PUBLICATION PENDING
This invited RAND white paper was presented at a RAND Symposium entitled Transforming Compliance on May 28, 2014, and will be published in September 2014 as a part of the final symposium report. It may be circulated prior to such publication if accompanied by this disclaimer prominently displayed on the header of every page. Past RAND Symposia Reports in this series may be viewed at http://www.rand.org/jie/centers/corporate-ethics/pubs.html

THE PRIVATIZATION OF COMPLIANCE

Scott Killingsworth, Partner
Bryan Cave LLP

"As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs."

U.S. Sentencing Commission[1]

Introduction

Achieving consistent legal compliance in today's regulatory environment is a challenge severe enough to keep compliance officers awake at night and one at which even well-managed companies regularly fail. But besides coping with governmental oversight and legal enforcement, companies now face a growing array of both substantive and process-oriented compliance obligations imposed by trading partners and other private organizations, sometimes but not always instigated by the government. Embodied in contract clauses and codes of conduct for business partners, these obligations often go beyond mere compliance with law and address the methods by which compliance is assured. They create new compliance obligations and enforcement mechanisms and touch upon the structure, design, priorities, functions and administration of corporate ethics and compliance programs. And these obligations are contagious: increasingly accountable not only for their own compliance but also that of their supply chains, companies must seek corresponding contractual assurances upstream. Compliance is becoming privatized, and privatization is going viral.

A Qualitative Shift

There has been an element of privatization in the compliance arena at least since the Federal Sentencing Guidelines for Organizations[2] were established. After all, the point of the Sentencing Guidelines is to leverage the government's limited regulatory and enforcement resources by offering a strong incentive for companies to take on more of the state's prevention, detection and enforcement burden. Corporate compliance programs augment state oversight by performing tasks that governments lack the resources or the line-of-sight to do efficiently.

But that state-incentivized privatization model still reflects the traditional vertical, two-party relationship between government and the governed. The new wave of privatization is horizontal, networked, and qualitatively different. The Sentencing Guidelines model simply mitigates the risk of compliance failure. It does not expose companies to new forms of risk, liabilities or forfeitures or to the possibility of multiple conflicting standards, but private-to-private (P2P) compliance may do so. Program elements and ethical policies become contractual obligations,

[1] U.S. Sentencing Commission, Guidelines Manual, §8B2 (November, 2013), commentary quoted is at p. 499 and was added effective November 2004 by Amendment 673. Available online at http://www.ussc.gov/guidelines-manual/2013/2013-8b21 (visited May, 2014).
[2] http://www.ussc.gov/sites/default/files/pdf/about/overview/Overview_Federal_Sentencing_Guidelines.pdf.

vulnerable to such contractual remedies as indemnities, damages, audits, default declarations, loan acceleration and termination. P2P compliance is reshaping the compliance task portfolio and raising new questions about who is answerable to whom, both internally and across company boundaries.

Private compliance pressures may originate from any point in the value chain: suppliers, customers, capital markets, insurers. Compliance officers may find themselves caught in the middle between demanding customers and reluctant suppliers, or, in the other direction, between manufacturers vitally interested in how their products reach market and resellers seeking the shortest route to revenue.[3] They may be simultaneously pitted against their own colleagues in charge of operations, procurement, business acquisition and contracting. And unlike the Sentencing Guidelines and most other government leniency programs, many of the privatized compliance requirements are truly mandatory – at least if you want to do business with the other party.

A Positive Direction

From Apple[4] to Zoetis,[5] major corporations are requiring their business associates to commit to third-party codes of conduct (P2P Codes) and related contract clauses. This trend signals a growing appreciation that enterprises across the value chain share one another's reputational and compliance risks, and that compliance processes play an important role in translating legal commands into lawful conduct. It reflects an awareness that if you are dependent on a business partner to keep you out of legal trouble, it might pay to take an interest in how they intend to accomplish that.

