ethicsinsight

# Beyond the Surface:

In-Depth Risk Assessment for Serious Investors

## The background

We reviewed five years of pre-investment risk assessment, gap analysis, and due diligence work to identify some of the best questions to ask to determine integrity, political and security risks.

When we ask these questions, we consider not only what the PortCo tells us but also how.

Deception detection, investigative interviewing, and behavioural analysis may seem unusual skills to bring to pre-investment due diligence, but these insights (the truth behind the words) help most.

They allow you to make the right decisions and help the PortCo uncover gaps in thinking, understanding, or action. The right questions lead to better, stronger, and more valuable companies.

## What's not there

The image below is a metaphor for our approach. As the US Air Force suffered high losses during the WW2 bombing campaigns, they studied returning aircraft, mapping the damage. The intention was to strengthen those areas until a statistician, Abraham Wald, pointed out that reinforcing those areas without the holes might be a better bet; planes with punctures in these parts had not returned. In our work, we look for what is there and what isn't.

Let us know if you'd like some quick tips on behavioural analysis basics before you start interviewing the PortCo management team. You can also check out our regularly updated resources using the 'tree' link in the footer 👇.

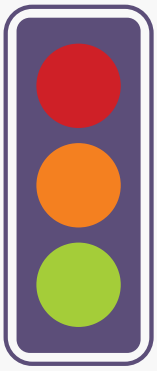
## Contact

www.ethicsinsight.co
hello@ethicsinsight.co

# Top 10 Business Integrity Questions

The questions that follow include detailed considerations. If you'd like to score each question, you can use the framework in the table below to help you prioritise which areas to work on with the PortCo.

| SCORE | DESCRIPTION |
|---|---|
| LIMITED | Nothing or little in place. |
| MODERATE | Inconsistent, not yet complete, or in the process of implementation. |
| EFFECTIVE | Controls are implemented, monitored, and tested. |



| Question | What to consider |
|---|---|
| 1. How does the company tailor its business integrity framework to address sector-specific risks? (For example, interactions with healthcare professionals for pharmaceutical companies and land acquisition issues for renewable energy projects.) | Many companies inherit legacy risk policies and frameworks (from previous investors, boilerplate legal shops, etc.). The danger is that these either provide a false sense of security or get ignored as they are (largely) irrelevant. By asking about "the framework", we get beyond ill-fitting policies and ask about risk management, which can often be effective (if informal and reliant on senior management judgment). From here, we can build something that enhances existing capacity rather than binary "Do you have Policy X?" questions. If you need a blend of "Do you have…" and implementation questions with varying ways to answer, we've included some in this Compliance Maturity Scorecard). When we have to think about the answer, we pay attention. When we can tick a Y/N or pick a point on the same Likert scale, our brains default to autopilot. |
| 2. How do you conduct background checks on third parties, especially those operating in high-risk areas or interacting with government officials on the company's behalf? | Again, in many PortCos, there will be informal processes to vet third parties. For instance, the leadership team might leverage their network to conduct informal reference checks, often more illuminating than traditional DD, which rely on trawling media in jurisdictions without a free press. To understand how these (informal) processes inform decision-making, we need to consider decision-making quality, not outcome. It's possible to arrive at positive conclusions through luck rather than judgment. Reviewing the process for decisions might reveal this. |

