk drivers and look for factors in each that could most affect the operation, then focus on these

This starts with a reasonable profile of the operation that will be undertaken in the target country, in terms of key attributes, assets on the ground, and timelines, to form a workable model of exposure, which then helps to identify when a factor is relevant to the operation.

Then one can work from past learning about common drivers of political risk, and apply those more likely to be relevant to this particular context (e.g. building an airport terminal in a North African country) to create a framework to help narrow the search for relevant factors. Main drivers, depending on the industry and region, could be, for example, conflict, instability, weak governance, regulatory inconsistency, resource nationalism, labour activism, civil society sensitivity, red tape, and erratic or populist economic and foreign investment planning.

Within each broader driver the scan for relevant factors is simpler and more focused than trying to do so at the level of the entire country. Depending on the framework used, there could be some significant linkages between drivers and factors which would have to be considered, and indeed to the extent possible the drivers defined should be as mutually exclusive as possible to minimise overlap and redundancy in analysis.

This approach is not new nor especially creative, but it lends itself well to organising the assessment project (e.g. assigning different analysts to consider different discrete drivers), and one can envision a report wherein the main sections align with the analytical framework. Another advantage is that it relies on established indicators of political risk, many of which are tracked and reported by public organisations and country risk services. It is also quite straightforward to regular users of political risk intelligence. The significant downside is that is there some a priori selection going on – these might be relevant drivers in many similar cases, but some might not be relevant in this case. This is not exactly starting from a blank slate, and there is a risk of focusing too much on irrelevant factors and of missing other issues that are particularly unique to this operational context.

b) Conduct a blank slate initial scan using a basic operational profile, set hypotheses, test, then focus on the most important factors

This is a more scientific approach in the sense that it does not carry as many assumptions into the analytical process, but rather builds up assumptions as knowledge accrues.

Starting with a similar operational profile, the next step is to scan the socio-political environment looking for potential characteristics, actors and trends which could be problematic. This leads to a set of hypotheses about what the relevant risk factors are. Each one is then tested in more detail to see if it is relevant, in other words if it is worth worrying about and assessing in detail. This knocks out some hypotheses, and the exercise is also likely to yield other more relevant ones. The result is

a refined target list of risk factors. These can be organised in coherent categories for purposes of structuring the research and reporting, but the fact remains that the target factors were not pre-assumed according to common wider drivers of political risk, they were derived from the ground up.

The benefits of this approach are that it identifies only the most relevant factors and by not applying a prior framework it might also catch factors that would have slipped through the cracks in more standard checklists. It is, however, a more complex process, and requires discipline in terms of focus, not getting into details too early in the process in order to save nuance for where it matters, and in terms of assessment team coordination. The resulting report would also need to explain to a user why some "usual suspects" in terms of political risk factors were not actually addressed (this would explain why they were of very low relevance to the case at hand). Regular users of political risk intelligence would no doubt welcome a more focused read, but they also come to expect a certain menu and might be surprised to see a different take on their usual fare.

c) Start with assumptions about success and focus on factors these rely upon

This is another blank slate approach, but instead of starting with a concise model of the operation and then working mainly from information about what is going on in a place, it uses the operation as the basis to help to derive relevant factors.

This approach ideally begins with a workshop with people very familiar with the operation in question. They can help to address the question, "What are the critical assets or performance factors of the project, and what conditions, behaviours and trends in the operating environment would have to hold true in order to sustain these factors?" One critical asset for example, is people. To sustain people and their performance, they would have to remain safe and feel secure. Another critical performance factor, for example, is operating permits, and to sustain this, permits would need to be granted within expected or budgeted timeframes, and would need to be respected by inspecting authorities. If these seem too general, one can consider that a roomful of operational managers would even know which specific routes need to remain open in order for logistics to work smoothly, or the number of national staff that they would need to rely on as part of the local workforce. A very robust picture of operational requirements can derive from this exercise, making the subsequent risk assessment very aligned to real needs on the ground.

The next step is to consider what could happen to prevent the assumptions underlying success and sustainability from holding. For example what could make people unsafe or feel insecure, or what could impede the timely granting of operating permits? (As this is a political risk assessment, the focus is not so much on internal errors or weaknesses, but on factors in the socio-political

environment, although the exercise also can yield some useful insights on potential organisational challenges). Similar answers can be aggregated for simplification. The answers at this point could be quite generic, but they still point to relevant types of factors to focus on.