By recasting compliance and ethics from a vertical, state-imposed constraint on business to an integral, horizontal expectation of how business is done, P2P compliance encourages the adoption of best practices both as a cultural norm and, critically, as a path to profit. Coming now from external business partners rather than just the internal ethics and compliance staff, this message has the potential to re-orient some attitudes and remove some ethical blinders. As more businesses are forced by their counterparties to examine their compliance processes and routinely accept business and legal consequences for them, we can expect increases in overall investment in compliance, in the scope and robustness of the average compliance program, and in ambient awareness of compliance issues outside the compliance, audit, and legal staffs. The viral nature of the process, in which each participant can exert pressure on a large number of direct and indirect upstream or downstream parties, while simultaneously fielding demands from other members of its value chain, suggests that the trend will continue and its influence will grow.

---

[3] For example, customers may exert pressures regarding the sourcing of raw materials from regions that are known for forced labor or are involved in conflict, or regarding the social or environmental impacts of extractive activities; while manufacturers and value-added sellers may have a strong interest in pushing anti-corruption compliance through their sales and distribution channel.

[4] The Apple Supplier Code of Conduct is available at https://www.apple.com/supplier-responsibility/pdf/Apple_Supplier_Code_of_Conduct.pdf.

[5] The Zoetis Supplier Conduct Principles and an accompanying Position Statement are available at http://www.zoetis.com/supplier-information.

Historically, most P2P Codes have covered key integrity risks and issues of corporate social responsibility at the level of policy rather than of procedure – and at this level they have reflected broad consensus on compliance best practices and accepted principles of corporate responsibility. They have been easy to accept without fear of adverse side effects, and most still are. But the newer trends of adding process or "how-to" components, of more granular and prescriptive drafting, and of embedding P2P Codes more firmly in a contractual mesh, raises a note of caution. We can hope that as P2P assurances become more routine, a consensus will emerge around generally accepted practices for demanding and enforcing assurances from one's counterparty and its value chain. Today, however, P2P compliance is in its awkward, adolescent phase. Before turning to some of the challenges, let's review how we got here and where we are.

Origins and Protagonists

We can trace the origins of this trend to three main protagonists: governments, both in their sovereign roles and as customers; the human rights/corporate social responsibility movement; and companies themselves.

Government Instigation in the Enforcement and Procurement Spheres. Blockbuster fines, civil penalties and disgorgements, monitorships and burdensome settlement agreements are attention-getters. They provide not only object lessons about compliance risk – and lately, third-party risk especially – but also a "bully pulpit" from which officials can provide specific guidance to an increasingly attentive audience about compliance program features that will affect enforcement decisions. For example, FCPA deferred/non-prosecution agreements[6] today send a message by routinely requiring settling defendants to institute appropriate compliance process controls over business associates,[7] such as advance due diligence and ongoing oversight, "flowing down"[8] codes of conduct, imposing training requirements, and securing contractual commitments covering recordkeeping, audit rights, vendor compliance undertakings, and associated termination rights – all principles that are echoed in more conventional DOJ guidance[9] and in official guidance on the U.K. Bribery Act[10] as well. Similarly, in 2013 the Office of the Comptroller of the Currency offered risk management guidelines to financial institutions for critical services contracts, including requirements for due diligence evaluations of suppliers'

[6] *See*, e.g., Ralph Lauren Non-Prosecution Agreement, April 22, 2013, Attachment B, pp. B-2 through B-7, available at http://www.justice.gov/criminal/fraud/fcpa/cases/ralph-lauren/Ralph-Lauren.-NPA-Executed.pdf.
[7] The required third-party controls apply, "where necessary and appropriate," to a very broad class: "outside parties acting on behalf of the Company in a foreign jurisdiction, including but not limited to, agents and intermediaries, consultants, representatives, distributors, teaming partners, contractors and suppliers, consortia, and joint venture partners."
[8] To "flow down" a contractual or code requirement is to impose it upon third parties representing successive links in a contracting chain, such as subcontractors and suppliers, or distributors and sales agents. Ordinarily this is done by requiring each link to incorporate an identical or equivalent clause in its contract with the next link, sometimes *ad infinitum*.
[9] *See*, e.g., A Resource Guide to the U.S. Foreign Corrupt Practices Act, issued November 20, 2012, available at www.justice.gov/criminal/fraud/fcpa, and DOJ Opinions 08-02, June 2008 and10-02, July 2010, available at www.justice.gov/criminal/fraud/fcpa/opinion.
[10] Ministry of Justice, The Bribery Act 2010 Guidance, available at http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

legal and regulatory compliance programs, audit rights over their risk management and internal controls, and ongoing monitoring and remediation activities.[11] This kind of "advice" is ignored at one's peril.

