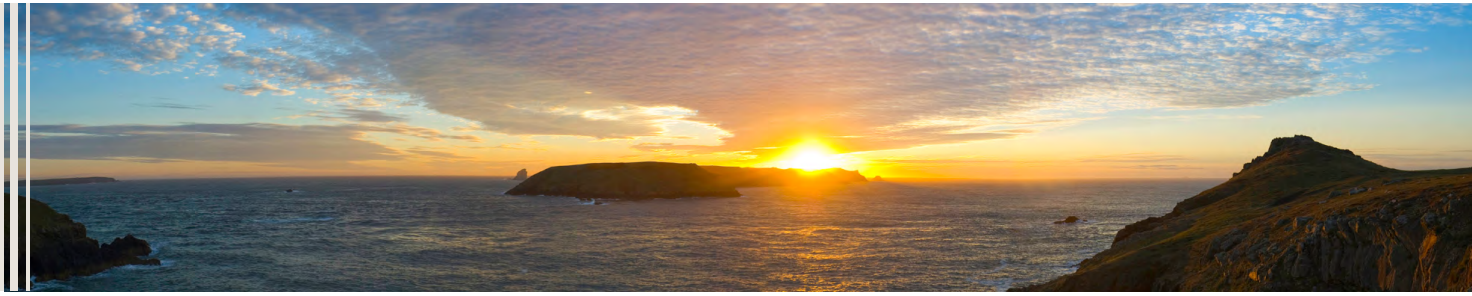
Linklaters

Risk Insights from Linklaters' Operational Intelligence Group
2014



* This PDF is best viewed and printed in landscape

Introduction

2014 will undoubtedly see the regulatory landscape for large, multinational corporations continue to shift, both in terms of the trends in regulators' behaviour and the specific, major pieces of regulation that will be introduced. In this, our inaugural insight, we look ahead and identify regulatory trends we anticipate for 2014 and their implications for large corporations.

We anticipate that regulators, in both developed and developing economies, will ratchet up their expectations of corporates, which will result in more extra-territorial enforcement, further aggressive levying of fines, and an ongoing trend towards the regulator-cum-lawmaker. More than ever, adapting to the more dynamic and holistic regulatory environment and demonstrating continuous improvement in compliance is key for corporates in order to stay ahead.

Companies also need to recognise more fully the nexus between social media and regulation. Social media is not simply a new mouthpiece for an old message, but is exposing entirely new aspects of business to public scrutiny. Companies likely to be the subject of NGO interest – and that means most multinationals – should consider their engagement plans carefully.

In the fields of, antitrust and anti-bribery, data protection and cyber-security, important, specific trends are worthy of companies' attention.

> "More than ever, adapting to the more dynamic and holistic regulatory environment and demonstrating continuous improvement in compliance is key for corporates in order to stay ahead."

★ Key points

> Legislators continue to tighten anti-trust and corporate governance requirements across emerging market jurisdictions. We are also seeing more regulatory activity in areas of public concern - corruption, product standards and anti-trust.

> Regulators will be keener than ever to use their powers to shape corporate behaviour. This will be a global phenomenon, not just limited to developed economies.

> Regulators globally will remain much more likely to show leniency if an organisation can show that it has a considered and well implemented governance and compliance structure that failed on a particular occasion, than if governance and compliance is out of date or poorly implemented giving rise to "systemic concerns". A well designed and adaptable structure is an important risk management tool that organisations should embrace.

> 2014 is expected to see the EU bring in legislation which will lead to the biggest shake up in privacy law for 20 years – the impact on global corporations will be substantial.

> Recent aggressive interpretation by the European Commission on what constitutes a "cartel" will have significant implications, especially for commercial practices in the financial, extractive and commodities sectors.

> Cyber security (and the need to take action) will step up a pace and will come to the front of boardroom agendas, backed by legislative discussion at an EU level.

Great expectations

Globalisation and brand power have created corporations known across the globe, with governments competing for their intellectual and financial capital and the contribution they can make. However, with such status also comes elevated expectations, which translate into increased responsibility and risk.

