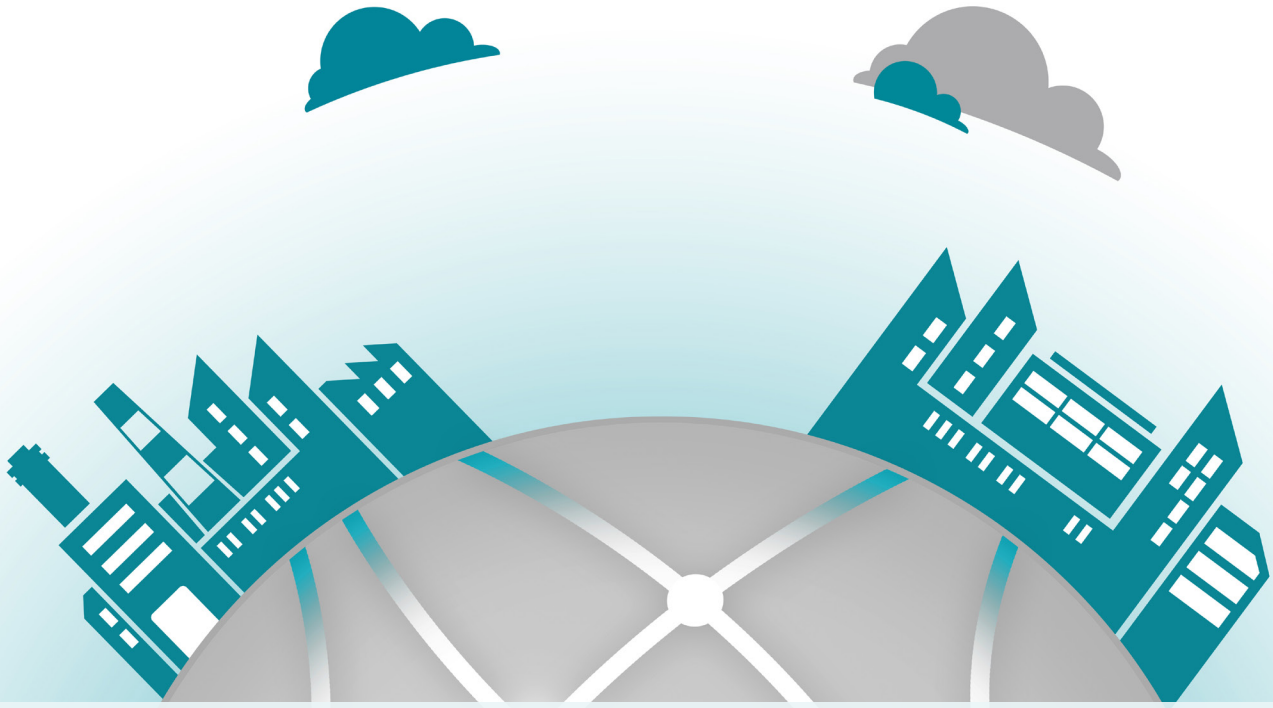

The Twelve Compliance Steps Every Multinational Corporation Should Undertake in Light of Recent Trump Administration Enforcement Activity

Prepared by:
Gregory Husisian
Foley & Lardner LLP

LORMAN®
Published on www.lorman.com - September 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

The Twelve Compliance Steps Every Multinational Corporation Should Undertake in Light of Recent Trump Administration Enforcement Activity

Written by Gregory Husisian – 5/14/18

Over the last month, regulators with the Trump administration sent a loud message to companies subject to U.S. jurisdiction: Enforcement of laws governing international activities is alive and well and the laws will continue to be enforced with vigor. Companies that are subject to U.S. jurisdiction – whether because they are located within the United States or otherwise subject to U.S. jurisdiction (such as through the use of U.S.-origin goods or the use of the U.S. financial system) – need to evaluate whether their compliance measures are sufficient to detect and halt potential violations of U.S. international regulations, including the Foreign Corrupt Practices Act (FCPA), U.S. export control regulations (the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), the economic sanctions regulations maintained by the Office of Foreign Assets Control (OFAC), and the various anti-money laundering laws.

As recent enforcement activity under the Trump administration illustrates, enforcement of this suite of international regulatory laws is alive and well. In light of these developments, this Client Alert summarizes the most recent enforcement activity, as well as the steps that companies subject to U.S. jurisdiction can take to identify and mitigate the risk of costly enforcement actions under these regulatory regimes.

Recent Enforcement Activity Shows U.S. Government Willingness to Impose Record Penalties for Violations of International Regulations

Under the Obama administration, enforcement of the FCPA, export controls, economic sanctions, AML, and FCPA regulations was steady and strong. Although the numbers varied year by year – mostly due to timing issues related to when large matters were settled – it was not uncommon to see large enforcement settlement that surpassed the $100 million level.