The government's role as a customer may be even more influential, at least in the US. All holders of large federal contracts are now required to institute compliance programs that track the Sentencing Guidelines' (otherwise voluntary) criteria, and are specifically required to contractually flow down these obligations to large subcontractors.[12] This general procurement rule is supplemented by a growing number of topic-specific supply-chain diligence provisions in areas as diverse as human trafficking and information security for controlled technical information. [13]

The Human Rights and Corporate Social Responsibility Movement. The role of the human rights and corporate social responsibility movement, including advocacy groups and multinational NGOs, is quite distinct from that of the state, both in origins and in aims. Focused on global human rights, environmental and social issues, and corruption, and on the ambivalent economic interactions between developed and undeveloped nations, NGOs such as the International Labor Organization, the OECD, the World Bank, the United Nations and the International Chamber of Commerce (ICC) have campaigned for global acceptance and implementation of ethical business standards – in some cases implementing them with integrity standards for their own suppliers.[14] In parallel, advocacy groups such as Friends of the Earth and the Rainforest Action Network have pursued issue-oriented campaigns to change business practices through the court of public opinion, often targeting specific entities or industries.[15] These NGO campaigns and the principles they stand for claim legitimacy from world community consensus rather than from national legislation; and they seek implementation of this collective conscience in the business world via the exertion of influence by one private organization upon another.

An illustrative product of this type of effort is the Equator Principles,[16] a voluntary private compact among 78 major financial institutions that sets environmental and social impact standards for the activities of commercial banks in global project finance. Under these principles, the banks must require project-finance borrowers to implement an "environmental, social, health and safety management system…including policies, management programs and plans, procedures, requirements, performance indicators, responsibilities, training and periodic audits and inspections with respect to Environmental or Social Matters" – essentially, a full-blown

[11] Office of the Comptroller of the Currency, OCC Bulletin 2013-29, Risk Management Guidance for Third-Party Relationships.
[12] See Federal Acquisition Regulation (FAR) §52.203-13. A "large" contract or subcontract is one with a value of at least $5 million and a performance period of at least 120 days, to be performed at least partly within the United States.
[13] *See* (as to human trafficking) Executive Order13627, "Strengthening Protections Against Trafficking in Persons in Federal Contracts" and FAR §22.1703 *et seq*., FAR § 52.212-5, and (as to supply chain information security) FAR Subpart 239.703 and §252.239-7017 *et seq*.
[14] *See* UN Supplier Code of Conduct, September 2013, available at http://www.un.org/depts/ptd/pdf/conduct_english.pdf.
[15] *See* O'Sullivan, *infra* note 16, pp 108-112.
[16] Niamh A. O'Sullivan, Social Accountability and the Finance Sector: The Case of Equator Principles (EP) Institutionalisation (doctoral dissertation 2010), available at dare.uva.nl/document/185897.

environmental and social compliance program – backed up by independent consultants who report to the banks. The associated loan agreements include covenants, representations, warranties, and events of default keyed to the program's goals.

The Equator Principles took a number of years to become fully institutionalized and to gain a critical mass of adherents. By contrast, within three months after the recent Rana Plaza factory collapse, major customers of the Bangladesh garment industry established both the Accord on Fire and Building Safety in Bangladesh[17] and the competing Alliance for Bangladesh Worker Safety.[18] Both initiatives mandate independent inspections, remediation, training, worker reporting mechanisms, and required cooperation from the suppliers. Multinationals have gotten the supply-chain compliance message and have learned to respond decisively to failures.

Corporate Developments. Apart from reacting to the direct external pressures just outlined, companies have been forced to come to grips internally with the reputational, legal, and financial risk implications of the global trend towards disaggregation of the enterprise and the consequent atomization of the supply chain across national boundaries. Improved enterprise risk and compliance management has focused attention on the exponential increase in third-party exposure that companies incurred by outsourcing of all but their "core" functions. Headlines provide daily reminders that outsourcing a critical, compliance-sensitive function does not outsource the associated reputational, legal or financial risk. Companies have responded by re-investing in managing and monitoring business partners' compliance just as they do product quality.[19] As with quality, the management tools employed include direct monitoring and auditing, explicit contractual allocation of compliance responsibilities and risks, and requiring the business associate to institute and flow down specified compliance policies, procedures and processes.

