5 Essential Elements of Corporate Compliance

: A GLOBAL TEMPLATE

Baker & McKenzie

Content

Introduction →4

Essential Element 1 - Leadership →6

Essential Element 2 - Risk assessment →8

Essential Element 3 - Standards and controls →10

Essential Element 4 - Training →12

Essential Element 5 - Oversight →14

Top 20 FCPA Settlements →16

Where the Bribes Are →16

Compliance Milestones →17

Map: Corruption Perceptions Index →18

Introduction

Today's compliance environment

Maintaining a strong corporate compliance program designed to help prevent corporate officers and employees from engaging in illegal practices such as bribery, collusion, money laundering and fraud sounds simple enough. In reality, it's much more challenging. Today's multinational companies have thousands of employees, multiple business partners and extensive operations throughout the world, including in emerging markets where the rules of public and commercial engagement often differ greatly from what they're used to at home.

In China, for example, foreign multinationals do most of their business with state-owned or state-operated companies, which can get them into trouble under the US Foreign Corrupt Practices Act's prohibition against making illegal payments to foreign officials. In Russia, a foreign company may find it challenging to get its products into the country without bribing customs officials. In Brazil, foreign companies may have difficulty winning public bids without paying someone to shape the request for proposal in their favor.

Despite the impact of globalization on the business landscape, enforcement officials aren't giving companies any breaks for improper behavior. In fact, FCPA investigations have shot up dramatically in recent years, fines have skyrocketed and multi-country government investigations have become increasingly common. These days, a Brazilian subsidiary of a US company that comes under investigation by Brazilian authorities will likely also receive a subpoena from the US government.

With the stakes so high, what is a compliance-minded company to do? Where should it look to evaluate the strength of its compliance program?

The answer to that question has become increasingly complicated. The gold standard for what types of rules, protocols, communications and oversight a company must have to meet the government's compliance program requirements used to be the US Sentencing Guidelines' "Seven Elements of an Effective Compliance Program," originally published in 1991. Since then, however, those guidelines have been revised numerous times and other standards have been added to the equation.

In 2004, for example, the US government enacted additional amendments to the federal sentencing guidelines for organizations. The amendments placed an even greater emphasis on promoting a culture of ethical corporate behavior by highlighting the responsibility of boards of directors to oversee corporate compliance programs and the importance of exercising due diligence to deter, prevent and detect criminal conduct. In 2010, the Organization for Economic Co-operation and Development released its "13 Good Practices on Internal Controls, Ethics and Compliance." A year later, the UK Ministry of Justice published six principles for "adequate procedures" following the enactment of the UK Bribery Act. Transparency International, a leading anticorruption organization, has also established "Nine Business Principles for Countering Bribery."

Beyond those standards, US Justice Department prosecutors routinely insert compliance program requirements into settlement agreements they reach with companies under investigation for corruption — further adding to the long checklist of what the government expects companies to do to detect and prevent misconduct.

The good news is that although these guidelines vary in length, tone and language, they have a lot in common. They all touch upon a set of key issues that can be boiled down to five essential elements: leadership, risk assessment, standards and controls, training and communication, and oversight.

If a company's corporate compliance program effectively covers these five essential elements, it will likely fulfill the wide variety of law enforcement expectations around the world and help prevent costly prosecutions. In the event of a government investigation, a company with a robust compliance program that encompasses these five elements is much more likely to be granted compliance credit, a reduction in penalties and other forms of leniency that could ultimately minimize damages.

The key factors that US prosecutors consider when deciding whether to file an enforcement action include a company's level of cooperation and its preexisting compliance program. To help companies meet the government's demands for maintaining successful compliance programs, we've distilled the various standards to five essential elements based on our extensive experience working on these cases in jurisdictions around the world. For each element, we've included specific actions that companies can take to ensure they are fulfilling the requirements of each element.

Global compliance requirements boiled down to five essential elements.

Leadership

What the guidelines say about leadership:

USSG: Leaders understand and oversee the compliance program to verify its effectiveness; specific individuals have the authority and responsibility to carry out the program. The company denies leadership positions to people who have engaged in misconduct.

OECD: Support from senior management is strong, explicit and visible. Program is overseen by senior corporate officers with sufficient resources, authority and access to the board.

UK's 6 Principles: Top-level commitment.

A successful compliance program must be built on a solid foundation of ethics that are fully endorsed by senior management. Otherwise it's just a hollow set of internal rules and regulations. But compliance standards require even more than support from the top. Companies must have high-ranking compliance officers with the authority and resources to manage the program on a day-to-day basis. And compliance officers must have the ear of those ultimately responsible for corporate conduct, including the board of directors.