Once we have a long list, they can be aggregated where possible to form relevant types of risk factors, and these can be categorised appropriately for coordination and reporting purposes. Research then ensues to see if and how these factors are or could be present in the operating environment.

As with the approach outlined in b), this one has the advantage of not making prior assumptions, and by starting with the operation first, it is even less prone to preconceived notions of which political risks are relevant. Another benefit is that it yields a more in-depth profile of the operation, so that results are even more tightly wedded to actual exposures. The same caveats apply - it is more complex than more conventional approaches, and it might not be what users are accustomed to, although the latter point is mitigated somewhat if they are involved in the initial process of building success assumptions.

d) A selective combination of the above

The above approaches are not mutually exclusive, and can be used to take a different perspective on the problem. For example, one can use the common risk drivers in the first approach to help organise an initial scan of the environment to set hypotheses. Factors deriving from this can be matched against detailed operational requirements for maximally relevant targeting. Indeed, using the same approach to every "customer" challenge often yields sub-optimal results, and a creative design process taking into account these and other options to focus the assessment is ideal. The issue can be time budget – it seems easier to roll out a standard way of doing things (often approach a), but prior planning for a tight and relevant focus often saves time later on.

2. What is a Risk? Challenges in Socio-Political Risk Definition

In political risk analysis, an art which has traditionally put knowledge about a place or situation before conceptual interpretation, the very definition of a risk can be confused or obscure. Some examples that the author has seen include:

- Equating the prevalence of a broad condition with a risk, for example looking at the prevalence of corruption or ethnic tension in the country, considering it quite high, therefore calling it a significant risk, when in fact the risk is only relevant insofar as it could manifest against the operation and affect it.

- Taking each potential effect of a harmful trend or event and calling it a separate risk – for example a coup d'état might be assessed as a credible risk, deriving from the risk factor of military interference in politics. The error would be to then look at the effects on people, business continuity, reputation, etc. as separate risks, when in fact these are only parts of the wider impact of a coup. This can multiply the final list of risks to unwieldy proportions, and fragment what should be a coherent explanation of the full implications of this one risk, an event which is to some degree foreseeable or estimable and therefore which we can plan to mitigate insofar as it would affect us.
- Equating an existing problem with a risk – one old favourite dealt with a client question on the risk of dual taxation, and as there were no relevant dual tax treaties, indeed it was no longer a risk, it was a certainty. Yet the game had to be played, and the "risk" was duly assessed as high probability and whatever impact, and mapped with the all the other risks. The current downsides of an investment climate need to be elucidated, but once known, they are not risks and the company can take it or leave it, or take it but with some planning to reduce the effect. The only risk when a problem actually exists is not recognising when it starts to go away, and therefore missing out on an opportunity that one's competitors might be aware of sooner. This point illustrates an inherent problem in trying to frame an entire socio-political assessment in purely risk terms - the risk assessment label might be fine, but if not taken without a dose of common sense, the logical convolutions in trying to turn every relevant insight into risk-speak can be painful to both analyst and user.
- Trying to cram a potential negative outcome into a risk box when in fact it is better treated as a scenario, for example "the risk that current instability becomes a civil war leading to widespread insecurity and making the operating area inaccessible". This question is too long-term and there are too many variables involved for it to be a risk, rather it is a potential three to five year outlook, and other outlooks building from the current state of tensions and hostility could be equally plausible. A risk is premised on what might derive from existing or near future conditions and is therefore estimable. When considering long-term shifts in the wider environment, risk assessment necessarily yields to scenario analysis and such contingencies are given full treatment in a more appropriate framework.

There are entire books on risk which help to refine the concept, hence we will provide only a few pointers on how to address some of the conceptual problems above:

- **A risk** is a potential future change, event, or action which could manifest from known trends and conditions; it is uncertain but estimable (unlike a potential future state of full

uncertainty), and if it did manifest it would have a harmful effect on the operation. This does bear a bit more explanation. One could, for example, estimate the risk of an electoral change that would bring a resource nationalist regime to power as 50 % likely. That means it could go either way, and this seems to represent full uncertainty, but it is not the same as saying "Who knows, anything could happen," and in risk assessment 50 % likelihood is actually well on the radar of things we would need to worry about (depending on the impact).