This trend is not just about the product supply chain; it is proliferating in other business relationships as well. An important recent development is the emergence of compliance risk management as a prerequisite for conventional access to capital. Promising to obey the law is no longer enough; today, corporate credit agreements and securities underwriting agreements commonly include additional representations and covenants that the borrower/issuer has "implemented and maintains policies and procedures designed to ensure, and which are reasonably expected to continue to ensure, compliance" with specified laws including the FCPA and other anticorruption legislation, Office of Foreign Assets Control sanctions, anti-money laundering legislation, the USA PATRIOT Act, securities disclosure requirements and insider trading prohibitions for public companies, and industry-specific regulations such as HIPAA and information security requirements. Credit rating agencies have revealed that they are examining

[17] http://bangladeshaccord.org/wp-content/uploads/2013/10/the_accord.pdf.
[18] http://www.bangladeshworkersafety.org/about.
[19] One effect of more engaged management of outsourced functions is that it requires surrendering some of the cost savings that fueled the outsourcing epidemic in the first place. This swing of the pendulum is part of a larger reconsideration of the balance between risks and rewards of outsourcing at a more granular level than in the past. For example, a similar adjustment seems to have occurred in a related quarter as "companies have reversed a trend toward reducing the number of suppliers in order to cut costs and have added them to reduce risk" of supply-chain disruption. *See* Jaeger, "Are Firms Lacking in Supply Chain Management?", Compliance Week, November 2013, page 43.

compliance markers for red flags as part of their ratings process,[20] and at least one insurer requires those seeking FCPA investigation-cost insurance to have their compliance programs benchmarked by a third party.[21]

The potential impact of this recent market focus on effective corporate compliance systems reaches well beyond access to capital. In late 2012 a major proxy advisory firm announced that it will recommend voting against retention of directors, in uncontested elections, where there has been a material compliance failure.[22] By May 2014 it had done so.[23]

The Anti-Corruption Archetype

Needless to say, these themes of governmental enforcement and procurement mandates, corporate social responsibility, and risk management across the global supply chain all converge upon the problem of official corruption, and anyone curious about the future of privatized compliance should consider the current state of anti-corruption compliance. Enforcement of anti-corruption laws has reached new heights and, encouraged by the OECD anti-bribery convention,[24] national anticorruption laws continue to proliferate. Several prominent NGOs including the World Economic Forum,[25] Transparency International,[26] the ICC,[27] the World Bank,[28] and the OECD itself[29] have published detailed guidance on third-party compliance management, guidance that universally includes due diligence, flow-down of anti-corruption policies, training and communication, documentation of business associates' compliance efforts, and imposition of audit rights, ongoing monitoring, and contract remedies such as termination.[30] The debates about best practices are settled, save for skirmishes over when they can be practically applied.

---

[20] *See* Standard & Poor's Ratings Direct Methodology: Management and Governance Credit Factors for Corporate Entities and Insurers, November 13, 2012, Table 2 and items 47, 61 and 62.
[21] Author background interview with a Senior Vice President of a major insurance broker.
[22] *See* ISS U.S. Corporate Governance Policy 2013 Updates, November 16, 2012, citing the 2010 BP Deepwater Horizon spill and News Corporation UK's 2011 integrity scandal as material failures of board risk oversight.
[23] *See* Paul Ziobro and Joann Lublin, "Ouster of Target Directors is Urged," Wall Street Journal, May 29, 2014, p. B2. ISS recommended "no" votes on seven incumbent directors of Target Corporation, claiming that inadequacies in risk oversight had set the stage for the 2013 data breach.
[24] OECD, Convention on Combating Bribery of Public Officials in International Business Transactions, available at http://www.oecd.org/daf/anti-bribery/oecdantibriberyconvention.htm.
[25] World Economic Forum, Partnering against Corruption – Principles for Countering Bribery, 2009.
[26] Transparency International, Business Principles for Countering Bribery, 2013.
[27] International Chamber of Commerce, ICC Rules on Combating Corruption, 2011.
[28] World Bank Integrity Compliance Guidelines, 2010. The principal function of these guidelines is to establish preconditions for ending a noncompliant supplier's debarment from participating in World Bank-financed projects.
[29] OECD Guidelines for Multinational Enterprises, 2011, available at http://www.oecd.org/daf/inv/mne/oecdguidelinesformultinationalenterprises.htm.
[30] The ICC even offers a booklet of suggested contract clauses, ICC Anti-corruption Clause, ICC Publication No. 740E, 2012.

