The Board of Directors and Internal Control

Melvin A. Eisenberg

1-1-1997

Follow this and additional works at: https://scholarship.law.berkeley.edu/facpubs

Part of the Law Commons

Recommended Citation

The Board of Directors and Internal Control, 19 Cardozo L. Rev. 237 (1997)
THE BOARD OF DIRECTORS AND INTERNAL CONTROL

Melvin A. Eisenberg*

INTRODUCTION: THE FUNCTIONS OF THE MODERN BOARD

Under the traditional legal model of the corporation, the board of directors was charged with the management of the corporation's business. Over the years, it became increasingly clear that the boards of large publicly held corporations—with which this Article is concerned—rarely, if ever, performed the management function. Today, there is a widespread consensus that in such corporations the management function is vested not in the board, but in the executives.

Boards do not manage because they are institutionally unable to do so. Boards typically meet only six to twelve times a year. The complex business of a publicly held corporation cannot be managed with such a limited investment of time. Boards include persons who either are not managers at all or are managers whose experience lies in different businesses. The complex businesses of a publicly held corporation cannot be managed by such persons.¹

The picture does not change even where a corporation has a controlling shareholder. As Warren Buffett points out, if the controlling shareholder is an owner-manager, the board has virtually no functions:

In these situations . . . the directors cannot effect change except through persuasion. Therefore, if the owner/manager is mediocre or worse . . . there is little a director can do about it except object. If the directors having no connections to the owner/manager make a unified argument, it may well have some effect. More likely, it will not.²

¹ For these reasons, when a board does try its hand at managing, the results are unlikely to be felicitous. See, e.g., Susan Carey, TWA Insiders Say CEO's Departure Was No Surprise—Airline's Contentious Board Undermined Top Management, Critics Claim, WALL ST. J., Oct. 28, 1996, at B6.

Where a controlling owner is not an owner-manager, the board's role is only slightly larger. As Buffett goes on to say, if in such a case the outside directors "become unhappy with either the competence or integrity of the manager, they can go directly to the owner (who may also be on the board) and report their dissatisfaction. . . . [T]he dissatisfied director has only that single course of action."3

Of course, a board might manage the business of the corporation if it was entirely comprised of full-time managers and met regularly. In such a case, however, there would be no separate corporate organ consisting of a "board"; the board would be only a management committee with a fancy title.

Although the board cannot manage the corporation's business, it does have a significant role. Those who manage must be monitored to ensure that they are the right persons for their jobs, and that they are managing in the shareholders' interests. Because of the diffusion of shareholdings, the shareholders as a body are neither motivated nor able to engage in such monitoring. Large institutional shareholders operating on their own may monitor management, but under present conditions such monitoring is sporadic at best. Although a variety of other mechanisms can and do serve monitoring functions, they are all flawed, some deeply.

Because every monitoring mechanism is flawed, it is desirable to have overlapping mechanisms. The board is not itself flawless, but as an organ that is compact and cohesive, individualized to the corporation, and capable of being made relatively independent of management control, it is well situated to monitor management on an ongoing and close basis on the shareholders' behalf. To quote Buffett again, where a corporation "has no controlling shareholder . . . directors should behave as if there is a single absentee owner, whose long-term interest they should try to further in all proper ways."4

This modern view of the board's role, based partly on its comparative limitations as a managing organ and partly on its comparative advantages as a monitoring organ, has led to a new model of the board in which the selection and monitoring of managers is given pride of place. This model is embodied, for example, in the ALI's Principles of Corporate Governance,5 the ABA's Corporate

---

3 Id. at 41.

4 Id. at 39.

5 1 Principles of Corporate Governance: Analysis and Recommendations § 3.02 (1994) [hereinafter Principles of Corporate Governance].
Director's Guidebook,6 and the Business Roundtable's Corporate Governance and American Competitiveness.7

Thus, section 3.01 of the Principles of Corporate Governance provides that the management of the business of a publicly held corporation should be conducted by or under the supervision of the senior executives, subject to the functions and powers of the board. Under section 3.02, the leading board functions are to “[s]elect, regularly evaluate, fix the compensation of, and, where appropriate, replace the principal senior executives, . . . [and over-see] the conduct of the corporation’s business to evaluate whether the business is being properly managed.”