Any thought that the Trump administration might take a more lenient approach toward these international regulations has been laid to rest by the strong record of enforcement under the current administration, as underscored by two recent enforcement actions.

First, Panasonic agreed to pay $280 million to resolve FCPA offenses for payments to consultants of its U.S. inflight entertainment unit in the Middle East and Asia, including the payment of $143 million in disgorgement to the Securities and Exchange Commission. In both cases, the resolutions were related to activities of Panasonic's U.S.-based subsidiary, Panasonic Avionics Corporation. According to the U.S. government, senior management of Panasonic Avionics established a

bribery scheme to pay a Middle Eastern government official more than $900,000 for a "purported consulting position, which required little to no work," allowing Panasonic Avionics to help gain over $700 million in business from a state-owned airline. The U.S. government further stated that Panasonic Avionics concealed the payment "through a third-party vendor that provided unrelated services" to Panasonic Avionics and then allegedly falsely recorded these (and other) payments in its books and records. Other payments related to Asian sales.

The Department of Justice (DOJ) gave Panasonic Avionics a 20 percent discount off the low end of the U.S. Sentencing Guidelines fine range because of the cooperation of the company and what the DOJ characterized as strong remediation efforts, including the severing of several senior executives who were either involved in or aware of the misconduct by Panasonic Avionics or Panasonic. Nonetheless, because the remediation efforts only recently had been instated, the deferred prosecution agreement provides for a two-year independent monitor, followed by an additional year of self-reporting.

Independently, the Department of Commerce's Bureau of Industry and Security (BIS) took the unusual step of suspending an export control settlement deal with Chinese telecom equipment maker ZTE Corporation, while at the same time revoking the export privileges of the company. ZTE Corporation was operating under a settlement of claims that it had violated U.S. export control and economic sanctions regulations by engaging in 251 transactions with persons in Iran or with the Iranian government. These transactions had last year resulted in the largest-ever export controls penalty – nearly $1.2 billion, with $300 million of it being suspended during a seven-year probationary period. As a result of the export ban, the ability of ZTE to export any goods or technical data from its 14 offices and six research centers in the United States will be virtually eliminated until March 13, 2025, thereby endangering the ability of ZTE to take a leading role in the rollout of next-generation 5G wireless technology.

These settlement actions illustrate the ability of U.S. regulators to discover and punish violations of U.S. international regulations, as well as the willingness of the Trump administration to impose groundbreaking penalties. In light of the aggressive enforcement mentality of the U.S. government, this Client Alert presents a series of steps that companies subject to U.S. jurisdiction can take to help identify and manage their international regulatory risk. Careful consideration of each step will take the company from identifying the risks, through examining any deficiencies in dealing with those risks, to the goal of compliance as informed by appropriate procedures, internal controls, and training. For any company that has not gone through such an exercise in the last few years, systematically working through the 12 steps is likely to lead to a significant payoff for ameliorating the organization's risk profile through an effective compliance system.

A Twelve-Step Program for International Compliance

As illustrated by the record export controls penalty against ZTE (almost $1.2 billion, followed by a denial of export privileges) and the Panasonic FCPA settlements, the risk of severe enforcement actions under the Trump administration for violations of international regulations continues to be high. Yet many multinational companies find themselves in a quandary regarding how best to implement their international regulatory risk management. They may well know they face heightened risk but are not clear regarding the best way to proceed. This section of the Client Alert summarizes the typical steps that most multinational companies should consider when evaluating their international regulatory risk management procedures and internal controls. Through careful implementation of these measures, most multinational organizations should be able to implement the kinds of compliance that U.S. regulators would consider to be industry best practices.

Step 1: Secure Buy-In at the Top

Many companies looking to implement an international regulatory compliance program start by drafting a written compliance policy. But long before it comes time to draft the policy, a well-thought-out compliance strategy will look to put in place the underpinnings of the compliance program. Chief among these is the need for consistent management support for compliance initiatives.

Although the phrase "tone at the top" encapsulates management support, the concept requires more than just support from the CEO and other top management officials. When properly executed, the idea of tone at the top is a pyramid, with the concept of "doing the right thing" and respect for compliance flowing down from the CEO to personnel at all levels. Senior management ensures it is known that compliance has full support at the top, and that compliance has the resources to function properly, while also trying to ensure that respect for compliance with legal and company mandates flows through the company.

Management support is especially important for companies with international operations. The connection between the sales and operational activities of international subsidiaries, on the one hand, and regulatory risk management and adhering to the requirements of U.S. law, on the other, can appear tenuous when viewed by far-flung actors. The reality, however, is these far-off operations often represent the highest regulatory risk. This may mean that the organization must pay special attention to these foreign subsidiaries so it can reinforce the compliance message and its importance to the overall organization.