In fact, the US Sentencing Commission reinforced the importance of giving compliance officers direct access to the board of directors when it published amendments to the US Sentencing Guidelines in 2010. To receive a "culpability score reduction" during sentencing, a company must now show that its compliance officers can promptly report any matter involving criminal conduct directly to the board or appropriate board committee. Compliance officers should also report to the board on the implementation and effectiveness of the company's compliance program at least once a year.

As a best practice, however, we advise clients to take this component of their programs a step further. We recommend that a company's chief compliance officer or legal department compliance manager provide quarterly presentations to the board about ongoing internal investigations, general developments in anticorruption laws and enforcement, compliance challenges the company is facing and what is being done to address those challenges. That way, it is clear that the line of communication between the compliance team and the board is open.

Recommendations

Here are some other recommendations to help your company fulfill the leadership element of effective compliance:

Make sure central compliance is communicating with those in the field. One of the biggest impediments to effective compliance leadership is poor communication between a company's central compliance department and country managers working in the field. This can be a major oversight considering that country managers are often the employees in the trenches overseeing sales people and third-party agents who are selling and distributing the company's products and services. Neglecting to provide appropriate compliance training for country managers or keep them in the corporate loop increases the chances that efforts to establish a strong local compliance culture will fail. Local managers are often best situated to set the tone for compliance and to detect and address illegal or unethical practices before they become compliance issues that put the company at risk.

Place compliance officers in high-risk markets. Another common oversight is failing to have well-trained compliance personnel in a company's foreign offices. Maintaining a leadership structure that is too centralized will stifle efforts to foster a healthy compliance culture across all geographies and to minimize global risk. Ethical edicts issued from faraway headquarters are often ineffective without buy-in from local managers who have the training and experience to reinforce such rules. The determination of which overseas offices should have the strongest compliance presence should be made on a risk basis. Companies can begin by building an active presence of trained compliance managers in markets with the greatest compliance risk, then expand this presence to other jurisdictions.

Create a global compliance committee. Another way to avoid communication breakdown is to establish a global compliance committee comprised of trained leaders from your central compliance department, internal audit, country managers and local compliance officers working in your foreign offices. The committee should consider holding monthly or bimonthly conference calls to discuss compliance issues and keep members aware of potential problems, as well as what is being done to address them. A commitment to this level of global communication increases your chances of establishing a healthy compliance culture that permeates the entire company.

Conduct periodic board training and provide reports on hot topics in compliance and risk management. Corporate board members face the possibility of personal liability for failing to meet their fiduciary responsibilities in overseeing the business' policies and practices. With greater awareness of compliance issues from sources such as whistleblowers and bloggers comes a greater duty to act. By providing regular, timely compliance training for board members and keeping them updated on compliance and risk management trends, general counsel can help directors fulfill their compliance obligations and steer the company away from potential misconduct.

Risk assessment

What the guidelines say about risk assessment:

USSG: Companies must conduct periodic assessments of risk of criminal conduct and take appropriate steps to design, implement or modify each element to reduce risk.

OECD: Risk assessment should be the basis for effective internal controls and compliance programs.

UK's 6 Principles: Broad categories of risk must be carefully examined, including country, sectoral, transaction, business opportunity and partnerships. Program priorities, resources and controls should be determined based on the results of the risk assessment.

Although the original 1991 version of the US Sentencing Guidelines did not specifically identify the completion of a formal risk assessment as one of the seven elements of effective corporate compliance, Sarbanes-Oxley directed the Commission to add it to the list. As a result, government officials now routinely emphasize risk assessments as the foundation of an effective program. What changed? The answer may be globalization.

As multinationals have expanded their enterprises and grown more dependent on global supply chains, knowing and understanding the nature and extent of business risks has become a critical first step for implementing successful compliance programs. Enforcement authorities increasingly expect multinationals to have formal processes for periodically assessing the compliance risks everywhere they do business, particularly in higher-risk regions, including emerging markets like China, Russia, India and Brazil.

During the risk assessment process, companies must evaluate numerous compliance issues, including the degree to which the company's employees conduct business with government officials, the company's use of third-party agents and intermediaries, the regulatory environment of the regions where the company operates, and the effects of any recent business developments such as new joint ventures, corporate affiliations, or expansion into markets that could create additional risk.

Recommendations

Here are some recommendations to help your company fulfill the risk assessment element of effective compliance:

Conduct annual risk assessments. The purpose of a risk assessment is to gauge where your company's greatest compliance risks are so you can target your resources in those areas and establish policies and protocols to minimize those risks. Yet it's surprising how many companies do not perform this task. Companies will often wait until something goes wrong before self-assessing. To avoid the inherent risks in the "wait and see" approach, we recommend that you conduct a formal risk assessment every year. Because enforcement trends and anticorruption laws evolve rapidly and multinationals tend to go through numerous significant changes within a given fiscal year, we have found this to be an optimal timeframe.