Regulators are keener than ever to use their powers to shape corporate behaviour – either by increasing public pressure on companies through increased disclosure in key areas or by the imposition of ever larger fines and sanctions.

Fuelled by increasing politicisation – the need not just to change, but to be seen to change, corporate behaviour – and a desire to find further revenue streams, the consensus has been that regulators would continue to broaden their remit. Indeed, as we have identified in the specific instance of the cartel developments described below, their reach is becoming much wider than many would have foreseen even a few years ago. The trend towards the publication of "guidance", rather than black-letter law will continue, giving the regulator much more flexibility and, accordingly, power.

Regulators in developing countries will increasingly flex their muscles in a bid to quell unease at home about domestic corruption (and no doubt also incentivised by the potential revenue stream). We saw this in China last year with the focus on allegations of corrupt payments in the pharmaceutical sector, vigorous investigations of suspected anti-competitive practices in a broad range of industries by the relevant agencies (NDRC and SAIC), and the continued growth in power of the merger regulator, MOFCOM, exerting influence (and delay) even where the transaction had no obvious link to China. Brazil will bring in anti-bribery and corruption legislation this year. We expect some of the more developed African nations to follow suit. Multinationals should expect to be the primary focus of enforcement activity in emerging economies and plan accordingly. This may also be accompanied by greater scrutiny of their activities by their "home" regulators in such new and emerging markets. They should take particular care with regard to community investment mechanisms, as corporate scrutiny of these can be patchy, the scope for corruption significant, and the potential impact on social licence to operate, disproportionate.

But it is not just about combating corruption. Governments of developing economies are also keen to focus on governance and corporate culture and are looking further afield for best practice precedents. In India, for example, new legislation will make it mandatory to have at least one female board member and listed companies above a minimum turnover are required to allocate 2% average net profits to corporate responsibility activities or explain why not.

In developed countries, regulators are likely to broaden their remit to focus on corporate culture more generally.

"Regulators in developing countries will increasingly flex their muscles... Multinationals should expect to be the primary focus of enforcement activity in emerging economies."

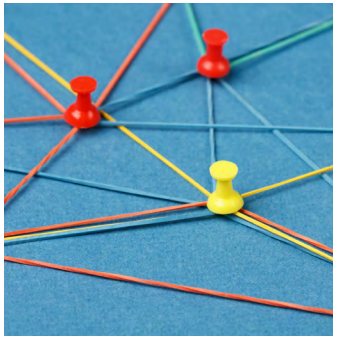
> As fines begin to be calculated as percentages of group global turnover, it will become more vital than ever to ensure that your carefully crafted policies do more than sit on your computer screens.

Concepts initially developed in financial regulation will influence regulators in other sectors. In addition, for some years now, regulators have had the opportunity to scrutinise examples of best practice systems. Companies should therefore expect the bar to be raised in terms of what "good" looks like. We have also seen regulators, such as those in the US, extend the armoury of weapons they are willing to use – from censures to fines, to potential debarment from public contracts and even the use of immigration and visa laws in order to increase leverage in other areas.

Whether to induce public pressure on companies by requiring disclosure on key issues (such as payments to governments or the number of women on boards, for example), or to force boards to focus on certain issues that regulators themselves think crucial (for example company audit issues), we anticipate increased disclosure requirements and the need to have them signed off by boards or board committees.

We anticipate that more regulators will follow what the antitrust authorities have started – a refusal to see subsidiaries as separate entities and instead, to view groups of companies as a single entity for the purposes of regulatory sanctions. This has a two-fold effect: it facilitates the extra-territorial reach of regulation (for example, the FCPA or UK Bribery Act) and it increases the resources to be considered in setting a fine or penalty.

As fines begin to be calculated as percentages of group global turnover, it will become more vital then ever to ensure that your carefully crafted polices do more than sit on your computer screens. Compliance teams will need to adopt a risk-based approach that is regularly updated to reflect evolving concerns and to prioritise resources in order to strike the right balance. Programmes will have to adapt to the varying degrees of risk across different jurisdictions, as well as take into account the local enforcement realities. Where in the group's business and activities is it more likely that a particular risk will crystallise? What extra steps need to be taken to implement relevant policies in those countries? Answering these questions must not be a one-off process. Demonstrating a clear desire for continuous improvement, and a sensible process to achieve it, is a major part of any mitigation argument – and can have a big effect on the level of any sanction – when problems occur. We are assisting a number of companies benchmark their programmes both with peers and across industry sectors to continually evolve best practice.



