Corporate Duty to Respect Human Rights: Due Diligence Requirements

John F. Sherman, III
Deputy General Counsel
National Grid
November 30, 2007

What is the scope of the due diligence process required to determine if a company has discharged a duty to respect human rights? This note suggests that the COSO internal controls framework, which is widely used in the United States, could provide a robust due diligence foundation for such an assessment. There are other control frameworks from other countries to be considered, but COSO is a good place to start.

The UN Committee on Economic, Social, and Cultural Rights (CESR) has defined the state duty to respect human rights as a negative duty to "refrain from restricting the exercising of human rights." [1] It is, in essence, a duty to do no harm. However, this does not describe the steps that a company should take to respect human rights and do no harm to human rights holders.

Before the steps can be defined, the state duty to respect must first be translated into corporate obligations, since companies, unlike states, are limited purpose entities with no power to legislate or adjudicate, and varying abilities to impact human rights.[2] Expectations of appropriate corporate conduct are unclear; currently, companies are uncertain as to what practical actions they should take to discharge their human rights obligations, beyond the need to comply with statutes imposing liability directly upon them and to avoid complicity with human rights violations committed by others.

Once this translation is done, it is critical to understand what steps a company must take to discharge its human rights obligations. Even a negative corporate obligation to avoid harming human rights may require considerable positive action. A company will not know if it harming human rights unless it understands the impact that it has on human rights holders, and takes effective measures to avoid and mitigate any adverse impacts. These activities require proactive measures. For example, well run companies understand that they must provide a discrimination-free workplace for their employees as a matter of law and/or enlightened self interest. Moreover, providing such a workplace also discharges a fundamental human rights obligation.[3] No one would argue seriously that a company could provide such a workplace merely by issuing a code of conduct

---

[1] CESR, The Right to Water, General Comment 15, par 21.

[2] Such translation is a core part of the ongoing work of the Business Leaders Initiative on Human Rights (BLIHR). www.blihr.org

[3] Universal Declaration of Human Rights, Article 2; International Covenant on Civil and Political Rights, and International Covenant on Economic, Social and Cultural Rights, Article 2; Various ILO Conventions.

prohibiting discrimination. Instead, a company must take active steps to create such an environment, including training, monitoring of workforce demographics, the investigation of discrimination allegations, and the creation of a culture that promotes inclusion and diversity.

Thus, it would not be accurate to conclude that a corporation can discharge its duty to avoid harming human rights only by refraining from taking action. As seen below, the steps could be negative or affirmative depending upon the human right at issue, the impact that the company has on that right, the degree of control and capacity that the company has to affect that right, and the reasonable alternatives available to the company to avoid or minimize infringing that right.

Defining Due Diligence: The COSO Internal Control Framework

The steps that a company should take to discharge a duty of care are commonly referred to as "due diligence". Before discussing due diligence, a brief discussion of the corporate duty of care in the United States is in order. Generally, a board of directors owes a monitoring duty to the company with respect to certain critical activities, including ensuring legal and ethical conduct by the company's officers and employees.[4] This duty must be discharged with a fiduciary duty of care and loyalty. With respect to prevention of misconduct, for example, directors would not have discharged their fiduciary duty if they "utterly failed to implement any reporting or information system or controls" regarding the prevention of misconduct, or "having implemented such a system of controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[5] The steps that a board needs to take to discharge this duty are called due diligence; it is not a fixed and immutable term, but is quite protean and varies according to the duty and the circumstances.[6]

What then, would be the due diligence steps necessary to determine whether an effective set of internal controls has been established? In the United States, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published its "Internal Control - Integrated Framework" Report in 1992 in order to assess the effectiveness of corporate controls to prevent financial fraud (the "COSO Report"). www.coso.org COSO is a private sector initiative of five accounting and auditor industry associations, formed in 1985 to examine the causes of financial fraud, and to develop recommendations for public companies, independent auditors. It extensively studied systems of internal control to develop a common definition that could be used by companies, independent public accountants, legislators, and regulators, and provide a

---

[4] Knepper and Bailey, *Liability of Corporate Officers and Directors*, s. 3.12 (LexisNexis, 2006)

[5] *Stone v. Ritter*, 911 A.2d 362, 370 (Del. Sup. Ct., 2006).