In establishing the tone at the top, senior management must understand the importance of a consistent and reinforced message. Too often, the role of senior management seems confined to issuing "the compliance letter" (*i.e.*, a letter from the CEO stating that compliance is important). Thereafter, the topic is put on the

back burner and left to the legal or compliance department to implement, often with inadequate resources to back up the compliance mission.

While there is nothing wrong with issuing such a letter, the compliance message should be reinforced so it becomes part of the internal DNA of the corporation. The importance of compliance to the company cannot be communicated by a one-time effort; rather, it should be a part of the day-to-day management of the organization.

With that goal in mind, senior management should take advantage of "non-training" training opportunities, such as integrating mentions of compliance missteps or accomplishments into quarterly calls, including compliance topics in sales meetings, and mentioning the topic frequently in company newsletters. Further, when teachable moments occur, such as compliance missteps by competitors, it is a good idea to bring this to the attention of relevant personnel, such as through a mass email from a senior manager or the general counsel's office.

Senior management must set a strong example. It should be common knowledge that compliance rules apply across the entire organization, including for senior personnel; that the company promptly follows up on credible red flags; and that the company is willing to walk away from business that requires stepping too close to the risk threshold. People throughout the organization, whether in the United States or elsewhere, should realize there are consequences for compliance missteps. Through these means, senior management can communicate its respect for compliance throughout the organization.

Step 2: Perform a Risk Assessment

The second step for most organizations is to perform a risk assessment. A risk assessment is a survey of the company's operations to determine the exposure of the organization to various forms of regulatory risk, considering both the likelihood and the severity of possible violations and the current enforcement priorities of the relevant authority.

The importance of the risk assessment lies in the recognition that it is not possible to eliminate all regulatory risk. Since organizations need to minimize the risk of violations, while coping with the reality that they have limited resources to put into risk mitigation, they need guidelines for allocating their scarce compliance resources. The risk assessment provides this guidance by assembling data needed to create an organization-wide risk profile.

Compliance at international organizations should be tailored to the organization, taking into account all factors that bear on the risk profile of the organization. Items to consider include U.S. government enforcement priorities, prior compliance issues within the organization, risks and trends in the industry (including whether the U.S. government seems to be targeting the industry for a

given legal regime), and recent changes in the scope of operations of the organization. Such changes are frequent sources of weakness if they are not mirrored by changes in compliance oversight.

A typical way for companies to proceed with a risk assessment is to survey business units that represent areas of high regulatory risk. Questions for an anti-corruption survey, for example, might examine whether the relevant stakeholders often deal with state-owned enterprises, whether they have frequent interactions with government regulators, whether there is significant entertaining of non-U.S. persons, whether the organization does significant business in countries known to have a reputation for corruption, and whether the company does significant business in the United Kingdom (which can draw the UK Bribery Act into play). For export controls, the relevant topics to explore would include whether the organization deals with controlled items or controlled technologies; whether the company deals with items on the U.S. Munitions List (USML) or modifies commercial items for military use or to meet military specifications; whether the company has recently conducted a classification review; the degree to which non-U.S. nationals potentially have access to controlled technical data; whether the organization sells products that rely on encryption; and whether there are sales to known diversion points (the Middle East, Mexico, Russia, Pakistan, and so forth). For economic sanctions, relevant topics to cover would include whether there are sales by non-U.S. subsidiaries to sanctioned countries or specially designated nationals, whether there are sales to known diversion points, and whether the organization as a whole maintains adequate screening for SDNs (Specially Designated Nationals, or persons who have been sanctioned under U.S. law as being off-limits for business transactions and financial dealings). Finally, an anti-boycott risk assessment would examine the extent of dealings with Middle Eastern countries and with firms operating out of that region.

One thing to remember is that the conduct of a risk assessment can lead to the discovery of potential regulatory violations. The company accordingly should have the risk assessment process conducted in a way that stresses confidentiality. If possible, it also is preferable that the risk assessment be overseen by an attorney. This is so the exercise can be conducted under the rubric of attorney-client privilege. Doing so could be important if the investigation uncovers evidence of apparent violations.

Once the risk assessment is complete, the results should be carefully evaluated to determine where the areas of greatest compliance concern lie. The results can be distilled down to a company-wide risk profile, which can guide the allocation of compliance resources. The results can then be used for such useful exercises as determining which areas merit the greatest attention, which areas likely need additional internal controls, whether there are patterns of deficient compliance (based on geography, product lines, subsidiaries/divisions, etc.), and whether the basic knowledge of the relevant legal requirements appears to be in place. By

formalizing the results in a risk profile, the corporation can determine the appropriate way to manage the identified risk.