Social media and the 24/7 news society: the ultimate tool for activists

Executives and decision-makers trying to steer their organisation through the risk and reputation minefield should not just focus primarily on current law and regulation. They need to be mindful of incoming rules, the trends in how regulators are interpreting and enforcing guidance, and of public sentiment. Running through much of this is the question of "what are society's expectations for your organisation?".

As well as change pursued by regulators, whether for political ends or otherwise, we expect to see society's expectations of how corporates should behave become more pronounced. Social media channels and the 24/7 news society mean that public perception of the behaviour to be expected from multinationals will become an increasing focus for companies. Social media tools available to all, undoubtedly make individual campaigns more effective, and potentially give them disproportionate importance. The speed of broadcast news and the democracy of social media are being exploited by a broadening range of stakeholders.

On the one hand, this poses new legal issues for corporates. One of the striking findings of our new social media handbook (available here) is that social media (i) results in much more activity becoming actionable and (ii) leaves assets, (eg contact lists), that previously could be protected at law, unprotectable once moved into a social media environment.

On the other hand, social media poses wider practical and commercial issues. There are growing numbers of activist shareholders with the ability and inclination to mobilise other investor groups to push for changes in corporate strategy. These investors don't need to play by the same rules as more traditional institutions, and are often adept at using law and the media to exert pressure – our Activism Rising survey has highlighted some of these trends already.

Separately, we expect that the activities of civil society groups, campaigners, and non-governmental organisations (NGOs) will continue to expand beyond their traditional energy/environmental base to address broader social matters and corporate behaviour – the recent attention on the UK tax affairs of certain multinationals is a perfect example of this.

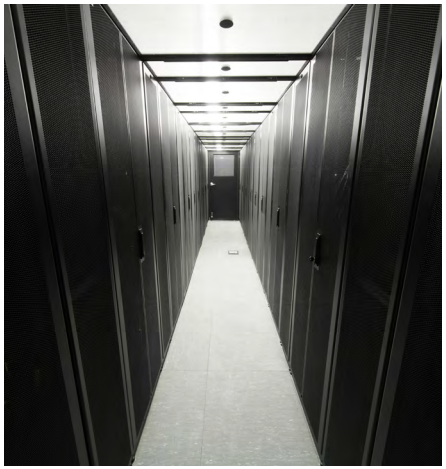
Sustainability will remain a focus for NGOs, but human trafficking and labour rights abuses within corporate supply chains will start to gain traction. There will be increased pressure on large corporates to use their influence to ensure good corporate behaviour in their supply chain organisations and for the highest risk issues to enforce compliance in a similar way to that adopted in the field of employee safety or corruption risk.

Given the new role of and access to social media, concerns arising thousands of miles away can land on the front doorstep in a matter of minutes.

> "Social media tools available to all undoubtedly make individual campaigns more effective, and potentially give them disproportionate importance."

Notable changes in 2014: antitrust, data protection and cyber security

As well as these broader trends and themes, companies will need to be aware of changes in certain key areas of regulation – competition and anti-bribery / corruption and data protection.



Competition authorities have upped the ante. Although cartels have sometimes been difficult to define, they have generally been recognisable: an understanding between competitors with the object of restricting competition: the so called "smoke filled room".

In recent investigations, however, it is clear that the European Commission, US authorities and other authorities, are taking a bolder approach and testing the limits of antitrust law with aggressive enforcement in the "grey zone" – namely where information has been shared, sometimes unilaterally and with a clear commercial rather than anti-competitive rationale.

This moves the goalposts in terms of antitrust risk, with very real implications for corporations and their employees. Certain sectors are particularly affected, including those in the financial and extractive sectors supplying, as they often need to do, data to third party organisations that set indices for price discovery, trading or other processes, or informing investors and others in relation to market trends, etc.