- **A risk is only a risk**, and not just an attribute of the operating environment, when it would harm the operation if the operation were exposed to it.
- **A political risk** is something that happens in the socio-political environment or through the action of a socio-political stakeholder, and while it might have several effects on the operation, each separate effect is not a risk, it just part of the full impact of the risk (and sometimes an impact timescale suggests how to stop the full chain of impact on the operation from occurring).
- **A known problem is not a risk**; it might be a barrier to entry, a hassle we need to live with, or something that we need to plan around, but if it is known and certain, even if it has a detrimental effect, it is not a risk, and is not assessed the same way.
- When a risk is a broad potential change contingent on an array of possible triggers or pressures that could produce a result beyond the estimable horizon, it is best incorporated into a **scenario analysis**; "risk" is a better concept when looking at how a relatively well defined situation could affect us (albeit given short-term variances), while scenarios are more useful when looking how that situation could change over time.
- While we are on the subject we will raise another point, the concept of **upside risk**. This refers to investing in a situation when one recognises that the outcome is uncertain, and betting at least somewhat on it turning out well – upside risk is that it could turn out well. This has led many commentators to propose that risk is "neutral" and simply refers to uncertain but reasonably estimable outcomes that are relevant to one's interests. What this seems to be referring to from our perspective is that even though things might not work out for us, we still commit some resources in the event that a situation evolves in our favour, in other words we **take a risk**, which means that we do something in spite of the potential downside. The conceptual difference between risk as a potential negative and upside risk is hazy, and while in certain political risk cases directly dealing with upside risk makes sense (for example if a future election could bring to power a regime dedicated to ending foreign sanctions and improving the investment environment, but we are unsure of the outcome), it

can complicate an analysis considerably when it is misused or simply replaces the notion of window of opportunity.

- One final point on defining risk – there has been some tendency since the inception of ERM (enterprise risk management) to create extensive "failure to..." lists as part of the pressure to fill risk registries, e.g. "failure to hire the best talent, failure to identify new opportunities, failure to set prices correctly..." In other words, failure to do one's job as a competent business. This seems to be just the inverse of a basic checklist of necessary competencies and tasks. "Failure to" is best left aside during a political risk assessment, which focuses more on external variables far less under our control, and better approached in a risk management planning phase (The main exception to this is when considering risks to reputation, which almost always involve a mistake made by the organisation, and a re-interpretation of the mistake in the socio-political environment. For example, taking "closed door" deals to expedite a project can often lead to allegations of ethically dubious behaviour and lead to a loss of credibility and even protests based on allegedly unfair practices).

3. Measuring and Prioritising Risks

Using a risk assessment framework, or positioning challenges or issues as risks, necessarily leads to measurement and prioritisation. Challenges and issues can be prioritised as well, but "risk" strongly implies that something can be more or less risky than something else. This is another area of political risk management where method and concept often have not kept pace with subject matter expertise, and political risk analysts often use off-the-shelf approaches which are not strongly linked to a preceding narrative, and which can oversimplify or confuse a final result.

This section first examines the use of a stock tool of the trade among many analysts, both in-house and among advisory firms, the impact-probability framework. It then looks at risk prioritisation approaches, how to factor in time sensitivity, and how to handle stakeholder intelligence in a risk assessment framework.

a) Challenges Using the Likelihood-Impact Framework

Not everyone does it this way but it is common, and users are often familiar with it. Indeed the likelihood (or probability)-impact framework shows up in most basic texts or manuals on risk assessment. It seems to date back to the 1960s when management models were making their entry into strategic and policy planning, and since then has not changed much.

The idea is that through research and analysis, risks are identified, then assessed for the likelihood of their occurrence within the relevant timeframe (perhaps the duration of a project or a phase), and impact on the organisation or operation if the risk did manifest or occur.