Step 3: Survey Current Controls

Step 3 involves surveying current compliance procedures and internal controls. Most larger multinational corporations already have some kind of compliance procedures in place, whether in a formal compliance program or at least ethics provisions in the code of conduct. In determining how to proceed, these procedures are the best starting point. The company should assess the current compliance program to see if its compliance measures and internal controls line up with its risk profile.

The evaluation should consider whether the plan properly covers the following aspects of the company's risk model:

- Does the plan reflect all of the circumstances that may put the organization at risk of a violation? Is it based upon a realistic risk assessment that is up to date and consistent with the company's current circumstances?
- Does the program cover all aspects of the business that operate or sell overseas?
- Does the plan extend to any business units that might have dealings with non-U.S. officials, whether in a procurement, regulatory, or other role?
- Does the plan include model procedures and training for non-U.S. consultants and business partners with whom the organization does business?
- Does the compliance program reflect the nature of the firm's foreign business operations and the extent to which they are subject to government control or influence?
- Does the compliance program contain adequate procedures to ensure that the firm can monitor disbursements and reimbursements?
- Does the plan contain adequate internal controls to help buttress the compliance procedures?
- Does the plan compare well with codes of ethics and compliance policies used by comparable businesses in the industry and in the countries where the firm operates?

In making these determinations, the company should consider the company's general risk profile, not just those related to the specific legal regime. Problems in multiple areas may indicate a careless corporate culture toward compliance issues.

Another key issue that should be covered in the compliance survey is whether the program covers the identified outside actors who can expose the organization to the risk of a regulatory violation. The U.S. government considers all affiliates, joint ventures, agents, distributors, suppliers, subcontractors, and other third parties to be extensions of the organization.[1] The organization should evaluate whether the controls and compliance procedures extend appropriately to any person or entity with which it is affiliated and whether that entity may cause third-party liability.

Where anti-corruption is concerned, organizations operating abroad need to assess whether the current plan adequately covers the regulatory risk posed by resellers, vendors, consultants/agents, sales representatives, joint venture partners, freight companies, customs brokers, and any other third party that could be viewed as being a source of bribes while representing the interests or carrying on the business of the U.S.-based company. Where exports and sanctions are concerned, the organization must consider not only its own affiliates (joint ventures, agents, distributors, and so forth), but also the risk profile raised by its own customers who might be diversion risk points. Where anti-boycott is concerned, the organization should consider whether it has agents who might be viewed as providing information on behalf of the organization, and therefore might provide boycott-related information to countries cooperating with the Arab League boycott of Israel.

Step 4: Identify Available Resources

Compliance is an exercise in identifying and managing risk. Appropriate risk management requires matching compliance promises and expectations to the available resources, and vice versa.

After the compliance procedures have been identified and catalogued, a key next step is to ensure that the organization has not fallen into the classic compliance trap of over-promising and under-delivering. It is a classic mistake, from a risk-management standpoint, to impose compliance requirements and then fail to implement them. Yet this is often what many organizations do, either due to institutional drift or a lack of resources to implement the promised compliance tasks.

No compliance initiatives will work without adequate support. This issue is covered in the McNulty Memorandum. As the McNulty Memorandum states:

> Prosecutors should … attempt to determine whether a corporation's compliance program is merely a "paper program" or whether it was designed and implemented in an effective manner. In addition, prosecutors should determine whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts.

Once the company has identified the risk and necessary controls relating to those risks, it should develop a realistic sense of the cost of a program and the resources needed to run it. Senior management should sign off on the budgeting, with the understanding that the company will need to invest time and resources to maintain the program on an ongoing basis.

Without proper resources, a corporation risks certain failure. Compliance can be expensive, so a company should decide at the outset that it will budget adequate funds and employ sufficient resources to follow through on its compliance

initiatives. In determining whether sufficient resources are available, the company needs to consider that success in compliance efforts takes a commitment of both tangible company resources (hiring people and spending money on due diligence) and intangible ones (setting aside employee time for training). The resource identification should take a candid look at whether the company is adequately funding current compliance efforts. If the company has put in place a program that demands substantial due diligence of every foreign agent hired, for example, but has not adequately funded such activities, then the company should view this as a compliance failure. Viewed in an enforcement context, the corporation would look like it has failed to meet its own compliance standards.[2]

In the international realm, some of the most common areas where compliance resources tend to lag include:

- **Anti-corruption**. Promises of systematic due diligence for vetting agents, distributors, joint ventures, and other third-party entities; adequate oversight of the activities of third-party intermediaries; resources to conduct compliance audits; adequate training of overseas actors.
- **Economic Sanctions**. Resources for systematically checking the SDN and other blocked lists; allocating adequate resources for "know your customer" diligence; adequate training of overseas actors; failure to reflect new rules regarding what subsidiaries of U.S. companies can and cannot do.
- **Export Controls**. Inadequate classification of controlled items and technical data; failure to implement "know your customer" guidelines for end-use and end-user controls; failure to take into account potential diversion risks; failure to check the SDN and other blocked lists.
- **Anti-boycott**. Resources for reviewing contracts, purchase orders, letters of credit, certificates of origin, bills of lading, and other commercial documents.