As international cooperation between antitrust authorities continues to expand, cartel enforcement is also spreading across the globe. Emerging regimes are now also testing new antitrust theories, picking up on precedents drawn from elsewhere and using extra-territorial enforcement to make their own mark.

In the field of data protection, many companies will need to consider the general attitude of regulators to the collection and use of personal data. Data is clearly a valuable resource, indeed an entire industry has grown up around the analysis and exploitation of it. On the one hand, this information can be used to offer a consumer something tailored to their individual needs and budget. On the other hand, might the information some businesses hold make it so difficult for new players to enter that market that it erects barriers to new entry, prejudices consumer access to products, and reinforces dominant market positions? Opinion is divided on the extent to which the collection and use of personal data may impact competition. Would it be enough to give the competition authorities grounds for refusing merger clearance for example, or opening an abuse of dominance investigation? It is, as yet, unclear but it would be wise for companies to think about how they use and store the data they hold and continue to collect.

More specifically, a new Data Protection legal regime is expected to be debated at length over the next 12 months at EU level and finalised towards the end of the year. It will deliver the biggest shake-up in privacy for 20 years. Its impact on business will be immense and so too will be the potential fines – between 2% and 5% of the annual global turnover of a group is being mooted, making it akin to the competition regime. It will require companies' not only to comply but be seen to comply. New mandatory concepts, such as "accountability", "privacy by design" and mandatory privacy officers will result in regulators introducing much more into the back office of companies privacy compliance. Companies will need to start considering recruitment and will also need to ensure appropriate systems and controls are in place to avoid them being exposed to these potentially enormous fines.

Related to the protection of data, but a much wider issue, we anticipate cyber security finally becoming more of a priority for companies. As the US and EU continue to encourage, and potentially compel, companies to disclose security breaches, we expect the scale of the problems to become more apparent, both to boards and to regulators, and the focus on cyber security to increase accordingly. Again, legislators are responding; in the EU a draft network infrastructure security directive is under consideration.

"Get out of jail free": the importance of governance and compliance systems

Most regulators genuinely want to change corporate behaviour, and legally they are required to behave proportionately and to have regard to the compliance measures companies have taken.

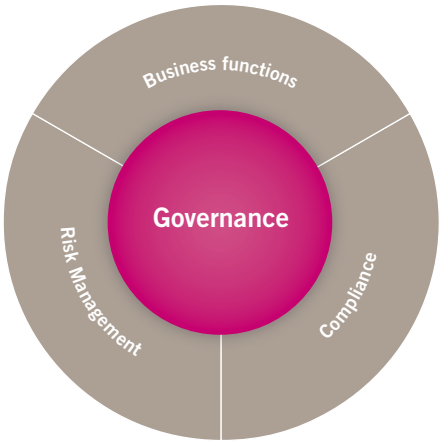
If your organisation can show that it has a considered and well-implemented governance and compliance structure that failed on a particular occasion, then the regulators are much more likely to show leniency. If governance and compliance is a paper exercise only, is out of date or is poorly implemented or under resourced, your risk of prosecution will be significantly greater. We have seen an increasing number of examples of this coming out of enforcements in the US and elsewhere.

Given the direction in which the level of fines (and cost of investigations) is heading, having a "fit for purpose" governance and compliance model that helps to create transparency, accountability and that is adaptable over time, is an essential risk management tool that organisations should embrace.

"If governance and compliance is a paper exercise only, is out of date or is poorly implemented or under resourced, your risk of prosecution will be significantly greater."

Secondly, despite the rhetoric arising from the financial crisis, we do not anticipate that personal, civil or criminal risk liability for directors or senior managers will increase. Therefore, this should remain a relatively low risk unless there is serious personal wrongdoing or neglect, and should give some comfort to boards. However, the position may be less benign in some developing economies and in the US where "big game hunting" is likely to continue with the targeting of high profile individuals.