These recommendations have been implemented by a growing number of companies, albeit on a risk-prioritized basis.[31] Third-party due diligence is commonplace and anti-bribery provisions appear frequently in international contracts and universally in P2P Codes, quite often with domino-style flow-down requirements. With this pattern firmly established, code and contract language that was originally drafted only for the anti-corruption context is now being extended to cover other high-priority compliance domains such as export sanctions, money laundering, data privacy and conflict minerals. With this growing adaptation of accepted anti-corruption methodology to other risks,[32] "FCPA" could stand for Future Compliance Paradigm Adopted.

Codes, Contracts, and Consequences

As mentioned, third-party compliance obligations are increasingly imposed contractually – either within a commercial contract, through a separate P2P Code, or, commonly, together by incorporation of the P2P Code into the contract. As an alternative, business associates are sometimes asked to ensure compliance with the other party's internal code of conduct, which may include provisions specific to third parties.[33] Even where there is no formal contract, a company may impose due diligence, P2P Codes, monitoring and auditing as a precondition for beginning or continuing a business relationship.

P2P Codes commonly contain several distinct types of provisions: broad human rights, labor and corporate social responsibility standards; ethical rules governing relationship issues such as conflicts of interest and gifts and entertainment; requirements to obey specific laws of concern and laws generally; and procedural rules such as the right to audit the partner's records or train its personnel. Process and structural rules may be imposed on the partner's compliance activities, such as requirements to establish management accountability, develop appropriate policies and procedures, maintain an anonymous reporting system and an anti-retaliation policy, train employees, conduct periodic audits, risk assessments and remediation, and of course, sometimes to cascade these program elements to downstream associates.[34]

---

[31] See Dow Jones Anti-Corruption Survey Results 2014 showing *inter alia* that 82% of survey respondents maintained anticorruption programs, 77% perform due diligence on new partners, 53% rank partners by risk and 35% train their business partners.

[32] *See*, e.g., OCC Bulletin 2013-29, *supra* note 11, which addresses not only a variety of compliance risks but also strategic, operational, reputational and credit risk.

[33] *See* Ronald Berenbeim, "Finding a Delicate Balance: Third-Party Ethics Program Requirements," a Conference Board-Ethics and Compliance Officers' Association Survey (PowerPoint presentation available at http://www.13iacc.org/files/Third_Party_Ethics.pptx), October 31, 2008, finding that at that time 69% of respondents' internal codes purported to apply to third parties, while 25% of respondents had a separate P2P Code. One impetus for adopting P2P Codes is that stretching an internal employee code to cover a wide variety of third-party business partners and relationships can present thorny questions of interpretation and application.

[34] Notably, all of these compliance-program elements are required or recommended in two leading industry model P2P Codes and accompanying guidance: See Electronic Industry Citizenship Coalition® Code of Conduct, available at http://www.eicc.info/documents/EICCCodeofConductEnglish.pdf, and the Pharmaceutical Industry Principles for Responsible Supply Chain Management and its Implementation Guidance, available respectively at www.pharmaceuticalsupplychain.org/downloads/psci_principles.pdf and www.pharmaceuticalsupplychain.org/downloads/psci_guidance.pdf.

Many P2P Codes also include provisions of a more traditionally "contractual" nature, such as terms governing intellectual property, use of assets, subcontracting, information security, business continuity, media relations, and statements imposing strict and apparently unlimited liability for subcontractor compliance. Meanwhile, the related business contract will likely contain its own representations, warranties and covenants imposing compliance obligations, often of a detailed and context-sensitive kind.

Needless to say, neither P2P Codes nor contractual compliance terms are uniform across contracting parties, and even a single party's P2P Code and its contractual compliance provisions are often written by different people in different departments, with little or no coordination. Some codes suffer from multiple authorship by specialists with different agendas, adding both length and a fluctuating level of detail.[35] All this heterogeneity, combined with the wandering boundary between code and contract, can lead to mischief.

