Published on *The National Law Review* https://natlawreview.com

What Every Multinational Company Should Know About . . . Implementing an International Compliance Program (Part II)

Article By:

Gregory Husisian

John E. Turlais

Jenlain A. C. Scott

In our prior update (published November 29), we provided the first five steps in our twelve-step program for international compliance. These steps are intended to help companies identify international regulatory risk inherent in their international operations. By carefully working through these twelve steps, most multinational organizations should be able to implement the kinds of compliance that U.S. regulators would consider compliance best practices, including in the newly emphasized area of supply chain due diligence and compliance.

Step 6: Create a Written Compliance Policy

It is unfortunate that Step 6 — the drafting of the compliance manual — is often Step 1 for many companies. As shown in our prior update, however, there is considerable groundwork to cover before an organization should begin the actual drafting of the compliance manual.

Although the contents of the compliance program should be tailored to the organization, the written program for most companies will include:

- ***A Written Policy Statement.*** A policy statement, such as a "Code of Ethics and Business Conduct," succinctly sets out the company's commitment to comply with the law. The organization should draft the policy statement in clear, straightforward language. The statement should clearly impose responsibility on each employee to abide by the company's compliance policies.
- ***A Written Compliance Program.*** One of the most important elements of a good compliance program is a well-constructed written manual and policies. The written manual and policies should accurately summarize the regulations, using plain language that employees without legal training can readily understand and follow.
- ***Supplemental Materials.*** Depending on the risk-informed view of the area, it may be appropriate to distribute supplemental compliance materials to individuals either at high risk of potential violations or who need specialized training to oversee or comply with the relevant

legal regime. All major international compliance areas (anticorruption, export controls, economic sanctions, international antitrust, anti-money laundering, and antiboycott) may warrant this treatment, depending on the nature of the company's business and risk profile. Items to include are in-depth lists of red flags that are pertinent to the company, lists of sample contractual language to use when hiring third-party intermediaries, detailed summaries of the relevant legal requirements, frequently asked questions, descriptions of compliance missteps that have occurred at the organization (including how they were handled), and resources for handling compliance issues. These supplemental compliance resources may be distributed as appropriate and need not be distributed to the entire organization.

- ***Internal Controls.*** Any internal controls that are implemented to help serve compliance goals should also be memorialized. This topic is covered in Step 7.

Compliance policies should be written in plain language, provided in the native language of those responsible for implementing and complying, and tailored to the company's risk profile. A company should not expect its workforce to fully understand every nuance of the law, like a law professor, and the compliance policies should not strive for this level of detail. Rather, the materials should distill the relevant information and serve as a tool to arm people with enough knowledge to recognize a potential problem and understand how and when to notify the appropriate compliance personnel. In some circumstances it may be appropriate to publish basic guidance broadly and to provide supplemental guidance to persons most likely to need more detailed compliance information on a need-to-know basis.

Step 7: Establish Internal Controls

Internal controls are one of the three pillars of compliance (along with written policies and training). Internal controls are one of the main mechanisms by which compliance policies are implemented and thus merit as much attention as the written compliance policies themselves.

The purpose of internal controls (sometimes called "standard operating procedures") is to provide procedures that implement the compliance program, create consistent and repeatable methods of implementing compliance dictates, and to build a self-reinforcing cycle of compliance improvement. Compliance policies set the standard, while internal controls implement and reinforce those standards.

When designing internal controls, it often is possible to harness existing processes. By way of example, to add controls in the anticorruption realm, multinational companies may take existing internal controls, such as those governing disbursements and reimbursements and accurate recordkeeping, and integrate them with procedures intended to track potential payments to foreign officials and personnel who work at state-owned companies. Similarly, some companies use customer-intake and credit-check procedures as mechanisms to screen new customers against lists of blocked persons (like those published by OFAC, the EU, and the UN). Grafting onto existing company procedures minimizes the time necessary to implement a functioning set of internal controls and the effort needed to oversee their operation. Plus, modifications to existing procedures are more easily adopted than adding entirely new processes in a large organization.

Some specific internal controls that multinational companies should consider relate to the following high-risk international areas:

- ***FCPA.*** Using existing disbursement and reimbursement policies to ensure notification to

compliance personnel of potentially troublesome payments; creating special trigger mechanisms for entertaining foreign officials (including people who work for state-owned entities); and implementing controls regarding gifts, meals, entertainment, and travel expenses that exceed pre-defined limits.