[6] Traditionally, due diligence is defined as the "diligence reasonably expected from, and ordinarily exercised by, a person who seeks to satisfy a legal requirement or to discharge an obligation." Black's Legal Dictionary (West, 2004).

broad framework of criteria that companies could use to evaluate the effectiveness of their internal control systems.[7]

The criteria of the COSO Report have enjoyed widespread acceptance; external auditors have used it to assess the effectiveness of a company's financial controls; the US Securities and Exchange Commission followed COSO in implementing the financial self assessment requirements of Section of 404 of the Sarbanes Oxley Act; the US Congress used COSO to define an effective ethics and compliance program to prevent corporate crime; and its elements appear in the BLIHR Human Rights Business Management Guide described below. This shows that the principles are highly adaptable to different control environments.

The US Sentencing Guidelines, described in further detail below, deserves special mention. Congress enacted them in 1991 to restrict the discretion of federal judges in sentencing individuals and companies, out of a concern that sentences were highly variable and unpredictable. As applied to companies, the Guidelines created a series of maximum penalties which can be reduced sharply if the company shows that the employee who committed the crime was, in essence, a rogue who violated clearly articulated and enforced company policy. To mitigate the penalty, the company had to show the judge that at the time of the crime, it had an effective program to prevent criminal conduct by its employees. The Guidelines were based on COSO principles and outline the minimum requirements of such a program.

Although the Guidelines were enacted in the federal criminal context, their requirements took on an independent life in the corporate governance arena, which is a matter of civil law in the company's state of incorporation. In particular, in the *Caremark* case in 1996, the Chancery Court of Delaware (home state of incorporation of many if not most major US companies) used the COSO-derived due diligence program in the Guidelines as the benchmark for determining whether a Board of Directors has met its fiduciary duty to its shareholders to have an effective compliance program.[8] This represented a significant departure from prior law, because it replaced "a relaxed approach to director oversight with one that created a fiduciary obligation to assure that a

---

[7] See," *Management" Reports on Internal Controls: A Legal Perspective*, Committee on Law and Accounting, American Bar Association, 49 Bus. Law 889 (1994); Covington & Burling Memo on Internal Controls, June 13, 2003, p 5.

[8] "Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account [the promulgation of the Guidelines] and the enhanced penalties and the opportunities for reduced sanctions that it offers." *In re Caremark Int'l, Inc. Derivative Litig*., 698 A.2d 959, 970 (Del. Ch. 1996) (applying the Guidelines' definition of an effective compliance program to a health care company). *Caremark* was a derivative action filed by Caremark's shareholders in Delaware state court against its board of directors in Delaware state court, alleging that the Caremark Board of Directors breached their fiduciary duty of care to Caremark in connection with alleged violations by Caremark employees of federal and state laws and regulations applicable to health care providers, which resulted in a four year federal investigation, a criminal indictment, a guilty plea to mail fraud, and the payment of about $250 million in fines and reimbursement. The shareholders sought to recover the $250 million from the Board members.

legal compliance mechanism existed within the organization."[9] The *Caremark* standard makes the board liable for inaction; *i.e.*, failing to have the appropriate reporting circuitry in place that would have enabled it to learn about and prevent potential criminal conduct by its employees.[10]

In the future, the oversight responsibilities of boards could expand to include a duty to ensure that the company is respecting human rights. This expansion could result from a variety of factors, including greater appreciation of the connection between ethical business conduct and human rights, the translation of the Universal Declaration of Human Rights into practical business obligations, and generally accepted practice due to the voluntary adoption of human rights duties by major companies.[11] Whatever the source of such a duty, it will be necessary to develop due diligence standards for a control system to enable companies to know whether they meet that duty.