ethicsinsight

# Top 10 Business Integrity Questions

| Question | What to consider |
|---|---|
| 3. How does the company ensure its speak-up/whistleblowing mechanisms are accessible to and trusted by all stakeholders, including employees, suppliers, and local communities? | This should be a difficult question to answer. In most cases we've worked, PortCos will answer "yes" to the "Do you have..." question. A grievance box onsite, an email buried in the Code, or a phone number no one rings are ineffective speak-up mechanisms. If we can probe to understand if these systems are used, how often, by whom, and with what sorts of issues are raised, we can start to get the data we need to inform education, training, and tone from the top messages on speak-up. |
| 4. What steps has the company taken to integrate business integrity considerations into its operational processes and decision-making beyond policies? | Potential investments want your money. They will say and show what you want. You'll get policies (document review) if you ask for them. Here, we need to see if these are actually integrated. For example, having a gift and hospitality limit in the anti-bribery policy is good, but it's meaningless if you don't have the associated expense approval and recording processes. |
| 5. How does the company monitor and audit high-risk transactions, such as payments to government entities, donations, or sponsorships? | Most companies we've dealt with are increasingly aware of the risks associated with gifts and hospitality. Some of that risk has migrated to donations and sponsorships (spurious NGOs to the local mayor's football club, etc.). What gets measured gets managed. We need to know what sorts of financial transactions are subject to genuine scrutiny (four eyes, approvals, reconciliation, monitoring, etc.). |
| 6. What processes exist to identify and manage conflicts of interest, especially in contexts where personal and business relationships often overlap? | Every business we've worked with (from so-called squeaky clean markets to the most challenging) faces a conflict of interest challenge somewhere. WFH and side hustles may be the latest variety, but in most growing PortCos, you'll have a tight management team that relies on connections, referrals, and recommendations to get things done. That can be great, but it can also get messy. Conflicts of interest only become an issue when the potential for one isn't disclosed and dealt with. Many PortCos have nothing in place here; check. |
| 7. How does the company ensure its business integrity expectations are communicated to and understood by employees at all levels? | When leaders of the PortCo have (or had) their boots on the ground, they will often have excellent (if informal) methods to communicate to frontline employees about risk. When the management team are distanced from that operational day-to-day, you'll hear phrases like "We have an induction program..." Think back to your induction; how much of it do you remember? One-and-done training is largely useless (research on why here). Find out how well issues are communicated (if you don't know, consider asking employees to complete a survey like this). |





ethicsinsight

# Top 10 Business Integrity Questions

| Question | What to consider |
|---|---|
| 8. What measures has the company implemented to prevent and detect fraud in areas like inventory management, asset write-offs, and expense reporting? | Fraud is the forgotten risk child. In an investigative capacity, we see more fraud than any of the big scary risks (corruption, sanctions, human rights abuses). Yet we see near-no maturity (across the board, right up to listed entities) when managing the risk outside of a small group for whom it's a reputational killer (e.g., banks helping consumers avoid scams). Some statistics suggest fraud costs between 1%-5% of revenue in average businesses. The exact amount doesn't matter. Even if it's only 0.5%, most companies would love that back on their bottom line. Ask sector and business-model-specific questions about fraud. Stuck on what to ask, we put together a comprehensive guide here, with an accompanying assessment here. It's pitched at the mid-cap market, so remove questions that will be excessive for smaller PortCos. |
| 9. How does the company approach facilitation payments in markets where they may be common? What guidance and support does the company provide to employees facing such demands? | The "just say no, kids" approach to facilitation payments in many zero-tolerance policies is unhelpful, at best. Requests are often extortive, and the other party has leverage. "So you don't want your goods to perish on the dockside while I delay processing? Pay an express fee then." The PortCos that manage this risk well train the frontline people who face these threats. The training is a mix of negotiation strategy, deflection, and making yourself a hard target (corrupt officials generally don't want to work much for what are usually small amounts). Ask how the PortCo manages this risk, not what's on paper. We all know it still happens. |
| 10. What processes are in place to ensure that lessons from past incidents or near misses are incorporated into the company's risk management framework? | This question is intentionally presumptive. Any organisation of a size where you're considering investing will have experienced some sort of issue (HR, compliance, security, safety, etc.). That's fine. Learning from it is what counts. Many organisations, including the large ones, are weak at root cause analysis and remediation efforts. So, don't judge PortCos too harshly here. We want to sow the seed that learning lessons is one of the most essential ways to rightsize risk and make it relevant to our people. |

These questions go beyond basic policy checks to probe how companies operationalise and adapt their business integrity frameworks to their specific risk environments. They focus on critical themes like third-party management, a speak-up culture, operational integration of integrity considerations, and continuous improvement, as we've observed that these areas are consistently challenging.

ethicsinsight

# Political and Regulatory Risks

In some projects, you must factor in political and regulatory risk. For instance, in disruptive sectors where the legislation has yet to be (appropriately) written, like telemedicine, AI, and fintech, we can find that the most significant risk to a potential investment is regulatory. Capricious politicians might also turn an extortive eye your way in other sectors, especially those involving critical infrastructure or land. These issues are usually only relevant in a minority of projects, but they can be the most catastrophic - ending businesses almost overnight.