Build this annual risk assessment into your compliance program. Not only should you conduct annual risk assessments, but you should try to perform them at the same time each year. To pass muster with the government, you need to demonstrate that your risk assessment is a regular, systemic part of your compliance efforts rather than an occasional, ad hoc exercise cobbled together when convenient. We also recommend designating a specific group, such as your internal audit department or enterprise risk management team, to conduct the annual review. This will help demonstrate to the government that your risk assessment is a formal corporate process.

Scrutinize new business partners and third-party agents. One of the areas that can get companies into compliance trouble is their lack of internal controls over business partners and third-party intermediaries such as consultants, distributors, contractors and sales agents. In fact, the majority of FCPA enforcement actions involve some use of third parties. Compliance standards require companies to conduct due diligence on new business partners and third-party intermediaries. But in the rush to close deals and enter new markets, that doesn't always happen as thoroughly as it should. Conducting a formal risk assessment each year provides an opportunity to take a closer look at newer business relationships to make sure partners and third parties do not have improper connections to government officials or involvement in unethical or illegal conduct. Any risk that you uncover should be addressed and remediated.

Update your policies and procedures based on enforcement trends. Throughout the course of a year, government officials file numerous enforcement actions against companies for all kinds of corporate misconduct. Paying attention to the specific compliance areas that the government is targeting in these enforcement actions will tell you a lot about what your program needs to focus on to stay out of the government's cross hairs. If, for example, you notice that the government has been clamping down on gift giving and hospitality in Asia and you conduct considerable business in that region, that should become a focus area for your risk assessment. Then, depending on whether your hospitality policies and procedures in Asia are in line with what the government now expects, you should make necessary changes.

Memorialize your findings in an annual report. When conducted every year, routine risk assessments should only take three to four weeks, depending on the size of your company and your compliance resources. Once the assessment is complete, the compliance or audit team should compile its findings and recommendations in a comprehensive report to be presented to the chief compliance officer and board of directors for review and consideration of appropriate program enhancements.

Standards and controls

What the guidelines say about standards and controls:

USSG: Companies should have standards and procedures to prevent and detect criminal conduct. They should provide incentives and discipline misconduct.

OECD: Company policy should clearly and visibly state that bribery is prohibited. Compliance programs should address key risk areas. Companies should conduct due diligence on business partners and implement effective internal controls for accurate books and records. Employees should be able to report violations confidentially without fear of retaliation.

UK's 6 Principles: Policies and procedures should be clear, practical and accessible. Companies should have due diligence protocols for screening third-party intermediaries.

It would be challenging to find a global company today that doesn't have a code of business conduct — an easy-to-read summary of corporate do's and don'ts. But compliance standards require that companies go much further. Besides a flagship code of conduct, corporations should have detailed written policies covering issues such as bribery, corruption and accounting practices, as well as clear procedures and protocols for making sure those policies are followed and enforced.

For example, a company's code of conduct may state that bribery is prohibited. However, best practices now require companies to have additional standards and controls, including, for example, detailed due diligence protocols for screening third-party business partners for criminal backgrounds, financial stability and improper associations with government agencies.

Ultimately, the purpose of establishing effective standards and controls is to demonstrate that your compliance program is more than just words on paper.

Recommendations

Here are some recommendations to help your company fulfill the standards and controls element of effective compliance:

Establish stringent protocols for screening business partners and third parties. In most risk assessments we perform for clients, we find gaps in the company's third-party due diligence program. Many companies have not yet created an effective platform for screening business partners and third-party intermediaries for previous misconduct and improper ties to the government. Some companies still give their business partners only a cursory look — a considerable oversight considering how often government investigations involve allegations of impropriety by a company's third-party agents. To conduct proper due diligence, companies must require third parties and other business partners to complete background questionnaires detailing, among other things, their financial stability, foreign government ties and any history of investigations. Third parties should also declare their commitment to robust corporate compliance in a signed certification form. To increase accountability, we also recommend using business sponsor forms in which employees who refer or hire third-party agents provide background information about the agents, such as the experience and attributes that qualify the agents for the role they will play as new company partners.

Conduct background checks on important business partners in high-risk markets. Performing background checks on third parties can be an expensive undertaking. But it may be advisable when screening major business partners and third parties in higher-risk markets to make sure they've represented themselves accurately in their paperwork. Accordingly, consider hiring trained, local investigators to get an even clearer picture of whether your potential partner could become a compliance liability.

Include strict compliance covenants in your third-party contracts. Today's best practice compliance standards also strongly encourage companies to require third parties and other business partners to sign contracts with provisions that give the company the right to monitor their conduct. At a minimum, these compliance covenants should cover three core concerns: adherence to the FCPA and other international anticorruption laws, audit rights, and contract termination rights. More specifically, these provisions should require the business partner to agree not to violate the FCPA and other anticorruption laws, to give the company the right to review the partner's books and records, and to enable the company to terminate the contract if it later determines the partner is engaged in misconduct, unethical behavior or illegal activity.