- ***Export Controls and Sanctions.*** Creating internal controls to ensure routine scanning of Specially-Designated Nationals (SDNs and Denied Persons) for all new customers, and the entire customer list and transaction parties on a pre-determined basis; establishing internal controls regarding placing appropriate export control notices on outbound electronic paperwork and shipping documents; developing controls to ensure accurate reporting of information for the Automated Export System and communication of that information to any customs broker or freight forwarder involved in the business; implementing controls to automatically flag transactions involving controlled items or defense articles; and mandating controls designed to restrict access of non-U.S. nationals to controlled technical data, wherever it may be found at the company.
- ***Antiboycott.*** Designing controls to ensure that relevant front-line personnel, whether involved in the contracting, procurement, accounting, or credit functions, or other functions that are likely to encounter boycott-related activity, monitor and report boycott-related requests; and implementing controls designed to ensure all contracts have superseding language stating the company's policy of rejecting any requests to participate in the Arab League boycott of Israel.
- ***Customs.*** Designing controls intended to ensure accurate classification of goods, the performance of post-entry accuracy checks, and customs audits; designing controls regarding how to interact with Customs brokers and provide information required to timely clear imports at Customs.
- ***Supply Chain.*** Implementing procedures for maintaining an up-to-date mapping of the supply chain and the conduct of risk-based due diligence.

Step 8: Training, Training, Training

Comments to the U.S. Sentencing Commission's Sentencing Guidelines provide the "organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the [relevant] individuals . . . by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities."[1]

The basic task of training is to ensure, in conjunction with a well-written compliance program and appropriate internal controls, that employees and agents have sufficient knowledge to recognize red flags and other problematic situations and understand what they need to do to comply. The goal is not to create legal experts across the company; rather, it is to sensitize people to the legal requirements, so they know when to seek counsel from the appropriate compliance or legal personnel.

Training should occur for all new employees and annually for appropriate longtime employees, at least for high-risk regulations. Because no firm's workforce is static, the program should include automatic steps to ensure compliance materials are distributed to personnel at the time of hire or when personnel are transferred or promoted into positions that require training. The same is true whenever the company is making acquisitions, setting up new agent relationships, or establishing joint ventures.

Multinational companies should also consider how they can use technology to enhance their

compliance programs, including using intranets and establishing a “compliance corner” on company internal sites. Best uses of intranets for compliance include: posting basic training online; publishing the company’s compliance program and internal controls; providing plain-language summaries of applicable laws; providing real-world examples and frequently asked questions; consolidating and presenting model contract provisions; quickly disseminating updates to the compliance program and internal controls; establishing links to allow quick and simple reporting of potential problems; and informing employees how the company has resolved tricky issues it has encountered in the past. The company can use its intranet as a mechanism to identify problems quickly, to report potential issues, and to coordinate the company’s compliance initiatives. Using these tools can make compliance an ongoing process and give new employees meaningful access to company procedures at the outset of their employment.

Step 9: Integrate Outsiders

Outsiders — third parties who act (or could be construed as acting) for the organization — are often a key source of risk. Controlling the risk of a regulatory misstep requires close attention to the incremental risk added by third parties, including business partners, joint ventures, agents, sub-agents, consultants, and other third parties. Given the U.S. government’s expectations for supplier due diligence and compliance, the focus should be on the international supply chain as well.

Depending on the risk profile of the company, it may make sense to integrate outsiders into the risk management plan. This type of integration requires several common-sense solutions, including explicitly incorporating outsiders into the compliance program when possible, providing outsiders with training materials, conducting training for them, and exercising auditing rights on a risk-adjusted basis.

These procedures are especially important with respect to economic sanctions and export controls. The power of regulators is broad. Generally, U.S. jurisdiction follows the goods, services, or technologies, including through third parties, where the U.S. person “knew or should have known” that diversion was possible. Proving absence of knowledge is a difficult exercise. The importance of “knowing your customer” is not extinguished just because a third party is involved in the chain of commerce. If the U.S. government takes the view that the third party was brought into a transaction for the purpose of hiding aspects of the business, then the risk profile of a transaction involving an affiliated third party can be even higher than for a direct transaction.

Step 10: Auditing and Checkups

Sustaining a strong compliance program means the processes are regularly tested and updated. Multinational companies should use risk-based auditing principles to determine areas that should be monitored through audits and compliance checkups.

Additionally, multiple U.S. government agencies recommend supply chain audits. Many organizations neglect this risk point in favor of checks on the company’s own affiliates and joint ventures. Now that the U.S. government is focused on supply chain compliance, expressly recommending supply chain audits, and issuing penalties for supply chain failures, prudent companies that operate or source from abroad consider conducting such audits on a risk-based basis. Audits are especially valuable when key components are sourced from areas of the world known to implicate regulatory concerns.