To avoid these and other promise-resource mismatches, the organization should, with a clear and open mind, compare its identified risk profile with the inventory of current policies and internal controls, to determine whether there are any gaps between the two. Once such gaps are identified, the organization can, using normal risk-based principles, determine the best order and way to remedy the resource misallocation, whether by reallocating existing compliance resources, finding new sources of funding, or readjusting the compliance procedures.

Another key funding mistake in the international realm is failing to allocate sufficient resources to local compliance oversight. This topic is covered in Step 5.

Step 5: Assess Local Oversight

One of the key compliance considerations for organizations that operate in multiple countries is how the organization will oversee compliance outside the United States. The state of compliance, as envisioned at corporate headquarters, and the actual state of compliance, as implemented in the field, far too often diverge. This natural tendency is exacerbated when the organization operates in

numerous countries, which makes Step 5 a key stop on the path to effective international compliance.

It often is a mistake to assume compliance can be managed solely from a central location. While compliance initiatives can originate from a central legal or compliance department, and often are best managed in a centralized fashion, implementation and oversight often require on-the-ground attention. It accordingly is often necessary to set up a compliance infrastructure that includes compliance liaisons.

Establishing compliance liaisons has several advantages. First, managing full compliance centrally is difficult. There are just too many things to take care of (conducting training, monitoring red flags, conducting investigations, and so forth). Second, local personnel often have a better understanding of the regional or local environment and culture. Third, by being closer to operations, local personnel often are in a better position to identify and monitor red flags. Fourth, language issues often make local compliance issues a better direct interface for local employees. For all these reasons, it is a good idea to have compliance liaisons in place, at least where the organization is dealing with substantial, non-U.S. operations.

In assessing the adequacy of local oversight, it is necessary to consider areas of risk that may lie outside the organization. Relevant considerations include the state of oversight for non-entity risk points, including foreign subsidiaries, joint ventures, agents, distributors, consultants, and others. The review should be multifaceted and include a review of relevant contractual arrangements (to ensure the appropriate compliance-related provisions are in place), review of compliance certifications and updates to same, and consideration of any known red flags that have arisen regarding these third-entity risk points.

At most organizations, there are a variety of good options for compliance liaisons. Relevant local actors, who often are already in place and who can be harnessed for compliance oversight, include divisional or regional HR personnel, in-house attorneys, and auditors. If the compliance need is great enough, the organization can hire a new person dedicated solely to compliance. What is essential is that the compliance liaison be someone who is independent of business pressures. It should be someone who has the respect of local business people and who has the institutional authority and independence to follow up on potential compliance lapses, regardless of who is involved.

One item that should be assessed is the completeness of the local compliance oversight. The assessment should cover both the impact of U.S. and non-U.S. laws. However the oversight is locally managed, the organization should consider both the operation of extraterritorial U.S. laws and such local laws as local work rules, data protection and privacy laws (particularly in the European Union), competition laws, and laws regarding labor rights. The aim is to have local

oversight of all potential sources of significant regulatory risk, regardless of the governmental entity imposing the underlying legal obligations.

Step 6: Create a Written Compliance Policy
It is an unfortunate fact that Step 6 – the drafting of the compliance manual – is often Step 1 for many companies. As shown, however, there is considerable groundwork to cover before the organization should begin the actual drafting of the compliance manual. The goal is not just to have a written compliance policy; it is to have an effective policy that, through tailoring to the risk profile, operational needs, and culture, represents a workable compliance solution for the organization.

Although the actual contents of the compliance program should be tailored to the organization, usually the written program will include:

- **A Written Policy Statement**. A policy statement is just as the name implies. It succinctly sets out the company's commitment to comply with the law. The organization should draft the policy statement in clear, straightforward language, and should state that it is the responsibility of 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. The written manual should accurately summarize the regulations, using plain language that employees without legal training can readily follow. Many companies require that their employees sign certifications stating they have read the program and understand their compliance responsibilities, that they understand the law and the company's compliance procedures, and that they have communicated to the compliance department any information regarding any potential violations of the law or company policy. These certifications serve the purpose of reminding personnel about the legal standards and the company's compliance policies. They represent useful evidence of the importance of compliance in any enforcement action, and could become important if a disgruntled employee blows the whistle regarding information or actions he previously certified he did not know about.
- **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 of the major international compliance areas (anticorruption, export controls, economic sanctions, international antitrust, anti-money laundering, and even anti-boycott) may warrant this treatment, depending upon the company's risk profile. Items to include in such materials include in-depth lists of red flags (along the lines of those found in the Appendices to this International Compliance Guide), lists of sample contractual language to use when hiring third-party intermediaries, in-depth 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 other compliance-related materials. Such in-depth compliance resources should be distributed as needed, rather than to the organization as a whole.
- **Internal Controls**. Any internal controls that are implemented to help serve compliance goals should be memorialized. This topic is covered in Step 7.