Establish internal controls to ensure accounting records are accurate. The FCPA requires companies to book transactions correctly by securing receipts and accurately recording the date and amount of the payment. To be compliant, companies should reconcile bank accounts with outgoing and incoming payments every month and inquire into any suspicious payments and missing funds that could indicate misappropriation or off-the-books transactions. Companies should pay particular attention to transactions with consultants and business development agents, customs payments, charitable giving arrangements, and gifts and hospitality involving government officials.

Provide clear guidelines for gift giving and hospitality. Giving clients and business associates gifts, treating them to dinner or taking them to sporting events are common business development practices. But anything too extravagant could quickly cross the line into bribery. Differences in culture and economic prosperity can make it difficult for companies to establish one-size-fits-all gift-giving and hospitality guidelines for the countries where they conduct business. While paying $150 a head for a business dinner in France may not constitute bribery, for example, in poorer countries like Nigeria or Cambodia it could. That's why it's so important to tailor hospitality policies to individual countries. Companies can do this in any number of ways, including creating a thresholds table of allowable hospitality amounts that is based on local laws and regulations in each country where they operate, plus advice from experienced local counsel.

Training

What the guidelines say about training:

USSG: Companies must communicate the standards and procedures of its compliance program and conduct effective training.

OECD: Training should be periodic, consistent, and documented.

UK's 6 Principles: Effective implementation of compliance program policies and procedures through adequate training.

One of the most important elements of a strong compliance program is properly training company officers, employees and third parties on relevant laws, regulations, corporate policies, and prohibited conduct. In recent years, the rise of technology platforms such as webinars, video conferencing and online self-testing has made training easier and more affordable.

But simply conducting some compliance training for employees isn't enough. Enforcement officials want to be sure management's message got through. Thus, when determining whether a company's training program meets its expectations for effectiveness, the government often scrutinizes who a company trains, how the training was conducted and how often training occurs.

Recommendations

Here are some recommendations to help your company fulfill the training element of effective compliance:

Provide live compliance training for country managers. If resources permit, officers and managers in your foreign offices should receive live, in-person compliance training every year, particularly those working in your highest risk markets. In the compliance world, anticorruption laws, enforcement trends and government priorities change quickly. Thus, waiting more than a year to conduct periodic compliance training can impede awareness. If lack of resources is an issue, conducting live videoconferences or webinars with question-and-answer sessions is a good alternative.

Train the right people. When providing compliance training, it's important to prioritize which audience to educate first, particularly when you have limited resources. Besides country managers, it's important to focus your initial training efforts on high-risk markets and directors, officers and sales employees who have direct contact with government officials or deal with state-owned entities. Then expand the training around the globe and across your employee spectrum.

Conduct live, annual training in high-risk markets. Enforcement officials have made it clear that live, in-person training is the preferred method in high-risk markets and that this training should be relatively frequent. Therefore, merely conducting a simple five-question online FCPA test in a higher-risk country such as Russia, or performing training in China once every five years will probably not be sufficient from a regulator's perspective. Also, one of the many benefits of conducting live, in-person training is that you often receive immediate feedback when talking to employees in person that you would not typically get from an online course or webinar. During live training, employees are more likely to casually mention a potentially risky practice, giving you the opportunity to address an impropriety before it becomes a larger problem.

Develop your training to address a broad range of global issues. Some companies make the mistake of having a generic script for all compliance training that misses the practical challenges employees routinely face. Training programs typically cover the FCPA, UK Bribery Act, OECD guidelines and enforcement trends in other countries. Additionally, you need to focus on the specific compliance risks in the country where the employees are working. In China, for example, training should address the many corruption risks of dealing with state-owned entities. In Brazil, training should include guidance on how to handle government officials who expect facilitation fees to move business processes along more quickly.

Update your training regularly. Enforcement trends and anticorruption laws change quickly, and government officials are increasingly collaborating across borders to conduct large-scale investigations. That's why it is important to monitor what's happening around the world and incorporate those developments into your training. Compliance is a global issue that requires corporate vigilance and constant attention. By providing timely, effective employee training, companies can demonstrate their commitment to cultivating and supporting a strong compliance culture.

Oversight

(Monitoring, Auditing, and Response)

What the guidelines say about oversight:

USSG: Companies should monitor and audit their compliance programs and maintain reporting mechanisms. They should respond quickly to allegations and modify their programs as needed.

OECD: Individuals at all levels of the company should be responsible for monitoring. Companies should discipline employees for violations of the policy. Companies should regularly review their compliance programs and make necessary revisions.

UK's 6 Principles: Companies must monitor and review their compliance programs.