The foremost problem is that of remedies: a P2P Code may be expressly incorporated into a contract or may refer to one, with either a clear statement or a fuzzy implication that all contractual remedies apply. When made contractual, even an existing obligation to comply with a law automatically acquires a "private right of action" for damages or other contract remedies, whether the law's regulatory architecture includes one or not. Duties once owed only to specific parties such as employees or consumers are now enforceable by business partners. Likewise, matters of corporate social responsibility or sustainability, once voluntary and ethical, become mandatory and legal. And the standard remedies provided by contract law may be supplemented by custom remedies such as self-help, clawbacks, liquidated damages, suspensions, or debarment.

Given the usual inclusion of precatory, aspirational, and social-responsibility provisions in P2P Codes as well as the common use of debatable terms like "fair," "responsible," "ethical," and "human rights," application of many contractual remedies may simply be inappropriate. It may be reasonable to assume liability for damages, and even to indemnify your business associate, if you get them into regulatory trouble while performing a critical outsourced function – but does it make sense to risk a forfeiture of amounts due, a clawback of amounts paid, or a termination without right to cure if a labor-rights violation is discovered in an unrelated part of your business, or elsewhere in your supply or distribution chain?

The point is that if we are going to turn a compliance code into a contract, we need to consider all the same questions of reasonableness, proportionality and draftsmanship that we ask with any other contract obligations, and in some cases we will need different answers. Experience suggests that this type of legal analysis is the exception rather than the rule. To the contrary, there is anecdotal evidence that, having discovered that P2P Codes are seldom reviewed for contractual liability, some procurement or legal staffs have moved one-sided contract terms into their codes, where the omission of customary contractual exceptions and protections is less likely to trigger negotiation. At a minimum, P2P Codes regularly fail to consider predictable, legitimate

[35] The inconsistent tone, level of detail, and peripatetic coverage of some codes seems proof of a maxim usually attributed to H. G. Wells: "No passion in the world is equal to the passion to alter someone else's draft."

interests of the other party that would ordinarily be accommodated in a negotiated contract.[36] This combination of creeping contractualism and careless or predatory drafting leads in the wrong direction as compliance risk, immune to the laws of physics, expands via contracting.

The problem of impractical or unfair P2P compliance obligations is only made worse by the fact that vastly unequal bargaining power can pop up at any point in the value chain. Imagine the plight of a specialty distributor caught between the P2P Codes of a major manufacturer and a retailer dominant in the key market segment, each expecting their code provisions to be flowed through to the other. Even powerful market participants may trigger unexpected risks if they use their bargaining leverage too bluntly. If your P2P compliance demands are nonnegotiable and everyone accepts them because they must, how can you distinguish between those who sincerely intend to comply and those who are actually most cynical and least likely to comply? Negotiation, at least, shows that your counterparty takes the matter seriously. And if you have audit or training rights but do not exercise them, or if you do not insist on receiving the required reports or evaluate them when received, do you think you have effectively transferred the risk? Will a prosecutor equate your contractual risk-transfer provisions with a sincere effort to ensure compliance?

The Compliance Officer's Dilemma

If P2P compliance is in its awkward adolescence, so are the processes by which many companies confront it. Not surprisingly, many incoming P2P Codes and compliance provisions are never seen outside the procurement, sales or business development offices where they first land, and as a result companies take on unanticipated, un-bargained-for obligations. As the volume, sophistication, and associated risks of P2P compliance requests continue to grow, they will demand an organized response, led and coordinated by the compliance team.