Companies should give careful thought as well to the length of the written program. Some companies undermine the effectiveness of their program by establishing a drawn-out policy that covers every nuance in applying the law. This is a mistake, because employees will ignore a long and cumbersome compliance program. Instead of taking this approach, the program should focus on providing key points from the regulations, informed by useful examples relevant to the company and its industry. The goal is not to turn the workforce into law professors who fully understand every nuance of the law; rather, it is to give people enough knowledge so they can recognize a potential problem and notify the appropriate compliance personnel of the potential issue. If desired, supplemental guidance can be distributed to persons most likely to need more detailed compliance information on a need-to-know basis.

Step 7: Establish Internal Controls

Although internal controls are one of the three pillars of compliance (along with the written policy and training), they often are neglected. This neglect can be costly. Internal controls often are one of the main mechanisms by which the compliance policy is implemented. They accordingly merit as much attention as the written compliance policy.

The purpose of internal controls is both to provide procedures that implement the dictates of the compliance program and to create a self-reinforcing cycle of compliance improvement. Compliance policies set the standard, while internal controls implement and reinforce that standard. Through this mechanism, it is possible to enhance compliance in a positive fashion and to strengthen it over time.

In creating internal controls, it often is possible to harness existing processes. A good example of this lies in the anti-corruption realm. It is common for companies to take existing internal controls, such as those governing disbursements and reimbursements, and graft on 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 OFAC and EU lists of blocked persons. Doing so minimizes the time necessary to implement a functioning set of internal controls and the effort needed to oversee its operation.

Some specific internal controls that multinational corporations should consider involve 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 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 information regarding same to any Customs broker or freight forwarder involved; implementing controls to automatically flag any transactions involving controlled items or defense articles; mandating controls designed to restrict access of non-U.S. nationals to controlled technical data, wherever it may be found at the company.
- **Anti-boycott**. Designing controls to ensure that relevant front-line personnel, whether personnel involved in the contracting, procurement, accounting, or line of credit functions, or other functions that are likely to encounter boycott-related activity, monitor and report boycott-related requests; implementing controls designed to ensure that all contracts have superseding language stating the company's policy of rejecting any requests to participate in the Arab League boycott of Israel.

Step 8: Training, Training, Training

The importance of training as the foundation of compliance is widely acknowledged. Even the Sentencing Guidelines, which concisely focus on the basics of an effective compliance program, call out training for special attention. The Sentencing Guidelines commentary states that 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."[3]

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 all across the company; rather, it is to sensitize people to the law so they know when to seek counsel from the appropriate compliance or legal personnel.

The importance of conducting training appropriately is magnified in the international realm. Besides the normal problem of adequately communicating the compliance requirements, the training often will need to address local practices

and different cultural norms that may prove contrary to the compliance needs of the organization. Equally important is finding the best way to stress the importance of compliance with U.S. law, which may seem to many foreign nationals to be of limited concern because they are outside U.S. territory. Language difficulties, too, complicate things, making it essential to consider presenting compliance materials and training in languages other than English.

Training should occur for all new employees and annually for appropriate longtime employees.[4] Because no firm's work force 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 relevant positions that require training. The same is true whenever the company is making acquisitions, setting up new agent relationships, bringing on new distributors, or establishing joint ventures.

When preparing training materials, companies typically use a mix of written and training materials that summarize the law, frequently asked questions and answers about the law, training slides, and prepared oral presentations (which are best given in an interactive presentation with audience feedback and participation). The program should use real-world examples whenever possible, such as case studies drawn from actual problems confronted by the company in the past. The educational material should also reiterate the importance of compliance to the company's culture, and provide other useful information, such as recent enforcement actions against similarly situated companies.

Companies also should consider how they can use technology to enhance their compliance programs, including using intranets. Best uses of intranets for compliance include: posting basic training online; publishing the company's compliance program; 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; establishing links to allow ready reporting of potential problems; and informing employees regarding how the company has resolved tricky issues it has encountered. The company can use its intranet as a mechanism to identify problems quickly, to report potential issues, and to coordinate all of the company's compliance initiatives. Using these tools can make compliance an ongoing process and give new employees ready access to company procedures at the outset of their employment.

Another growing best practice is using automated training software. This software communicates compliance information and can be used to test the user's knowledge of both the substantive laws and the company's compliance procedures. Companies can place automated training software on the intranet and make completion of the training a required task for employees, allowing the company to develop a set of standards that employees must meet in a variety of substantive areas, such as export controls and sanctions compliance.