After all the ethical messages have been put in place and communicated to the appropriate audiences, the question remains whether the workforce is actually complying. Two of the seven compliance elements in the US Sentencing Guidelines call for corporations to monitor, audit, and respond quickly to allegations of misconduct. These three activities — monitoring, auditing and responding — are key components enforcement officials look for when determining whether companies maintain adequate oversight of their compliance programs.

Many companies, however, fall short on this element, often because of confusion about the differences between monitoring and auditing. Monitoring is a commitment to reviewing and detecting compliance problems in real time, then acting quickly to remediate them. The primary goal is to identify and address gaps in your program on a regular basis. An audit is a more limited review that targets a specific business component, region or market sector during a particular timeframe to uncover or evaluate certain risks. Some companies assume that because they conduct audits or have a dedicated auditing team, they are effectively monitoring. This is usually not the case. A robust compliance program should include separate monitoring and auditing functions.

While unique in protocol, however, these two program components are often viewed as compliance "cousins" because they often work in tandem. If, for example, you notice a trend of suspicious payments in recent monitoring reports from Indonesia, you may decide it's time to conduct an audit of those operations to target and further investigate the issue.

Recommendations

Here are some recommendations to help your company fulfill the oversight element of effective compliance:

Establish a regular monitoring system to spot problems and address them. Effective monitoring means applying a consistent set of protocols, checks and controls tailored to your company's risks to detect and remediate compliance problems on an on-going basis. For example, your compliance team should be checking in regularly with local finance departments in your foreign offices to ask whether they've noticed recent accounting irregularities. Also, as part of their corporate compliance accountability, regional business directors should be required to keep tabs on potentially improper activity in the countries they manage. And your global compliance committee or enterprise risk group should talk as often as feasible (perhaps every month) to discuss and address issues as they arise. Ongoing efforts like these will show the government that you are serious about compliance.

Require country managers to complete regular compliance reports. One of the nine factors that US prosecutors consider when deciding whether to file an enforcement action is whether a company is applying its compliance program in good faith. The program may look good on paper but the government wants to know, is it really working? One of the most effective ways of answering that question is being able to show prosecutors regular, periodic monitoring and auditing reports prepared by senior executives and managers across your operations.

Pay attention to what employees say during training. Training is a form of monitoring because it can alert you to potential problems based on the types of questions employees ask and their reception to certain concepts. For example, during training employees sometimes ask specific questions about their interactions with government officials or gift-giving practices that can raise red flags, which should be addressed quickly.

Establish protocols for internal investigations and disciplinary action. Responding swiftly and effectively to compliance issues will sometimes require your company to conduct an internal investigation. Before an internal investigation, however, each company should have procedures in place to make sure every investigation is thorough and authentic. Those procedures should include document preservation protocols, data privacy policies, and communication systems designed to manage information and get it to the appropriate people quickly. Best practice compliance guidelines also encourage companies to establish disciplinary policies that clearly state how they regulate and discipline employees engaged in misconduct.

Remediate problems quickly. A key concept behind the oversight element of effective corporate compliance is the idea that if companies are policing themselves for compliance-related issues, the government won't have to do it for them. That is why remediation is such an important component of oversight. If it's clear, for instance, that your sales people in Thailand are doing something potentially improper partly because they never received adequate compliance training, remediate the deficiency by scheduling that training immediately. In the end, it's not enough to just gather information and identify compliance problems. To fulfill this essential element of compliance, you have to fix them.

Top 20 FCPA Settlements*

	Company	Industry	Fine (USD)	year of settlement
1	Siemens	Electronics	$800 million	2008
2	KBR/Halliburton	Engineering/Energy	$579 million	2009
3	BAE	Aerospace	$400 million	2010
4	ENI S.p.A.	Energy	$365 million	2010
5	Technip	Engineering/Energy	$338 million	2010
6	JGC Corporation	Engineering/Energy	$219 million	2011
7	Daimler	Automotive	$185 million	2010
8	Alcatel-Lucent	Telecommunications	$137 million	2010
9	Deutsch / Magyar Telekom	Telecommunications	$95 million	2011
10	Panalpina	Freight forwarding/Transportation	$82 million	2010
11	Johnson & Johnson	Pharmaceutical/Consumer goods	$70 million	2011
12	ABB	Technology	$58 million	2010
13	Pride International	Energy	$56 million	2010
14	Marubeni Corporation	Trade	$54 million	2012
15	Baker Hughes	Engineering/Energy	$44 million	2007
16	Willbros	Engineering/Energy	$32 million	2008
17	Chevron	Energy	$30 million	2007
18	Titan	IT/Communications	$29 million	2005
19	Bridgestone	Auto parts manufacturing	$28 million	2011
20	Vetco	Engineering/Energy	$26 million	2007

*Fines listed are as of February 1, 2012

Where the Bribes Are

Passed in 1977, the FCPA has led to more than 200 cases covering illegal activity in 80 countries. Companies in certain industries are more prone to prosecution than others. Here is a list of the total FCPA fines by industry since 1977.