The monitoring model does not thrust a purely passive role onto the board. Although the most important functions of the board are to select, evaluate, and oversee the principal senior executive officers, the board also has important decisionmaking functions. For example, the Principles of Corporate Governance also provides that the board should review and, where appropriate, approve the corporation’s financial objectives, major corporate plans and actions, and major questions of choice with respect to “appropriate auditing and accounting principles and practices.”9

Now that the monitoring model of the board has been almost universally accepted, a new challenge has emerged: to flesh out the implications of that model and delineate exactly how the monitoring board should function. Several key structural elements of the monitoring model—including a board that has at least a majority of independent directors, and audit, nominating, and compensation committees—are already well-established. A number of additional structural refinements are now being tested. One is the concept of having either a nonexecutive chair or a lead outside director. This concept is adopted, for example, in General Motors Board of Directors Corporate Governance Guidelines.10

8 PRINCIPLES OF CORPORATE GOVERNANCE, supra note 5, § 3.02(a)(1)-(2).
9 Id. § 3.02(a)(3)-(4). As the comment adds, however, “while ultimate responsibility for approving major corporate plans and actions is vested in the board, and the board also has power to initiate their formulation, in practice these plans and actions will usually be initiated and formulated by the senior executives.” Id. § 3.02 cmt. f.
An even more important structural development is the treatment of the body of independent directors as a de facto corporate organ that is on the board, but not completely of it. For example, the GM Guidelines provide that the outside directors of the board will meet in executive session three times each year, and that decisions on matters of corporate governance presumptively will be made by those directors. Similarly, the Principles of Corporate Governance provides that independent directors "should be entitled, acting as a body, . . . to retain legal counsel, accountants, or other experts, at the corporation's expense, . . . if retention of an outside expert [is] required for the proper performance of the independent directors' functions and powers."

These developments, and others like them, concern board and committee structure. In contrast, I will develop in this Article a principle concerning the substantive role of the board. This principle is that the monitoring board must be responsible for the existence, integrity, and efficacy of the corporation's internal control. In developing this principle, I will discuss three related issues: the meaning of internal control (Part I); why the board should be responsible for internal control (Part II); and what board responsibility for internal control entails (Part III). Finally, I will discuss the legal framework of the board's responsibility for internal control (Part IV).

I. THE MEANING OF INTERNAL CONTROL

Until the mid-1940s, internal control was principally conceived as an incidental detail of audit practice: if an accounting function appeared to be under an adequate internal control, the auditor's investigation of the function could be limited to tests of whether the control was functioning as intended. In 1949, a special report issued by the American Institute of Certified Public Accountants' Committee on Auditing Procedure attached independent significance to the concept of internal control. The report defined inter-

---

11 Id. at 28.
12 Principles of Corporate Governance, supra note 5, § 3.04.
14 See Reports on Internal Control, supra note 13, at 892.
nal control to mean "the plan of organization and all of the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies."\footnote{Committee on Auditing Procedure, AIA, Internal Control—Elements Of a Coordinated System and Its Importance to Management and the Independent Public Accountant 5, 6 (1949).}

Even under this early definition, the scope of internal control included matters beyond accounting functions. The extended reach of internal control was elaborated in 1958 in \textit{Statement on Auditing Procedure No. 29},\footnote{Committee on Auditing Procedure, AICPA, Statement on Auditing Procedure No. 29, Scope of the Independent Auditor's Review of Internal Control 35 (1958).} in which the Committee on Auditing Procedure formally differentiated accounting control and administrative control. Accounting control related directly to the safeguarding of assets and the reliability of financial records. Examples included systems of transaction authorization and approval, physical controls over assets, and the plan of organization for separating duties concerned with record-keeping from duties concerned with operations or asset custody. Administrative control was mainly concerned with operational efficiency or adherence to managerial policies. Examples included statistical analyses, performance reports, training programs, and quality-control procedures.\footnote{See id. at 36-37.}

In \textit{Statement on Auditing Procedure No. 54}, issued in 1972,\footnote{Committee on Auditing Procedure, AICPA, Statement on Auditing Procedure No. 54, The Auditor's Study and Evaluation of Internal Control 231, 235 (1972) [hereinafter SAP No. 54]. The Statements on Auditing Procedure were later codified in Committee on Auditing Procedure, AICPA, Statement on Auditing Standards No. 1 (1973). With respect to internal control, SAS No. 1 was superseded by Auditing Standards Board, AICPA, Consideration of the Internal Control Structure in a Financial Statement Audit, Statement on Auditing Standards No. 55 at 1 (1988).} the concepts associated with internal control were further clarified, and redefined, in terms that are still in use. \textit{SAP No. 54} defined administrative control as the plan of organization, procedures, and records concerned with the decision processes leading to management's authorization of transactions. Accounting control was defined to require:

\begin{quote}
[A] plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability
\end{quote}
of financial records and consequently are designed to provide reasonable assurance that:

a. Transactions are executed in accordance with management's general or specific authorization.

b. Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles . . . and (2) to maintain accountability for assets.

c. Access to assets is permitted only in accordance with management's authorization.

d. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.19

In 1977, the Foreign Corrupt Practices Act ("FCPA") codified the accounting control provisions of SAP No. 54 virtually word-for-word, and thereby transformed accounting control into a requirement of federal law for corporations whose stock is registered under the Securities Exchange Act.20

Since the adoption of the FCPA, much of the emphasis in developing the concept of internal control has been on non-accounting control. In 1978, for example, the Institute of Internal Auditors set the following objectives for internal control:

1. The reliability and integrity of information

---

19 SAP No. 54, supra note 18, at 239-40.

20 The FCPA provides, in pertinent part:

(2) Every issuer which has a class of securities registered pursuant to section 78l of this title and every issuer which is required to file reports pursuant to section 78o(d) of this title shall—

(A) make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer; and

(B) devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—

(i) transactions are executed in accordance with management's general or specific authorization;

(ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets;

(iii) access to assets is permitted only in accordance with management's general or specific authorization; and

(iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

2. Compliance with policies, plans, procedures, laws, and regulations
3. The safeguarding of assets
4. The economical and efficient use of resources
5. The accomplishment of established objectives and goals for operations or programs.\textsuperscript{21}

These objectives are still adhered to.\textsuperscript{22}

The Treadway Report on fraudulent financial reporting, issued in 1987,\textsuperscript{23} also emphasized internal control,\textsuperscript{24} and pointed out that the system of internal control is a broader concept than the FCPA's internal accounting control.\textsuperscript{25} Given its objectives, the Treadway Report emphasized internal control as a mechanism to prevent fraudulent reporting. Subsequently, however, a committee consisting of five accounting organizations that had sponsored the Treadway Report, known as the Committee of Sponsoring Organizations, or COSO, undertook an extensive study of internal control that went beyond the Treadway objective. In 1992, COSO issued a comprehensive four-volume report on internal control entitled \textit{Internal Control: Integrated Framework}, which was designed to provide a broad framework through which business entities could assess the effectiveness of their internal control, including, but not confined to, accounting control.\textsuperscript{26}

The \textit{COSO Report} defines internal control as "a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in three categories: “effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.”\textsuperscript{27} Internal control over each of these objectives consists of five interrelated components: the control environment, risk assessment, control activities, information and communication, and monitoring. A system of internal control is deemed to be effective only if all five components are functioning effectively. The \textit{COSO Report} also sets out, in de-

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{21} Institute of Internal Auditors, \textit{Standards for the Professional Practice of Internal Auditing} 24 (1978) [hereinafter \textit{Standards of Internal Auditing}].
\item \textsuperscript{22} See id. at 34-38.
\item \textsuperscript{24} See id. at 33-34.
\item \textsuperscript{25} See id. at 34.
\item \textsuperscript{26} Committee of Sponsoring Organizations of the Treadway Commission, AICPA, \textit{Internal Control-Integrated Framework} (1992) [hereinafter COSO Report].
\item \textsuperscript{27} Id. at 9.
\end{itemize}
\end{footnotesize}
tail, specific controls through which internal control should be implemented. In 1995, the central principles of the COSO Report were codified by the AICPA’s Auditing Standards Board in Statement on Auditing Standards No. 78.

The COSO Report provides the definitive treatment of internal control to date. In 1994, the ABA’s Committee on Law and Accounting reported that “[t]he COSO Report may well become the standard for defining internal control and its interrelated components, and for measuring the effectiveness of internal control. The Report has serious implications for all entities and their managements and for their outside financial, accounting, legal, and other advisors as well.” Similarly, in SAS No. 78 the AICPA’s Auditing Standards Board expressed its view that “the COSO Report is rapidly becoming a widely accepted framework for sound internal control among United States organizations and its acceptance and use will continue to grow.”