There are five COSO internal control principles -- (1) Control Environment, (2) Risk Assessment, (3) Control Activities, (4) Information and Communication, and (5) Monitoring – which are explained as follows:

1. **Control Environment –** Sets the tone of the organization and is the foundation for all other components of internal control, providing discipline and structure.

2. **Risk Assessment** – Identification and analysis of relevant risks to the achievement of objectives.

3. **Control Activities** – Policies and procedures that help ensure that management's directives are carried out; control activities occur at all levels and functions of an organization and include activities such as: approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

4. **Information and Communication** – Timely identification, capture, and communication of all pertinent information; all staff must have means of communicating information upward, and the organization must have effective channels and strategies for communicating with external parties (e.g., shareholders, customers, suppliers, and regulators). Further, management must send a clear message to employees that control responsibilities must be taken seriously.

---

[9] Gyves, *In re Caremark: Good Intentions, Unintended Consequences*, 39 Wake Forest L. Rev. 691,699 (2004).

[10] "Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation … only a sustained or systematic failure of the board to exercise oversight--such as an utter failure to attempt to assure a reasonable information and reporting system exists--will establish the lack of good faith that is a necessary condition to liability." *Caremark*, 698 A.2d at 971.

[11] Sherman, *Human Rights Implications of the 2004 Amendments to the US Sentencing Guidelines for Organizational Defendants*, Paper submitted to the International Commission of Jurists (2006), available at http://www.ibanet.org/publicprofinterest/CSR.cfm; Williams and Conley, *Is there An Emerging Fiduciary Duty to Consider Human Rights?*, 74 U.Cinn. L. Rev 75 (2005).

5. **Monitoring** – Scope and frequency of internal controls evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures; organizations should establish self-monitoring systems and review processes.

COSO Example No. 1: The US Sentencing Guidelines for Organizational Defendants

Although the COSO internal controls framework had its origins in the prevention of financial fraud, its use has spread beyond the financial fraud arena. As noted above, it underlies the components of an effective ethics and compliance program that a company must adopt under US law in order to prevent its employees from engaging in criminal conduct of any kind.[12] The ultimate goal of the program – to prevent corporate crime -- can be characterized as negative. However, the actions needed to achieve this goal are quite proactive, and can be slotted into the COSO framework, as follows:

1. **Control Environment:** (a) promoting an ethical culture; (b) requiring the board of directors to be knowledgeable about and exercise reasonable oversight regarding the effectiveness of the program; (d) assigning high level corporate personnel with the responsibility to supervise the program; (e) assigning adequate responsibility, authority, and top level access to those running the program on a day to day level; and (f) enforcing the program through incentives and discipline;

2. **Risk Assessment:** assessing the risk of corporate crime;

3. **Control Activities:** (a) developing a program that is reasonably designed, implemented, and enforced to prevent and detect and prevent criminal conduct; (b) facilitating receipt of compliance complaints; and (c) investigating compliance incidents to identify causes and to implement effective remedial measures in order to prevent future incidents.

4. **Information and Communication**: (a) communicating periodically and practically the company's standards and programs to those responsible for running the ethics and compliance program on a day to day basis; and (b) training employees on their individual ethics and compliance roles and responsibilities

5. **Monitoring:** monitoring and auditing the program's effectiveness;

COSO Example No. 2: Human Rights Business Management Guide

Many of the COSO internal control elements are also present in the due diligence steps outlined in the *Guide for Integrating Human Rights into Business Management* (the "Human Rights Business Management Guide") prepared by the Business Leaders Initiative on Human Rights, the Global Compact, and the UN Office of the High Commissioner for Human Rights[13]. Again, its components can be fitted into the COSO framework, as follows:

---

[12] 2005 Federal Sentencing Guidelines, §8B2.1. Effective Compliance and Ethics Program.

[13] www.blihr.org The Guide also has elements of a related COSO framework, "Enterprise Risk Management: Integrated Framework" (2004), which is focused on risk identification and mitigation.