Industry	Total fines
Energy	$2.03 billion
Consulting	$846.76 million
Defense & Aerospace	$443.29 million
Manufacturing	$225.80 million
Telecommunications	$218.14 million
Infrastructure	$144.34 million
Health & Pharmaceuticals	$84.62 million
Agriculture	$50.83 million

Source: James Mintz Group

Milestones

1909

New York Central & Hudson River Railroad v. U.S., 212 U.S. 481

Significance: In this case, NY Central Railroad and one of its managers were convicted of bribery for giving lower shipping rates to certain sugar companies in violation of the Elkins Act. NY Central Railroad argued that Congress had no authority to hold the company responsible for a crime committed by one of its employees. In affirming the conviction, the US Supreme Court ruled for the first time that a company can be held criminally liable for the acts of its employees who commit crimes to benefit the company.

1991

Amendments to U.S. Sentencing Guidelines

Significance: For the first time, the US government provided a framework for how companies should deter and prevent crimes such as corporate fraud, bribery and collusion. Now often referred to as the "seven elements of effective compliance," the underlying theory was that if companies received sentencing breaks for having bona fide compliance programs, they would be motivated to police themselves internally. Largely as a result of these guidelines, today's public companies and the majority of private ones maintain corporate compliance programs.

1999

DOJ Principles of Federal Prosecution of Business Organizations

Significance: In this memo written by then-Deputy Attorney General Eric Holder Jr., the DOJ established nine factors federal prosecutors must consider when deciding whether to charge a corporation with criminal misconduct. Those factors include a company's "timely and voluntary disclosure of wrongdoing" and its "willingness to cooperate in the investigations of its agents." The principles, which have been amended many times in recent years, have had a major impact on the fate of corporations being investigated for corruption. A subsequent memo written by then-Deputy Attorney General Paul McNulty in 2006 required prosecutors to give companies credit for having a pre-existing compliance program when deciding whether to charge them. This provision of the McNulty Memo gave companies greater incentive to become more proactive in establishing corporate compliance programs before they came under investigation.

2002

Sarbanes-Oxley Act

Significance: Enacted following accounting scandals at corporations such as Enron, WorldCom and Tyco, this act, often referred to as "SOX," established new financial requirements for US public companies, such as requiring that all financial statements include an internal controls report certifying their accuracy. It also created new accountability for chief executives, corporate boards and auditors, who can be held personally liable for noncompliance. A CEO or CFO who submits an inaccurate certification, for example, is subject to a fine up to $1 million and up to 10 years in prison. SOX also encourages the disclosure of corporate fraud by protecting whistleblower employees who report illegal activities.

2005

FCPA Enforcement Surge

Significance: Since 2005, the DOJ and SEC have brought more than 200 FCPA enforcement actions against corporations and their officers and employees — a huge number considering that these agencies had filed less than 60 actions in the previous 27 years since the FCPA was enacted. In the past decade, the US government has made FCPA enforcement a much greater priority by hiring more prosecutors, training specialized anti-corruption units, targeting corporate officers along with companies, encouraging corporations to self-disclose violations and investigating more small and mid-sized companies. That surge in enforcement has led to a corresponding surge in corporate compliance. For example, during the uptick in enforcement, the DOJ and SEC have used calculated messages in settlement papers and public appearances to provide guidance on how companies can enhance their anti-corruption compliance programs to mitigate penalties and avoid prosecution. This, in turn, has motivated companies to strengthen their compliance policies and procedures, hire experienced compliance officers, broaden FCPA training efforts, and develop more robust internal controls.