Ideally, after risk identification, the whole assessment would be structured towards discerning likelihood and impact, and clearly explaining the relative ratings for each, so that the final risk prioritisation based on these variables would be crystal clear to the user. To derive relative risk severity, the ratings for likelihood and impact (each on a scale of 1 to 5) are combined, and those with higher overall scores are the most important ones to focus on. Then the results are mapped on a matrix with likelihood on one axis and impact on the other. Risks further into the upper right corner are more severe overall, while those towards the lower left are less severe. There are other nuances and it can be expected that the rating system is well explained with indications of what each rating means (in terms of intangibles such as personnel security and reputation, and in terms of potential loss or financial implication), but this is the approach in a nutshell.

One problem is that once an organisation knows about a risk (for example right after reading the report or getting a briefing) their chances of being exposed to it change, as do their preparations to address it if they are exposed (see later on residual risk). This framework does not account for the immediate impact of the intelligence on the user, and generally assumes a blank slate in terms of the user's knowledge of risk.

Another challenge involves how to account for seemingly small but actually important variances in the precise conditions underlying a risk event or condition, both in terms of the operation's exposure and the degree of manifestation of the risk. This can lead to some overlap between likelihood and impact assessment, and this overlap can challenge a clean outcome where these two axes are mapped against each other to define priorities.

For example, "A terrorist attack is likely, but unlikely to affect X because X is not in the usual target area and local terrorist groups have not defined foreign companies as a target set. At most, an attack would result in a temporary crackdown that would affect public transport. Thus, for X specifically, a terrorist attack in terms of risk to X is actually unlikely." So a terrorist attack might well happen, but looking at X specifically, exposure is minimal so the impact is minimal, hence the likelihood of this being a problem for X is low. By now we have already partly addressed impact too.

This sounds awkward, but consider the alternative of stating simply that a terrorist attack is very likely, 4/5. Since the assessment is done for the organisation in question, there is an implication that a terrorist attack is a likely problem for X, when in fact it might not be. Perhaps the question could

be framed as “The risk is a terrorist attack that directly affects X’s operation” but then the definition of “directly affects” would still need qualification and that gets into the chain of impact.

Assessing impact can also lead to spillover with likelihood. Do we assess it based on what we know about the organisation’s exposure and security measures, or do we assume that they are sitting on the bomb when it goes off? If we start to factor in exposure and vulnerability, as we probably should for the sake of realism, then we are in fact taking in assumptions about the probability of X being exposed to whatever degree when the risk event occurs, and we likely need to make other probability assumptions about the event as well. For example: X is a mining operation in a far flung corner of Mauritania, and the road there happens to cross a transit route used by armed smugglers; we might assess an encounter with an armed convoy as high impact, but do we assume that one company truck runs into a small army of well armed smugglers? We would have to list our conditions:

- It depends how many of X’s people are in the company convoy that encounters the smugglers – the more people affected, the higher the impact
- It depends on whether or not available convoy security that day is stronger or weaker than the smuggler contingent
- It depends on whether or not the smugglers have time to stop for a raid or care to bother with a kidnap, which can be lucrative but also a hassle especially when the smugglers are on a high-stakes and dangerous drug or gun run and would not want any distractions

Each of these would entail an estimate of the probability of certain conditions being met for the impact to be high. Ideally we would know what likely conditions would apply. If not or if there is variability, one could vary each condition and re-assess impact and perhaps take a median case of exposure and mutual behaviour based on recent history. We then build an impact from the mini-scenario we just created. But in so doing, likelihood of certain enabling conditions has been assessed, and therefore too the likelihood of a certain impact manifesting.

It is not so much that the above convolutions are wrong, as that they might be inevitable when trying to deconstruct a risk into two simple variables. In fact, in estimating a risk there is a range of conditions and causal linkages that need to be considered, and assumptions need to be explicit (Bayesian analysis might work for some well defined risks, as do other models such as competing hypotheses, but these might not work well in a broader risk assessment). Many analysts gloss this over by not even trying to explain exactly how a given rating was derived – they think about, probably slap the risk on the matrix first, see how it looks, then go and fill in the rating. This

subjective approach might yield decent judgement-based results in the end, but the whole idea behind using an analytical framework is to control subjectivity and enforce reliance on corroborated, qualified intelligence, not just to provide a slick veneer.