An appropriate response to the P2P challenge must cope with a number of mismatches evident from the earlier discussion:

- the mismatch between the compliance team's core role of providing objective, independent oversight of compliance risks, and the need to participate actively in the business function of negotiating vital commercial transactions that directly impact the compliance mission;

[36] A few examples of issues raised by partisan or careless drafting will suffice. Audit provisions in P2P Codes are often unrestricted in scope and lack protections for such concerns as confidentiality, waiver of attorney-client privilege, or competition-law exposure. Sweeping code provisions for surprise inspections and private employee interviews, designed for use in connection with human rights and labor issues in developing countries, take on a different flavor in the complex legal framework of the developed world. Zero-tolerance prohibitions on investment in suppliers by public officials or their families are not unheard of, and some P2P Codes require notification if *any* of the business partner's employees or their relatives have any financial interest in the code's sponsor – all this in this age of public companies, mutual funds and 401Ks. There is irony in receiving by ordinary e-mail a proposed P2P Code that requires encryption of all information sent over the Internet. And some companies seem to feel that investment bankers and lawyers should not be allowed to work more than 48 hours a week. Breach of any of these unrealistic requirements could be used as grounds for a pretextual contract termination, or withholding of payment.

- the mismatch between the scope of a given P2P Code (including, for example, issues of sustainability, corporate social responsibility, business continuity, information security, etc.) and the core mandate and competencies of the compliance team;
- the mismatch between the goals, priorities, and timelines of the compliance function and those of the sales, business development, and procurement functions where incoming P2P demands are triggered and received;
- the possible mismatch between the compliance activities and priorities demanded by third parties and those of the company;
- mismatches between P2P compliance demands, such as audit rights, and business objectives such as protecting one's competitively sensitive information or the trade secrets or personal information of third parties;
- and not least, the mismatch between the existing budget and resources of the compliance function and the burgeoning and always-urgent workload all this implies.

P2P compliance demands accentuate the inherent tension between compliance priorities and short-term operational goals, simply because they occur at such critical points in the operational cycle: the initiation of procurement, sales, or financing relationships. On the incoming side, P2P demands could present the compliance officer with a Hobson's choice of either disapproving a transaction or agreeing to unreasonable compliance terms. There is a strong element of irony in the prospect that a compliance officer might be forced to veto incoming compliance demands because they are impossible to achieve, unreasonably costly, or allocate risk unfairly: no one wants to be ridiculed as the compliance officer who "killed the deal because it required us to be *too compliant*." At a minimum, if the compliance officer does not have the final word on acceptance of P2P compliance terms, there should be a serious conversation about who owns the incremental risk of a compliance regime accepted on grounds of business necessity.

Managing P2P compliance responsibly and with consistency requires a protocol for handling both incoming demands and the company's requests of third parties (including those originated both by the company and as flow-downs). This should include cataloging standard acceptable and unacceptable provisions as well as triggers for escalated review (such as indemnity clauses); triage for the referral of issues to subject-matter-experts outside the compliance function, such as sustainability, business continuity, and information technology; identification of the stakes, including applicable contractual remedies, in each case; evaluation of alternative responses such as negotiation of terms, proposing tailored remedies rather than negotiating the substantive obligations, seeking approval of one's own code as a substitute, etc.; assignment of each of these tasks to identified personnel; and a decision-making framework for "business necessity" exceptions.

Critical to all of this is clarity – in advance – as to the authority and reporting lines of the compliance officers involved. A robust protocol, developed and implemented with senior executive input and board support, can do much to create this clarity, and to reinforce the compliance officer's objectivity and independence in carrying out the mandated role.

A reasoned, organized and disciplined approach to the accelerating P2P compliance trend can impose a certain amount of order on our unruly adolescent. But the single most effective approach to a complex problem is to simplify the problem. P2P compliance needs to grow up.

Childhood's End: Towards a Mature P2P Compliance Regime

The corporate community has a collective stake in simplifying management of the P2P compliance process while retaining its best features and fostering widespread acceptance of compliance cooperation and accountability throughout the value chain. Every company bears unnecessary costs stemming from the heterogeneity of P2P demands, the vanishing distinction between code and contract, the unprincipled attempts at risk transfer, and the administrative and operational burdens of sorting through, negotiating, and keeping track of all the commitments and seeing to their implementation.[37] Any company, at any given time, can find itself subjected to unreasonable demands from a trading partner possessed of superior bargaining power and a self-serving agenda. Any company may experience competing demands from opposite ends of its value chain, and every company will find it impossible to flow down everyone else's standards *ad infinitum*, in both directions. We need to develop a consensus on generally accepted principles of P2P compliance.