The company should maintain an attendance log to track all compliance training. Each employee should sign an acknowledgment form showing he or she has reviewed the compliance materials and understands his or her responsibility to comply with the company's program.

Step 9: Integrate Outsiders

As noted in the introduction to this International Compliance Guide, outsiders – third parties who act (or could be construed as acting) for the organization – are often a key source of risk. Once again, the First Law of International Compliance comes into play: The farther you get from your headquarters, the lower your degree of knowledge and control, and the greater the risk of a violation. This means that controlling the risk of a regulatory misstep requires paying close attention to the incremental risk added by third parties, including business partners, joint ventures, agents, sub-agents, consultants, and other third parties. Despite the operation of the First Law of International Compliance, the normal approach of most companies relies heavily – and often exclusively – on contractual protections for third-party protection. Such measures are essential. The U.S. government will consider any third-party arrangements that do not include such protections to be deficient. Yet by themselves, such contractual provisions generally offer limited protection that might be appropriate for low-risk actors, but not for other scenarios.

One example of this is in the FCPA realm. It has become common in recent years for third-party intermediary contracts to contain audit provisions, which allow the U.S. party the right to audit a third party, either as a general manner upon notice or based upon specific knowledge of a potential red flag. The U.S. government, however, has recently expressed skepticism regarding the value of such provisions if they are not regularly exercised. These types of contractual provisions lose their in terrorem impact once the third party discovers the provisions are seldom or never applied.

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 (where this is possible), providing them with training materials, conducting training for them, and exercising auditing rights on a risk-adjusted basis.

Such procedures are of use not only in the anti-corruption area, but also in the realms of economic sanctions and export controls. The rule is that U.S. jurisdiction follows the goods, services, or technologies, including through third parties, where the U.S. person "knew" that diversion was possible. Providing no such knowledge existed after the fact can be a difficult exercise. The importance of "knowing your customer" does not lose importance just because a third party is involved. If the U.S. government takes the view the third party was brought in to hide the nature

of the transaction, 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
It is difficult to have a strong compliance program unless it is regularly tested, probed, and analyzed. Stated differently, it is not enough to create a good compliance program and then let it run unattended, at least for high-risk areas. Companies should monitor compliance by direct observation, by supervising the program, and by testing the controls. One increasingly common way of ensuring the last element is to conduct regular compliance audits.

Checking on the operations of compliance programs and internal controls is increasingly common. Companies should use risk-based auditing principles to determine the countries, divisions, subsidiaries, and third parties that should be monitored through audits and compliance check-ups. Further, as noted in Step 9, companies also should consider extending such check-ups and audits to third parties as well.

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 to ensure they are keeping up with evolving compliance standards and industry best practices. A proper review, however, will go beyond ensuring the terms of the compliance program are state of the art. Companies also need to check the implementation of the program by making certain that people know of the policies and are following the requirements. Special emphasis, too, needs to be put on any changes in the organization that have 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, and so forth. It is also useful to consult any risk assessment previously performed to determine whether the compliance measures in operation are addressing these identified risks.

The audit and compliance checkup needs vary, depending upon the legal regime at issue. This topic is explored in the context of anti-corruption, export controls, economic sanctions, and anti-money laundering audits in the Annex to the Foley International Compliance Guide.

Step 11: Monitor Red Flags
The identification of red flags and appropriate follow up are the keystones to well-functioning compliance in all of the common international compliance areas. It is for this reason that one of the most important tasks when implementing international compliance is to train relevant stakeholders regarding the transactions and conduct that are suspicious given the regulatory requirements.

Identifying red flags is not a static process. The type of red flags to identify will depend on the company's profile, whether it uses controlled technology or sells/exports controlled goods, its interactions with international regulators, the industry in which it is engaged, its method of operation, and other, unique factors. As a starting point for identification, common red flags for FCPA, export controls, and economic sanctions appear as Appendices to this International Compliance Guide. It is a good idea for an organization to tailor such red flags to its own risk profile and then distribute them to company personnel.

In recent years it has become common to establish whistleblower hotlines and other reporting mechanisms. The goal is to empower one of the company's greatest compliance resources – the collective intelligence of its own work force – to help identify suspicious circumstances before they grow into all-encompassing problems. An easily available hotline, well-publicized and known both in the United States and abroad, is an important compliance resource.

It does little good to set up a helpline and then not to follow through on credible red flags raised. Once a credible report from the helpline is received, the compliance department should: (1) report the concern to relevant management actors; (2) evaluate the surface merit of the claim and develop a plan to deal with it; (3) follow up with an inquiry (if the report continues to seem credible); (4) log the investigatory steps taken; and (5) report the information up the compliance chain. The company should also give thought regarding steps to take to ensure the preservation of relevant evidence. The compliance department should record the results of every inquiry to allow the company to track reported concerns to see if they exhibit a pattern.