How have we addressed this challenge? We have made it clear that the likelihood-impact framework has limitations and is a general depiction of priorities based on assumptions about underlying conditions. We have constructed mini-scenarios that we regard as median or average given the type of risk and exposure, and making assumptions clear have derived ratings on that basis. For risks for which there could be considerable variance in conditions, we have mapped an "average" risk but included other positions in terms of overall severity, kind of a cluster of risks within a more hazy grey blob that positions the general risk while taking into account variations in underlying conditions. When discussing exposure, we try to transfer that to the impact side, and avoid questions of probability based on exposure to an event or condition – likelihood is of an event or condition manifesting, while impact accounts for impact on what / whom. It is a general model and is useful, but it needs to be caveated and handled with caution and explanation.

b) Deriving Overall Severity

In the likelihood-impact framework, a risk's severity is the intersection of the two variables, the likelihood of a risk manifesting, and the impact if it did manifest. For example a risk of very high likelihood (5) and high impact (4) would be 20 on the severity on the severity scale. Risks are then ranked to derive a list of top priorities. How to combine the two numbers has been a pain for many analysts, but in the end, a bad thing multiplied by its potential to occur means the risk is a multiple of its factors.

One question that has arisen from clients is why a remotely probable risk that would be catastrophic were it to happen might not rank among the priorities. This is not really a fault with the model, but more an indication that not every person or organisation is going to look at risk the same way. Those with higher risk appetites, for example, might be content to take their chances and not invest in mitigating the risk, while others would seek to at least have contingency plans in place to address it. How the relevant team or organisation feels about risk can be factored into its risk management planning, but it should not influence the blank-slate prioritisation, which should stand as an independent reference point.

Another question concerns linkages between risks. Quite often the likelihood-impact matrix will be peppered with risks, many of which are linked in terms of inter-causality and also the kinds of exposures they affect and the means of dealing with them. This could complicate prioritisation from

a risk management perspective. Again, an independent final assessment result should stand as a reference point, but once an assessment moves into planning, then these linkages can be taken into account to form broader, manageable sets of issues that lead into integrated risk management programming, rather than approaching each risk as a discrete problem. Original assessment priorities should still be reflected, but ideally the "to do" list is more coherent. In cases where an analyst has small variations in risks represented as separate risks, there is an opportunity to condense, but this needs to be carefully considered to avoid losing a necessary insight.

c) Factoring in Urgency or Time-Sensitivity

One thing the results of the likelihood-impact framework will not show is the urgency, in terms of what is near-term and what can be handled on a more evolutionary basis, of different risks. For example, petty corruption might be a low severity risk, but it could affect personnel as soon as they hit the ground. Labour friction, on the other hand, might be a severe risk but it takes time to build up, and can be addressed as a long-term programme. Another example: If an election is around the corner and there is likely to be electoral violence in the operating area, then addressing this is particularly urgent.

There is no point in trying to cram urgency into the likelihood-impact framework, but it needs to be a close corollary, because overall risk severity alone is not the only in factor in defining priorities, at least in terms of what to do first. When formulating recommendations, time sensitivity needs to be considered. Additionally, there needs to an examination of options for sequencing risk (and stakeholder) management initiatives such that by addressing some risks early on, other related risks are potentially reduced (as noted earlier, causal linkages can be considered at the planning stage).

d) How Does Stakeholder Analysis Fit with the Likelihood-Impact Framework?

Looking at near-term risks that could arise through trends and conditions in an environment is only one aspect of a comprehensive socio-political risk assessment. Along with scenario analysis looking at long-term change of the wider environment or key elements therein, stakeholder analysis is often a critical component of a more detailed analysis, and helps to inform users about the actors and interests they could be facing and need to adapt to. The outcome can be regarded as a separate corollary to the risk assessment, but useful insights on risk are often derived from a stakeholder analysis, and it can be beneficial to factor these into the wider risk assessment.

On the surface, the likelihood-impact framework is not set up to handle inputs from a stakeholder assessment. Stakeholder assessment often relies on capability-intent / attitude-influence models to derive priorities, along with linkage mapping to discern comprehensive interest groups. The

question, then, is how to account for the outputs of a stakeholder analysis in a wider risk assessment framework that includes risks inherent in the socio-political environment?

In our past work, in some cases we have completed what we call the “terrain risk analysis” focusing on exogenous risk inherent in the environment, for example quirky and changeable FDI regulations, weak governance including corruption and poorly resourced bureaucracy, and local or national power contests that could lead to unrest and violence. These indicate certain risks to an operation exposed to them.