The companies least vulnerable to unfair pressures, and most able to inflict them, are our largest and most powerful enterprises. They should accept a leadership role in the effort to rationalize P2P compliance standards, and many of them have done so, singly as well as in groups such as the Electronic Industry Citizenship Coalition, the Pharmaceutical Supply Chain Initiative,[38] and the Automotive Industry Action Group.[39] They recognize that increasing contractual demands produce diminishing practical returns and that, in the end, reputational risk cannot be delegated. And some, to their credit, simply take to heart their own Code of Conduct admonitions to treat suppliers and customers with fairness.

The goal of this effort should be to establish common expectations that are proportional, balanced, and sensitive to the particular risk profile of a given relationship. As one example of an avenue worth exploring, it would be useful to draw a principled distinction between what is the appropriate content of a P2P Code, what should instead be considered for inclusion in a commercial contract, and what kinds of remedies are appropriate for each. To minimize negotiation and complexity, P2P Codes should be principle-based, and should address issues that are subject to wide consensus and that apply to all business activities. Matters that are essentially ethical in nature should appear in codes, as should all aspirational encouragement of goals where success cannot be assured or a deadline assigned, and for initiatives with no well-defined end-point and no extrinsic mandate. For many P2P Code violations, especially those directed at compliance processes rather than outcomes, remedies should be focused on moving the other party towards compliance, correction of past non-compliance, or termination of the relationship.

---

[37] To be fair, not every company bears these costs. Some bear the alternate and deferred cost of ignoring the issues, agreeing to whatever comes over the transom, and dealing with the consequences later.

[38] *See* note 34 *supra*.

[39] *See* Ben DiPietro, "Automakers Face 'Herculean' Task in Implementing Supply Chain Guidelines," Wall Street Journal Risk & Compliance Journal, May 28, 2014, available at http://blogs.wsj.com/riskandcompliance/2014/05/28/automakers-face-herculean-task-in-implementing-supply-chain-guidelines/ (registration required); and the Automotive Industry Guiding Principles to Enhance Sustainability Performance in the Supply Chain , available at http://www.aiag.org/staticcontent/files/CorporateResponsibilityGuidanceStatements.pdf

By contrast to P2P Codes, contracts focus on very particular business goals; they are risk-based and highly sensitive to the details of the business context. They map a path to the defined goals and seek to further each party's legitimate interests under the factual variations most likely to arise. Hence compliance provisions that relate specifically to the particular parties, to their specific goals, to the relevant market, and to the risks inherent in each, should go into the contract where they can be negotiated in the light of those specific goals and risks, and appropriately targeted remedies can be assigned.

Collective action has been, and will continue to be, an important element in convening a consensus on P2P Code and contract content, but the foundation of true consensus will be the discrete but parallel decisions made by countless individual participants in light of their broader, long-term interests. These interests must be judged in the light of the company's dual role as both recipient and originator of compliance demands. Rather than having one code it imposes to protect itself and another set of principles that it is willing to be held accountable for, companies should develop a single, consistent portfolio of Golden Rule third-party commitments that it will accept as both obligor and beneficiary.[40] An essential companion effort, of course, is ensuring that one's compliance and ethics program and corporate social responsibility functions are up to the task of fulfilling these commitments. In the end, the goal is alignment among legal mandates, compliance program elements, and P2P commitments in both directions.

There will always be zero-sum business partners whose prime goal is risk transfer and who will do everything within their power to achieve it through contracts and P2P Codes. The tendency of standard-form documents to always grow, never shrink, and tilt ever more to one side is also well-known, and is trenchantly illustrated by the contractual creep of some companies' P2P codes. But the opposite can occur, and the proof is the dramatic evolution of internal corporate codes of conduct over the past several years. Fueled by a consensus about driving key values home, sticking to the main points, and leaving the details to other documents that can be consulted and applied when needed, corporate codes have become shorter, clearer, less adversarial and more digestible and memorable. With the right consensus within the business community, we can achieve the same new paradigm with P2P Codes. Let's get started.

[40] One of the most common responses to P2P Codes today is to trot out one's own code, indicating that it is substantially equivalent to the other party's proposed code, and offering to be bound by its conditions – and a few existing P2P codes expressly provide that the counterparty's code may be acceptable, especially for use in imposing flow-down requirements, if it is substantially equivalent to the first party's. When feasible, this process greatly simplifies administration; and converging standards of P2P Code content will facilitate its use.