1. **Control Environment:** (a) developing an overall human rights strategy, and refining it through a circle of continuous improvement; (b) defining and embedding appropriate management responsibilities; (c) integrating human rights into the company's activities;

2. **Risk Assessment:** identifying human rights risks and priorities for action;

3. **Control Activities:** (a) including human rights in existing policies; (b) developing stand alone human rights policies as appropriate; (c) learning from sector wide initiatives; (d) responding appropriately to unexpected human rights issues; and (e) setting key performance indicators to assess human rights performance.

4. **Information and Communication:** (a) understanding why human rights are important to business communications; (b) integrating human rights into internal and external communications; (c) training appropriate target groups in what they must know and do about human rights; (d) reporting on human rights performance to key audiences, external and internal.

5. **Monitoring:** (a) conducting human rights audits based on key performance indicators and (b) learning from the results of such audits.

COSO Example No. 3: A Due Diligence Program for Corporate Human Rights Performance

What, then, could the COSO internal control principles imply for the due diligence steps necessary to discharge a corporate duty to respect human rights? Combining elements of the US Sentencing Guidelines with the Human Rights Business Management Guide, a human rights due diligence program could fit into the COSO framework as follows:

1. **Control Environment:** The company promotes an ethical organizational culture that is aware of and respects of human rights through top commitment and appropriate incentives and disincentives;

2. **Risk Assessment.** The company identifies potential adverse human rights impact of its activities upon persons impacted by its operations by identifying the rights, the rights holders, and the specific company operations at issues

3. **Control Activities.** The company designs, implements, and provides sufficient resources for, effective management policies, plans and procedures to ensure that its mitigation/avoidance measures are effective, as measured by key performance indicators, and , takes human rights into account when evaluating the impact of its operations on rights holders; and provides effective mechanisms for addressing human grievances that arise from the company's operations;

4. **Information and Communication.** The company effectively communicates its human rights policies to the company, trains employees and managers

on how to identify and address human rights issues, and tracks its human rights performance using appropriate key performance indicators.

5. **Monitoring.** The company internally and externally monitors the effectiveness of its human rights performance, and studies the causes of human rights incidents in order to prevent their recurrence.

There could be many different articulations and orderings of these principles, but they easily form the basic elements of a human rights due diligence process in a manner that is well understood by corporations.

Key Issues: (a) Why Culture is Critical; (b) What Diligence is Due; (c) What Other Due Diligence Frameworks Are Available.

Why is Culture Critical?

The requirement of an ethical, human rights-aware culture as the essential foundation of the overall human rights control environment (COSO Principle No. 1) is critical. The string of financial/ethical corporate disasters involving Enron, WorldCom, etc., made clear to Congress that without more, a due diligence program to prevent crime that exists outside an ethical corporate culture will exist on paper only and degenerate into a mere check the box exercise. Enron had a highly developed paper compliance program that its executives ignored when it suited their interests to do so.

That is why the US Congress required companies to promote an ethical culture in the 2004 amendments to the Sentencing Guidelines. As Steven Priest of the Ethical Leadership Group testified in support of the amendments, "if you strip everything away there are only three things that any organization needs to foster good conduct. The first is to clearly communicate standards ... that promote good conduct. The second is to have a culture, an environment, or a context in which living up to those standards is possible, and, yes indeed, even rewarded because the third thing we have to do is have consequences, positive consequences, for behaviors that live up to those standards and negative consequences for behaviors that don't live up to those standards."[14]

The importance of culture as the foundation of good conduct has been noted in other arenas as well, such as the finding of the Baker Commission that an inadequate safety culture at BP in which an entrepreneurial culture that emphasized individual over collective responsibility for safety contributed to the Texas City Refinery Explosion on March 25, 2005[15] and the comparison of two Mexican Nike suppliers, both of which had passed a compliance audit of Nike's supplier code of conduct, yet one of which had severe labor problems anyway, due to in part to its problematic corporate culture.[16]

---

[14] Public Hearing, Ad Hoc Advisory Group On Organizational Sentencing Guidelines, Plenary Session I, November 14, 2002, p. 90.