Having built up Control Risks' political risk team in a past life, regular work involved predicting whether things will get better or worse when/if an incumbent administration changes. That's the wrong question. Most political and regulatory risk is not so binary. There are triggers and indicators along the way. Ask questions to get to that detail.

| Question | What to consider |
|---|---|
| **11. How does the company anticipate and respond to changes in political administration or regulatory landscape?** | If the PortCo is actively involved in industry associations or policy advocacy groups, that's typically an indicator they've identified the risk already. If not, you may need to lead their thinking a little here. "What happens if the proposed legislation around telemedicine prohibits public sector healthcare professionals from freelancing as private telemedicine consultants to protect the already stretched public hospitals?" If they aren't formally thinking about political and regulatory risks, they might have business continuity (and crisis management) plans that could be purposed to manage these risks. By discussing broader continuity threats, we can often start the process of planning for other risks. |
| **12. What mechanisms are in place to manage potential extortive requests from officials during licensing and permitting processes?** | Here, we're talking about major political risks. For example, politicians struggling for re-election might extort local businesses, threatening to cancel or frustrate concessions. Political risks tend to escalate - contract frustration or expropriation seldom happen overnight. Again, this question is designed to get the business thinking about stakeholders and dialogue. Businesses that navigate politically volatile situations successfully often have broader local community support. |
| **13. How does the company ensure compliance with local laws and regulations across different jurisdictions?** | In many jurisdictions, what's written into laws and what is enforced aren't linear. Companies that successfully maintain constructive dialogues with the enforcers fare best. For instance, when healthcare regulations appeared to overlap as the China healthcare clampdown sent shockwaves across Southeast Asia, we worked with a company that asked the enforcers, "How do you want us to comply?" and offered different options. Keeping a record of these conversations and maintaining communication can ensure continuity, even in turmoil. |

# Security Risks

For some investments, security risks will be a factor. Perhaps they have physical assets that attract (organised) criminals, like scrap metals, pharmaceuticals, or high-end consumer goods. Or maybe they operate in unstable or remote regions (e.g., agribusiness, renewables, resources, etc.), where they represent a source of funds for corrupt security forces, insurgents, terrorists, or other hostile non-state actors. Again, this is not a risk you'll come up against in every investment, but even in seemingly benign markets, we might see noteworthy security exposure in around 40% of investments. For instance, we worked with an immunotherapy firm with pioneering oncology treatments. Their facilities in Northern Europe were relatively poorly protected, and unvetted scientific researchers could easily enter some of the labs. The company was concerned about intellectual property theft until one of the researchers explained that some of the test samples could become weaponised pathogens in the wrong hands. That changed the security conversation.

| Question | What to consider |
|---|---|
| **14. How does the company assess and mitigate physical security risks?** | Unfortunately, in many cases, security personnel are not the tip of the spear. Having a few CCTV cameras, keycard access, and a somnolent ex-cop on the door might be inadequate. Security is a function of physical and electronic controls, predictability, and responsiveness. Ask questions about those latter categories. For instance, if the scrap metal stock count is predictable, that becomes an exploitable weakness. Or, if the response time to out-of-ours unauthorised access to IT systems is the following morning, that's a serious window for exploitation. If the PortCo outsources all of this, probe. The most horrible cases we've worked on (including those where people were murdered) involved complicit, outsourced security personnel colluding. That's the worst case. In many markets, a more likely case is that the outsourced personnel are corrupt cops moonlighting. |
| **15. How does the company secure its supply chain and third-party security exposure?** | Cybercriminals will now look to supply chains (and third parties) to penetrate security (the weakest link). For physical security, it's a similar proposition. Key risk areas will usually include transport, warehousing, and logistics. Similarly, don't ignore the human factor. It's normal to gravitate towards physical or technological controls, which have their place. But in our experience (including hunting spies from hostile states), the social engineering element is always more of an issue - humans are easier to compromise than systems, and insiders will know the weaknesses that random penetration testing would take too long to reveal (this very brief checklist might help get you started). |

These questions should get you started, but if you have questions or particular areas of risk you'd like to discuss, schedule a call here.