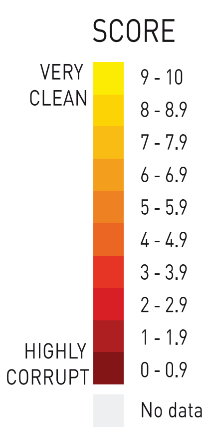
2010

UK Bribery Act

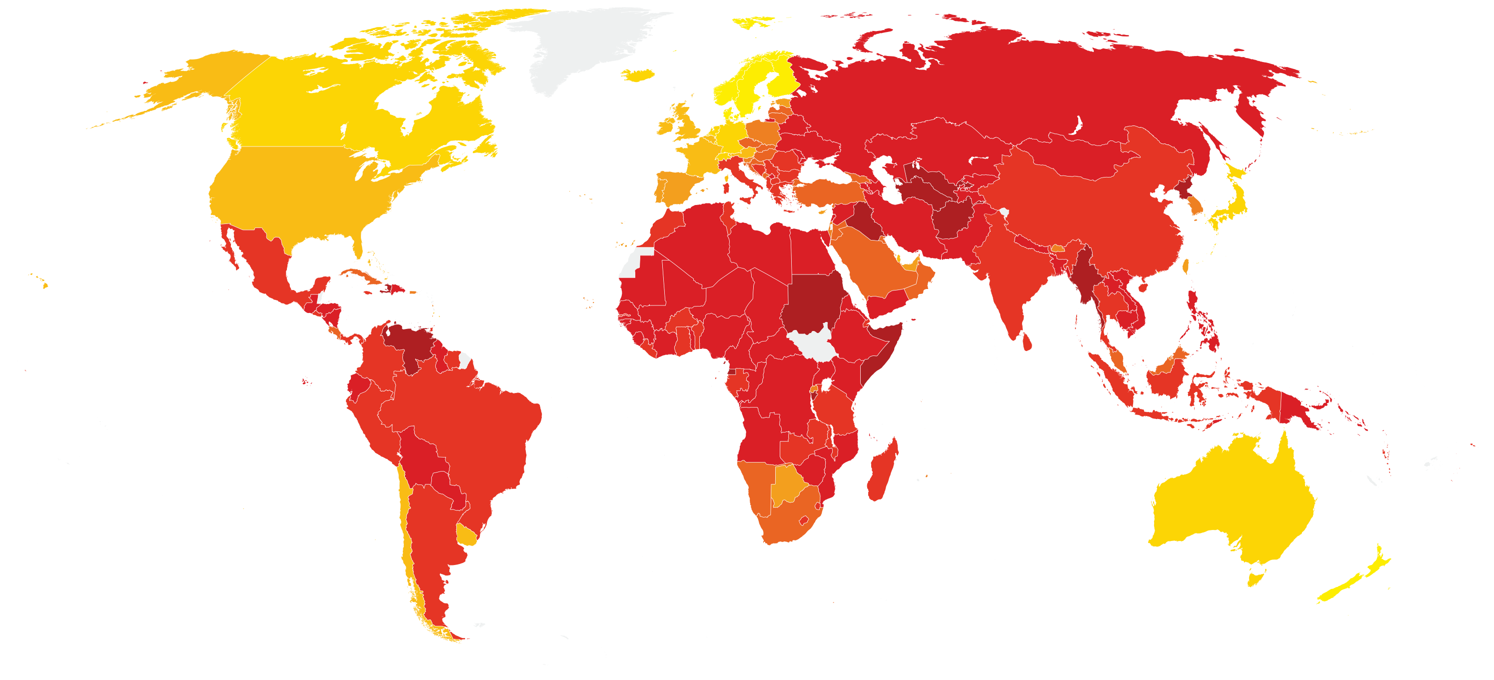
Significance: Since the FCPA was enacted in 1977, it has been the most far-reaching, aggressively enforced anti-corruption statute in the world. By passing the Bribery Act, the UK joined the US in providing its regulators with broad powers to prosecute foreign bribery — putting multinational companies at even greater risk of criminal and civil liability. In some ways the Bribery Act is even stricter than the FCPA because it makes it illegal for companies and its agents to bribe anyone, not just foreign officials. It also makes no concessions for facilitation payments — small fees paid to government employees to expedite or secure performance of routine governmental actions. The only defense to the Bribery Act's corporate offense for "failure to prevent bribery" by an associated person is the company's ability to prove it had "adequate procedures" in place to prevent bribery at the time of the alleged impropriety.