[15] Report of the BP U.S. Refineries Independent Safety Review Panel (January 2007), pp. 59-60.

[16] Locke and Romis: *Beyond Corporate Codes of Conduct: Work Organization and Labor Standards in Mexican Garment Factories*, Corporate Responsibility Initiative at Harvard JFK School of Government (2006).

Whether an ethical corporate culture is a subset of a human rights aware and respectful culture, or vice-versa, would make an interesting issue for academic debate. But this chicken/egg question is irrelevant, since the two cultures overlap greatly, and have common roots in an understanding that "ethics counts" in making corporate decisions that can potentially harm the rights and interests of the company's stakeholders.[17]

Moreover, the UDHR has a particularly strong claim to occupy the moral space of corporate decisions, since they are globally accepted and have universal authority.

What Diligence is Due?

As noted from the outset, the amount of diligence that is due in any particular case depends in large part on the circumstances. Two key drivers are the nature and definition of the human rights impacted by the company's operations, and the degree of control that the company exercises over that impact. This underscores the need for a common understanding of how the Universal Declaration of Human Rights (UDHR) translates practically into essential business obligations. It is difficult for a company to conduct a meaningful due diligence process under COSO or any other framework without clarity as to the particular human rights standards to which the company is to be held. This links directly to the work that the Business Leaders Initiative on Human Rights is doing to translate the UDHR into specific business obligations.

Once those standards are clarified, they can be applied to different aspects of the company's business. As noted at the outset, although there are numerous variations, it's generally accepted that in order to provide a discrimination free workplace, a company should take a variety of affirmative steps, including commitment by top management to implementing an such a workplace, identifying and mitigating discrimination risks, training managers and employees, and investigating discrimination incidents to identify their cause and prevent future incidents from occurring. Since many companies have highly anti-discrimination programs that don't mention human rights, the key to due diligence is making sure that the program is human rights compatible.

On the other hand, significant investments and/or construction projects that have a potential to affect the human rights of indigenous people would require a stand-alone human rights due diligence process, as described in the *Guide To Human Rights Impact Assessment And Management*, written by the International Finance Corporation, the Global Compact, and the International Leaders Business Forum, Road Testing Draft (June 2007). The Human Rights Impact Assessment (HRIA) describes an eight step COSO-compatible human rights due diligence process: (1) determining whether a full HRIA is needed; (2) identifying and clarifying the business project context; (3) setting the baseline; (4) consulting with stakeholders to verify the human rights challenges; (5) assessing the human rights impact and consequences of the project; (6) presenting the assessment findings and recommendations to management; (7) implementing a human

---

[17] Paine, *Value Shift: Why Companies Must Merge Social and Financial Imperatives to Achieve Superior Performance* (McGraw Hill, 2003), p. 141.

rights management process; and (8) monitoring, evaluating, and reporting on the management process.

As these examples suggest, the scope of due diligence should be tailored to the particular business operation. As Andrew Clapham writes, corporate human rights obligations "vary according to the nexus and the leverage that companies have with respect to the abuse."[18] The nexus and leverage is quite high in both examples, which dovetail with the Global Compact's concept of sphere of influence. The COSO principles seem sufficiently adaptable so that they can be applied to these cases as well as others over which the company has less control and impact.

What Other Due Diligence Frameworks Exist?

For public companies in the United States, the COSO internal controls principles are instantly recognized and are widely accepted by companies, accountants, auditors, legislators, prosecutors, and regulators. As a result, it is not a great leap for companies to apply the COSO principles to corporate human rights due diligence. However, for companies organized outside the US or for companies that do not trade their securities in the US, the same cannot be said. Thus a question for further exploration is what similar internal control frameworks apply in various states, and what they have in common.

Conclusion

As the foregoing discussion indicates, measuring the effectiveness of a company's respect for human rights entails a robust due diligence process that could be based on accepted and adaptable COSO internal control criteria.

[18] Clapham, *Human Rights Obligations of Non-State Actors*, (Oxford University Press, 2006), p. 230.