Good governance organises, integrates and embeds the disparate, sometimes conflicting, activities, values, and goals of an organisation into its core business



Staying ahead

The challenge for in-house counsel and decision-makers is to get ahead of these regulatory trends and requirements without stifling the business. What actions you need to take will depend upon your starting point, sector and the countries in which you operate but we set out below some steps all companies should consider taking:

1. Ensure compliance programmes are far more than just paper policies and processes.

There needs to be a risk-based approach. Are your policies tailored to the challenges your country teams currently face? Have you allocated the right resources to them depending on where the risks lie? Who is in charge of implementing and monitoring them? Build into your compliance programmes periodic reviews and evaluations. Demonstrating a clear interest to achieve continuous improvement and a sensible process to do this is a big part of any mitigation argument (and likely sanction level) when problems occur.

2. Ensure commercial teams investing in emerging economies do their due diligence.

Innovative solutions to lack of "traditional" diligence materials will be needed. A "desk top" analysis of the risks, potential contractual and diligence solutions, and remaining gaps can be performed so that decision makers can properly weigh up the risks against opportunities. Post acquisition, it may be sensible to undertake more detailed checks. Sorting out latent problems immediately on acquisition is easier and likely to involve lesser penalties than at a later date.

3. Be aware of enforcement trends and the push into new areas.

Particularly around reporting to price setting agencies, price and investment "signalling" and the scope for enforcing "indirect" cartels (eg via joint ventures, common suppliers and agents). Diligence concerning how business practices are evolving in response to periods of industry downturn and tough trading conditions. Be sensitive to the ways the same business practices may be considered across jurisdictions (eg Resale Price Maintenance). Do not underestimate the time it takes to change deeply entrenched commercial habits.

4. Current data protection regimes have already required much attention.

Especially in light of increasing enforcement, and fines, over the years, if the upcoming draft Regulation from Europe is adopted, it will revolutionise the way personal data is processed, with an impact expected beyond European borders. Compliance with this may be a challenge, especially in "data rich" sectors, and should be considered from the outset when designing business models.

5. On cyber security, treat the risk of theft of proprietary confidential data in the same way as you analyse and manage other business risks.

Analyse what information is the most important to your organisation, what can be done to protect it, and plan for what happens if there is a cyber breach. Remember cyber attackers often get in via companies and service providers further down your supply chain. Demand to know from them what protections they have in place, assess these as against your own requirements and ensure you diligence these risks appropriately.

6. Companies likely to be the subject of NGO interest need some friends.

Consider engaging with specific organisations and developing a broad range of allies well ahead of any issues arising. Legislators and regulators can be influenced by NGO activity, particularly where this generates sustained media interest. In the current climate, once parliamentarians have had issues brought publicly to their attention, the ability to make counter arguments effectively can be significantly reduced. (Witness the increased attention of the Russian authorities on licensing arrangements in the wake of the Western media scrutiny into the tax affairs of certain multinationals.)

Contacts

We hope that the issues outlined in this paper will be a catalyst for discussion and change in organisations keen to adapt. We look forward to keeping you up to date as to both changes in law and regulator behaviour as these unfold.

Please feel free to ask us questions or share your comments or feedback by contacting one of our Operational Intelligence Group members listed, or by e-mailing us at OIG@linklaters.com.

Further resources

To see our other insight pieces and publications and for information about forthcoming events, please click **here**.

Operational Intelligence Group members

Satindar Dogra
Co-head of the Operational Intelligence Group
Tel: (+44) 207 456 4316
satindar.dogra@linklaters.com

Clara Ingen-Housz
Partner
Tel: (+852) 2901 5306
clara.ingen-housz@linklaters.com

Vanessa Havard-Williams
Co-head of the Operational Intelligence Group
Tel: (+44) 207 456 4280
vanessa.havard-williams@linklaters.com

Lance Croffoot-Suede
Partner
Tel: (+121) 2903 9261
lance.croffoot-suede@linklaters.com

Tom Shropshire
Co-head of the Operational Intelligence Group
Tel: (+44) 207 456 3223
tom.shropshire@linklaters.com

Tanguy Van Overstraeten
Partner
Tel: (+322) 501 9405
tanguy.van-overstraeten@linklaters.com