Following the usage of SAS No. 78, in the balance of this Article, I will use the terms “internal control” and “internal control structure” interchangeably. In contrast, I will use the terms “control” and “controls” to mean one or more specific controls adopted as part of an internal control structure.

II. Why the Board Should Be Responsible for Internal Control

The need for internal control is currently not a matter of dispute. A more significant question is where ultimate responsibility for internal control should be vested. There are two reasons why this responsibility should be vested in the board.

The first reason is based on the problem of asymmetric information. The general problem of asymmetric information within a hierarchal organization is well described by Milgrom and Roberts:

We take it as given that some of the information that is important for the organization to make good decisions is not directly available to those charged with making the decisions. Instead, it is lodged with or producible only by other individuals or groups.
that are not empowered to make the decisions but may have a direct interest in the resulting outcomes. Examples of such information are many.

In such situations, the members of the organization may have an incentive to try to manipulate the information they develop and provide in order to influence decisions to their benefits. Such manipulation can take many forms, ranging from conscious lies concerning facts, through suppression of unfavorable information, to simply presenting the information in a way that accentuates the points supporting the interested party's preferred decision and then insisting on these points at every opportunity.

This influence activity can be costly to the organization in a number of ways. First, to the extent it is successful in biasing the decision maker's information, it may lead to decisions being taken that are inefficient from the organization's point of view.

In many situations the decision makers may strongly suspect that individuals or groups are attempting to manipulate their decisions by distorting the information they produce and provide. Yet, it may be impossible to be sure that this is going on or to undo the distortion so as to "ignore" the attempt at influence.

Milgrom and Roberts stress that informational asymmetry may be exploited to benefit the more knowledgeable actor. The term "benefit" is ambiguous. In publicly held corporations, at least, the concern is not that managers will attempt to exploit informational asymmetry to benefit themselves by lining their own pockets at the corporation's expense. Instead, the concerns are that managers will attempt to exploit informational asymmetry to ensure that the board will take actions the managers believe are best for the corporation, and, of greater significance, will view the managers' performance in a positive way so as to facilitate the managers' retention and promotion. The two concerns often come together, because there are few, if any, managers who don't believe that their own retention and promotion is exactly what is best for the corporation.

Accordingly, to exercise both its monitoring and decisionmaking functions, the board must have reliable information. There is a

---

serious asymmetry, however, between the information available to the executives who are being monitored by the board and are proposing decisions, on the one hand, and the board, which is monitoring the executives and making these decisions, on the other. The executives, normally have at their disposal all information that relates to their own performance and to the decisions they propose. For example, as Milgrom and Roberts point out, "[t]he directors of a firm may have the final say on whether a new plant will be built, but only the division whose products will be made in the plant can generate important parts of the relevant information on the likely profitability of the new facility."\(^{34}\) Because evaluations and decisions are shaped by the information available to the decisionmaker, if the executives control the information the board receives, the board's monitoring and decisionmaking functions often will be little more than nominal.

One strategy a decisionmaker may utilize to deal with the problem of asymmetric information is to adopt a skeptical posture.\(^{35}\) This strategy is usually effective only when the person who supplies the relevant information has a known monotonic agenda, such as maximizing sales to the decisionmaker, so that the information he supplies can always be evaluated in terms of that agenda.\(^{36}\) Much or most of the information supplied to the board by executives will not fit into that category.

A second strategy is to create competitive sources of information.\(^{37}\) This strategy is feasible in the corporate context, and an internal control structure can serve such a strategy. Viewed from the perspective of asymmetric information, an internal control structure furthers two related objectives. First, such a structure helps to ensure the reliability of the flow of information from the executives to the board by correcting distorted information before it reaches the board, and by deterring executives from creating such distortions in the first place. Second, such a structure creates a competitive source of information in the person of those who administer the controls. To further these two objectives, however, ultimate responsibility for the internal control structure must be vested in the board, because vesting ultimate responsibility for the structure in the executives would defeat the very purpose of using

\(^{34}\) Milgrom & Roberts, *Economic Approach*, supra note 33, at S156.


\(^{36}\) See id.

\(^{37}\) See id. at 19-20, 24-25, 31.
an internal control structure to correct the asymmetric-information problem.