A recent trend for accomplishing the goal of constant compliance self-improvement is for companies to benchmark their compliance policies against those of other companies in their industry.

Benchmarking helps ensure companies keep up with evolving compliance standards and industry best practices. Companies also need to check the implementation of the program by ensuring that personnel know of the policies and are following the requirements. Special attention should be directed to any changes in the organization that occurred since implementation of the policy, including modifications to laws or changes in the company and its scope of operations. Examples include the establishment of new subsidiaries or the hiring of new agents, distributors, suppliers, and so forth. Companies should carefully review any risk assessment previously performed to determine whether the compliance measures in operation are, in fact, addressing previously identified risks.

Step 11: Monitor Red Flags

The identification of red flags and appropriate follow-up are the keystones to well-functioning compliance. Thus, one of the most important tasks when implementing international compliance is to train relevant stakeholders about the transactions and conduct that are suspicious given the regulatory landscape.

The type of red flags to identify depend on the company's business and risk profile. These considerations include, for example, whether it uses controlled technology or sells/exports controlled goods, whether it interacts with international regulators, the industry, methods of operation, and other unique factors. An organization should tailor known red flags to monitor to its specific risk profile and then distribute a list to company personnel. (Note: An upcoming post will address common red flags.)

In recent years, companies wishing to collect red flags have established whistleblower hotlines and other simple reporting mechanisms. The goal for these tools is to empower one of the company's greatest compliance resources — the collective intelligence of its own work force — to help the company identify and address suspicious circumstances early and before they grow into large problems. A hotline, well-publicized in the United States and abroad, is a valuable compliance resource. But take note, companies that operate in the European Union will need to use care in establishing a hotline, and particularly how information is gathered from the hotline, to comply with local data privacy and work force rules.

Once a credible allegation is received, compliance personnel should: (1) report the concern to appropriate members of management; (2) evaluate the claim's merit, and develop a plan to further investigate or resolve it; (3) gather any information necessary to fully evaluate the claim; (4) log the investigatory steps taken; and (5) report the information up the compliance chain. The company should affirmatively preserve relevant evidence related to the threat. The compliance personnel should record the results of every inquiry, to allow the company to track reported concerns to see if they exhibit a pattern. They should also be encouraged to recommend improvements to the compliance processes from lessons learned from compliance issues as they arise.

Step 12: Communicate with Board & Senior Management

Board-level and senior-management involvement in compliance should be regular and institutionalized. The key areas for high-level involvement include thorough oversight of compliance initiatives, quarterly reports of compliance activities, and special communications for potentially serious matters.

Board members and senior management should receive regular reports detailing the number and type of reports of potentially serious compliance violations, interpretations of the meaning of this data, and recommendations regarding how the company should update compliance procedures to address

areas of concern, as well as potential changes to the organization's risk profile. The report should include the results of any investigations of serious possible violations and the results of any compliance audits. The report also might benchmark compliance efforts against those of competitors and other industry participants.

A final consideration is communications with shareholders, especially if a publicly traded company is involved. The board, or the compliance or audit committee, needs to determine when a potential compliance situation requires disclosure as a material fact. This can involve any situation where the potential costs of investigation are high (and therefore material for reporting), where the conduct could jeopardize important rights due to the conduct (such as the right to export), where the problem appears to be systemic, where senior management is involved, or where there is the potential for a serious penalty. Another consideration is whether the conduct might require disclosure for another reason, such as the need to disclose transactions involving the government of Iran under SEC disclosure requirements related to such conduct.

* * *

As shown, compliance at multinational companies is particularly complicated and covers multiple high-risk legal regimes. Nonetheless, a thoughtful and systematic approach to compliance, starting with a full risk assessment, can give guideposts to the creation and implementation of an effective compliance program that can minimize the chances of costly compliance missteps that can lead to costly penalties and reputational harm. Further, in the event of an enforcement action, a company that can show that the violation occurred despite a thoughtful and well-implemented plan likely will fare better than one that was negligent across the board. In other words, a regulator might be more inclined to grant mitigating credit if the company can show that the violation was truly a one-off because the company has taken great care in designing and implementing its compliance program.

---

[1] U.S. Sentencing Guidelines Manual § 8B2.1(b)(4). The individuals in subdivision B are "members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees and, as appropriate, the organization's agents." U.S. Sentencing Guidelines Manual § 8B2(1)(b)(4)(B).

National Law Review, Volume XIII, Number 347