Then we undertake the stakeholder assessment, looking at who matters to the operation and why, and actions that important or hostile stakeholders could take which could help or harm the operation. The potential harmful actions are stakeholder risks.

Finally, at risk of over simplifying, we line up all terrain risks in one column and all stakeholder risks in another and look for similar risks occurring in each column. Very similar risks between the columns are aggregated. When a stakeholder risk is a very specific manifestation or unique sub-type of a wider terrain risk, then it might remain as a separate risk (e.g. bureaucratic corruption pressure is a terrain risk, while among the stakeholders we would deal with, Ministry X has a track record of seeking kickbacks on bonus payments – this is so unique from general bureaucratic corruption that it remains as a distinct risk in the final aggregated list).

Quite often a standalone stakeholder analysis will focus on prioritising stakeholders for engagement (or in the case of hostile actors for deterrence or attitude modification), and a final risk assessment is not part of the process. But there is an opportunity to use the stakeholder element to refine an overall risk assessment and make it more nuanced and comprehensive, without adding too much additional “noise” to the final outputs. Similarly, even in a “stand alone” stakeholder assessment, a risk assessment can be useful to capture the potential downsides of stakeholder reactions.

Addressing Residual Risk – Necessary or Redundant?

This question pertains specifically to political risk analysis - the notion of residual risk might have clearer and more actionable definitions in finance and internal health and safety (and more technical areas), but with respect to political risk it presents problems.

Sometimes a user might expect an analysis to include the residual risk concept, or sometimes an analyst thinks that to be comprehensive and align their work with whatever manuals they have read, residual risk needs to be factored into the political risk assessment.

This is the idea as it is often applied:

- The risk assessment is conducted as though the operation and its managers were unaware of the risks and have taken no steps to mitigate them
- Then risk tolerance is examined – what can the operation afford to leave to chance, i.e. what level of risk or types of risk can it accept, and where is risk mitigation required to pull back overall risk to within tolerance levels?
- When it comes to recommendations, a round of mitigation steps are proposed, then ratings are adjusted to see if these bring overall risk within tolerance
- If not perhaps there is more finessing
- The final, final risk assessment yields ratings based on recommended actions having been taken (in theory depicting the risk remaining after mitigation measures have been put into place, and potentially giving users a chance to say "oh, no, that's not good enough, let's have another round of testing mitigation options to see if we can draw that back a bit..." and on it goes, relying on descriptions of risk management initiatives and resourcing that do not even exist yet to try to refine a fit with some "red line" overall tolerance level)

This might be a handy thought experiment in trying to decide on how much resource to dedicate to risk mitigation and where, but as an analytical exercise in the fast game of political risk, it can lead to some severe convolutions and a lot of extra work and user reading for not much additional value, if any.

One problem is that we are ignoring the observer effect when we discount a user knowing about the issues – as soon as they know (upon reading a report or getting a briefing, as mentioned earlier) then they will change their behaviour from unaware actor to aware actor, and we suggest that it is nearly impossible for an analyst to do an initial assessment on the assumption that the user is ignorant of the circumstances and does not have an existing risk management capacity (initially they knew enough to commission an assessment).

Another issue is that the hypothetical mitigation measures applied to bring down overall risk to within risk tolerance are not even planned yet and are highly speculative, especially if each risk is considered. Unless firmly in the stage of risk management planning where concrete capabilities and levels of experience are under discussion, the risk assessment itself is not the place to toy with mitigation planning simply as a way to move a red line on a matrix to some acceptable position.

In the end, while it might seem to be thorough, going through the process of "raw risk minus mitigation = within tolerance – Yes, stop, No, re-do..." seems to be unnecessary and to rely too much on hypotheticals.