2011 Corruption Perceptions Index

THE PERCEIVED LEVELS OF PUBLIC-SECTOR CORRUPTION IN 183 COUNTRIES/TERRITORIES AROUND THE WORLD



RANK	COUNTRY/TERRITORY	SCORE
1	New Zealand	9.5
2	Denmark	9.4
2	Finland	9.4
4	Sweden	9.3
5	Singapore	9.2
6	Norway	9.0
7	Netherlands	8.9
8	Australia	8.8
8	Switzerland	8.8
10	Canada	8.7
11	Luxembourg	8.5
12	Hong Kong	8.4
13	Iceland	8.3
14	Germany	8.0
14	Japan	8.0
16	Austria	7.8
16	Barbados	7.8
16	United Kingdom	7.8
19	Belgium	7.5
19	Ireland	7.5
21	Bahamas	7.3
22	Chile	7.2
22	Qatar	7.2
24	United States	7.1
25	France	7.0
25	Saint Lucia	7.0
25	Uruguay	7.0
28	United Arab Emirates	6.8
29	Estonia	6.4
30	Cyprus	6.3
31	Spain	6.2
32	Botswana	6.1
32	Portugal	6.1
32	Taiwan	6.1
35	Slovenia	5.9
36	Israel	5.8
36	Saint Vincent and the Grenadines	5.8
38	Bhutan	5.7
39	Malta	5.6
39	Puerto Rico	5.6
41	Cape Verde	5.5
41	Poland	5.5
43	Korea (South)	5.4
44	Brunei	5.2
44	Dominica	5.2
46	Bahrain	5.1
46	Macau	5.1
46	Mauritius	5.1
49	Rwanda	5.0
50	Costa Rica	4.8
50	Lithuania	4.8
50	Oman	4.8
50	Seychelles	4.8
54	Hungary	4.6
54	Kuwait	4.6
56	Jordan	4.5
57	Czech Republic	4.4
57	Namibia	4.4
57	Saudi Arabia	4.4
60	Malaysia	4.3
61	Cuba	4.2
61	Latvia	4.2
61	Turkey	4.2
64	Georgia	4.1
64	South Africa	4.1
66	Croatia	4.0
66	Montenegro	4.0
66	Slovakia	4.0
69	Ghana	3.9
69	Italy	3.9
69	FYR Macedonia	3.9
69	Samoa	3.9
73	Brazil	3.8
73	Tunisia	3.8
75	China	3.6
75	Romania	3.6
77	Gambia	3.5
77	Lesotho	3.5
77	Vanuatu	3.5
80	Colombia	3.4
80	El Salvador	3.4
80	Greece	3.4
80	Morocco	3.4
80	Peru	3.4
80	Thailand	3.4
86	Bulgaria	3.3
86	Jamaica	3.3
86	Panama	3.3
86	Serbia	3.3
86	Sri Lanka	3.3
91	Bosnia and Herzegovina	3.2
91	Liberia	3.2
91	Trinidad and Tobago	3.2
91	Zambia	3.2
95	Albania	3.1



RANK	COUNTRY/TERRITORY	SCORE
95	India	3.1
95	Kiribati	3.1
95	Swaziland	3.1
95	Tonga	3.1
100	Argentina	3.0
100	Benin	3.0
100	Burkina Faso	3.0
100	Djibouti	3.0
100	Gabon	3.0
100	Indonesia	3.0
100	Madagascar	3.0
100	Malawi	3.0
100	Mexico	3.0
100	Sao Tome and Principe	3.0
100	Suriname	3.0
100	Tanzania	3.0
112	Algeria	2.9
112	Egypt	2.9
112	Kosovo	2.9
112	Moldova	2.9
112	Senegal	2.9
112	Vietnam	2.9
118	Bolivia	2.8
118	Mali	2.8
120	Bangladesh	2.7
120	Ecuador	2.7
120	Ethiopia	2.7
120	Guatemala	2.7
120	Iran	2.7
120	Kazakhstan	2.7
120	Mongolia	2.7
120	Mozambique	2.7
120	Solomon Islands	2.7
129	Armenia	2.6
129	Dominican Republic	2.6
129	Honduras	2.6
129	Philippines	2.6
129	Syria	2.6
134	Cameroon	2.5
134	Eritrea	2.5
134	Guyana	2.5
134	Lebanon	2.5
134	Maldives	2.5
134	Nicaragua	2.5
134	Niger	2.5
134	Pakistan	2.5
134	Sierra Leone	2.5
143	Azerbaijan	2.4

RANK	COUNTRY/TERRITORY	SCORE
143	Belarus	2.4
143	Comoros	2.4
143	Mauritania	2.4
143	Nigeria	2.4
143	Russia	2.4
143	Timor-Leste	2.4
143	Togo	2.4
143	Uganda	2.4
152	Tajikistan	2.3
152	Ukraine	2.3
154	Central African Republic	2.2
154	Congo Republic	2.2
154	Côte d´Ivoire	2.2
154	Guinea-Bissau	2.2
154	Kenya	2.2
154	Laos	2.2
154	Nepal	2.2
154	Papua New Guinea	2.2
154	Paraguay	2.2
154	Zimbabwe	2.2
164	Cambodia	2.1
164	Guinea	2.1
164	Kyrgyzstan	2.1
164	Yemen	2.1
168	Angola	2.0
168	Chad	2.0
168	Democratic Republic of the Congo	2.0
168	Libya	2.0
172	Burundi	1.9
172	Equatorial Guinea	1.9
172	Venezuela	1.9
175	Haiti	1.8
175	Iraq	1.8
177	Sudan	1.6
177	Turkmenistan	1.6
177	Uzbekistan	1.6
180	Afghanistan	1.5
180	Myanmar	1.5
182	Korea (North)	1.0
182	Somalia	1.0

Source:

www.bakermckenzie.com

Baker & McKenzie has been global since inception. Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 3,800 lawyers in 42 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.

Contacts

If you have any questions about this document or would like more information about our Global Corporate Compliance Practice, please contact Sue Boggs at sue.boggs@bakermckenzie.com / +1 214 965 7281.

© 2012 Baker & McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.