In following up on credible reports, the steps to consider include such things as interviewing the employee who made the complaint and attempting to determine the circumstances behind the complaint to determine if there is any valid basis for it. The company should inform the employee that a confidential investigation will occur and that investigators may pass on the report to members of senior management. The investigator should instruct the employee that the company will conduct the investigation through normal channels and that the employee should not attempt to conduct his or her own investigation. The investigator also should inform the employee that the company forbids retaliation and instruct the employee that if retaliatory behavior occurs, the employee should notify the compliance or legal department. The company should thoroughly investigate any complaints of retaliation.

During any investigation, the company should treat the complaining employee like any other. The company should continue to evaluate the employee's work using normal procedures and standards and should both document any positive actions taken by the company toward the complaining employee (such as awards, promotions, or raises) and the full reasons for any discipline or reprimands in case the employee later raises claims of retaliation. At the end of the investigation, the

company should inform the complaining party of the results of the investigation and what corrective steps the company took to address the substance of the complaint. Studies show that employees who believe their concerns were addressed in a thoughtful way are less likely to consider taking outside action, such as becoming a whistleblower. Due to confidentiality concerns, the company often should provide only general summaries of what occurred and how it was handled.

Step 12: Communicate with Board & Senior Management

In corporations that set the proper compliance tone, board-level involvement is regular and institutionalized. The key areas for board-level involvement include thorough oversight of compliance initiatives, quarterly reports of compliance activities, and special communications for potentially serious matters.

Board members 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 and 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. Written materials should be accompanied by direct and personal briefing by the Chief Compliance Officer or General Counsel, as appropriate.

Based on these reports and other information, board members, or the compliance or audit committee, should consider whether the company is devoting sufficient resources to the program and whether compliance personnel have a direct conduit to the board or appropriate board committee.[5] They also should consider whether the compliance plan appropriately covers all areas of the company.

Boards or committee members that receive compliance reports also need to probe beyond the four corners of the reports. They should assure themselves that the reports are complete, accurate, and do not present a whitewashed version of compliance issues. If a high-level person who has oversight of compliance presents the report, this may require additional reports from the person who has day-to-day responsibility for the compliance program, as called for by the Commentary to the Sentencing Guidelines.[6] Sometimes, it may be appropriate for the board to meet with the internal auditor.

A final consideration is communications with shareholders, if a publicly traded company is involved. The board, or the compliance or audit committee, needs to determine when a potential compliance situation is important enough to require disclosure as a material fact. This can involve any situation where the potential costs of investigation are high (and therefore material), 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 the nature of a transaction involving Iran under new SEC disclosure requirements related to such conduct.

* * *

As noted above, compliance is an exercise in identifying and managing regulatory risk. The starting basis for such a compliance exercise is the conduct of a full risk assessment. A risk-assessment toolkit, including a detailed risk-assessment questionnaire, an International Compliance Guide, and a guide to conducting internal investigations (should compliance break down) is available by contacting the author at ghusisian@foley.com or +1 202.945.6149.

---

[1] For example, in the settlement of the ENI FCPA investigation, the SEC premised its claims, in part, on its view that ENI had "failed to ensure that Snamprogetti [a subsidiary] conducted due diligence on agents hired through joint ventures in which Snamprogetti participated." Securities and Exchange Commission v. ENI, Civ. Action No. 4:10-cv-2414 (Jul. 7, 2010), http://www.sec.gov/litigation/complaints/2010/comp-pr2010-119.pdf. It is true that in this particular case, the subsidiary was covered by ENI's FCPA compliance procedures. Nonetheless, this case underscores the view of the U.S. government that it is the responsibility of companies to ensure that close affiliates, including joint venture partners, are taking actions to ensure there is reasonable due diligence for anyone acting on behalf of the affiliated companies.

[2] In the Siemens case, the DOJ alleged that Siemens provided only limited internal audit resources to support its compliance efforts in comparison to the breadth of the company's operations. See United States v. Siemens Aktiengesellschaft, No. 08-CR-367 (D.D.C., Dec. 12, 2008) (information at ¶ 135), http://www.justice.gov/criminal/fraud/fcpa/cases/docs/siemensakt-info.pdf.

[3] 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).

[4] See, e.g., Hollis v. City of Buffalo, 28 F. Supp. 2d 812, 821 (W.D.N.Y. 1998) (rejecting a company defense based on good faith compliance efforts, due to failure of company to conduct ongoing education or to recirculate compliance materials).

[5] As the Sentencing Guidelines note, a corporation should support the person running a compliance program with "adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup." U.S. Sentencing Guidelines Manual § 8B2.1(b)(2)(C).

[6] U.S. Sentencing Guidelines Manual § 8B2.1 (commentary note 3) (discussing annual reports from the person with day-to-day responsibility).