There are even some models of risk assessment which take vulnerability and preparedness into account as part of the assessment framework. For example imagine a tabular format that includes:

- Risk A (e.g. corruption pressure by ministerial official, or terrorist bomb in capitol where we have our country office and rely on the port for equipment imports)
    - Risk situation, how it could manifest (situation description and plausible sequence of events)
    - Potential exposure to such an event or new condition: ?
    - Likelihood of this situation arising (taking causal linkages into account): ?
    - Impact if the situation manifests (based on exposure): ?
    - Preparedness for / vulnerability to risk manifestation (avoidance might be a foregone conclusion at this point, but in terms of prevention and mitigation response): ?
    - Mitigation options to plug preparedness gaps and reduce vulnerability

After doing this exercise for each risk (or main risk), then we can have a look at available resources in terms of management attention, time, external support contract costs, etc, and see how these are most effectively spread to reduce as much overall risk as possible. If the risk assessment includes at least a preliminary risk management planning element, then some take on the above framework is more workable than an iterative process to narrow down overall risk severity to some tolerable level based merely on hypotheticals.

In our experience, it is far better to have a reasonable understanding of the operation's exposures, then do a risk assessment on the basis of at least some common sense risk awareness. And only then to come back with a fresh start in a second phase focusing on risk management planning, a phase dedicated not only to generating, refining and integrating options, but one in which real risk management experience and capability can be addressed and considered in detail. But if initial planning indications are required in the assessment, then there are certainly better alternatives than trying to finesse some acceptable level of residual risk based on hypothetical and unknown risk management capabilities.

4. What if We Just Used Logic and Sound Intelligence Skills Instead?

The final point is not really a logical problem, but a question for both users and advisors – is a risk framework always the best approach to questions about an operation's challenges and sustainability in volatile socio-political terrain?

Intelligence agencies and strategy consultancies could easily put a risk spin on nearly everything they do, but instead they tend to focus on challenges and opportunities that could arise or be created, and what the operation could do about them. In the political risk context, this would rely on a solid intelligence process (e.g. some variant of precise intelligence targeting, credible sourcing, collation, corroboration, analysis / qualification) taking the user's operation as the subject, and would address such questions as:

- What socio-political dynamics and actors are relevant to the operation?
- What plausible situations could arise that would affect the operation?
- How can we avoid, prevent, manage (or in the case of opportunities exploit) such situations?
- How do we best address the principal challenges to make our operation more sustainable?

Within this framework, we might speak of challenges, issues and contingencies, and might use "risk" and "threat" in common sense terms, but we do not frame the entire discussion around the concept of risk.

This is liberating in many ways, and opens the door to creative project design that addresses the user's concerns without spending considerable thinking, time and text on formulating every relevant variable as an aspect of risk.

Experienced users of political risk intelligence might be biased towards what they are familiar with, but as much of the preceding sections make clear, trying to use risk-speak for the complex dynamics between an organisation and its socio-political environment can be awkward, and end up with logical digressions aimed at fulfilling a strict risk-based interpretation when an approach based on robust intelligence and logic aimed at facilitating an objective in the face of challenges would be more flexible and often far more concise.

Every analytical project needs a design, and models help to capture a complex picture. But there are many options in analytical design and approach, and as long as the core principles of relevance to the user's operation, robust intelligence, and internally consistent logic are applied, the best analytical approach is the one that yields actionable insight using the most straightforward path. That is not always a risk-based framework, and users, analysts and advisors should keep an open

mind when it comes to analytical frameworks to address the socio-political intelligence needs of an overseas operation. Relying too heavily on past practice or off-the-shelf frameworks might mean that we are trying to cram a unique problem into something that we are comfortable with, rather than adapting our approach for best fit with the challenge while still adhering to the tenets of sound intelligence and analysis. Indeed, one difference between risk consultancies and strategy consultancies is that the one tries to position the answers as risk resolution, and the other aims at pointing out what needs to be done to achieve the objective.

Conclusion

Thinking about thinking is a critical factor in how we focus and conduct intelligence gathering, and analyse and derive actions from refined outputs. With nearly ubiquitous access to open source intelligence via the Internet, basic information is a commodity. There is a often rush to learn more about what we hear of in the news, and a rush to meet this superficial demand. That might form a niche area of political risk intelligence, and the issue of appropriate analytical frameworks and internal consistency, not to mention corroboration and qualification, perhaps need not be as stringent. When it comes to high-stakes decisions and planning for a safe and sustainable presence in a complex environment, the standards need to be revised, and the question of thinking about thinking becomes all the more pertinent. The political risk “state of the art” when it comes to advising specific operations might benefit from questioning old assumptions and looking at more creative and logical approaches to providing actionable value.