The second reason for vesting ultimate responsibility for an internal control structure in the board concerns managerial opportunism. Managers often have short tenures at any given position and are typically under great pressure to produce short-term results if they are to be retained and promoted. Managerial compensation may also be linked to short-term results. Accordingly, it is often in a manager's interest to opportunistically maximize reported profits during his tenure, even if doing so involves taking actions of a kind that are either prohibited by corporate policies—because, as a class, the actions tend to decrease long-term profitability or threaten other vital corporate interests—or are prohibited by law. Furthermore, the anticipated profit to be made on a transaction that would violate a corporate policy or a legal rule is typically large, present, and vivid. In contrast, from a manager's perspective the possible loss from violating a corporate policy or legal rule will often seem insignificant, pallid, and very remote, especially when discounted for the probability of detection.

Moreover, managers, by the nature of their calling, may regard profitmaking as a gratification, and may view corporate policies and legal rules that stand in the way of profitmaking as costs, rather than as prohibitions. Correspondingly, managers may view internal controls intended to ensure compliance with corporate policies and legal rules as unwelcome and foreign constraints. Managers may therefore believe that such controls can be appropriately disregarded in favor of concrete opportunities that offer significant net profits if the uncertain cost of the violation of policy or law is put to one side.

Of course, reputational effects may limit opportunistic tendencies. These effects, however, often have only limited impact in this context. Managers typically operate as part of teams, and it is often difficult to fix blame on an individual member of a team. Furthermore, higher-ranking managers are often expert at deflecting blame to lower-ranking managers. Managers also know that they often will have either retired or moved on to another business unit within the corporation before a problem comes home to roost.

An analogy can be drawn here to the world of university athletics. Coaches, like corporate managers, are under intense external and internal pressure to produce short-term results. To achieve that end, coaches often are tempted to violate NCAA recruitment policies, which their university is committed to follow, even though
the violations, if discovered, will have drastic negative long-term effects on the university’s athletic program. Many coaches succumb to this temptation. An opportunity to recruit an outstanding athlete is present, vivid, and salient. The NCAA recruitment policies are unwelcome and foreign, and the costs of a violation are pallid and remote, especially when discounted by the risk of detection. Furthermore, the costs often will not fall on the coach: The coach can often deflect blame onto alumni boosters, assistant coaches, or both, and, in any event, NCAA penalties often fall much more heavily on the university than on the coach. The result is that coaches are highly motivated to opportunistically recruit outstanding athletes in violation of NCAA rules, often to the long-term detriment of the university. As with coaches, so with managers.

The proof of the pudding is in the eating. Examples of managerial disregard of corporate policies or legal rules to record short-term profits are numerous. Among the most recent are the Archer Daniels Midland debacle, involving price-fixing, that resulted in a $100 million fine, $90 million in damages, and the departure of two top executives, including the president’s son;\(^{38}\) the Sumitomo debacle, involving a loss of $1.8 billion from copper trading that Sumitomo claims was unauthorized, but which many believe was known to Sumitomo officials;\(^{39}\) and the Prudential scandal, involving damages against Prudential in excess of $400 million, and possibly as much as $1 billion, for abusive sales practices.\(^{40}\) At the core of the Prudential scandal was a sales practice known as churning, in which Prudential agents used misrepresentation, nondisclosure, trickery, and forgery to get policyholders whose policies had large built-up cash values to exchange their policies for larger policies. Prudential’s internal auditors began reporting serious problems to senior managers as early as 1982, and continued reporting serious problems into the 1990s. According to a 1994 report by Coopers & Lybrand, however, Prudential senior managers failed to pay appropriate attention to the issues raised in the internal audit reports.


Indeed, even after the Coopers & Lybrand report, some Prudential executives took the position that there was no widespread problem. 41

Two particularly dramatic examples of managerial overriding of corporate policies or internal controls, both involving banks, have recently surfaced. The first concerned Citibank, which engaged in extensive banking activities on behalf of Raul Salinas, the brother of the former president of Mexico. Raul Salinas was a Mexican government employee. His maximum annual salary was $190,000, yet he banked $80 million with Citibank, whose officers apparently found this no cause for concern. In 1996, the Wall Street Journal reported—not surprisingly, given the figures—that Citibank executives, in their dealings with Salinas, had failed to follow procedures widely used by other banks to reduce the risk of money laundering. 42 The Journal also reported that when senior Citibank officials finally launched an internal investigation of the Salinas problem, they blocked Citibank’s top money-laundering compliance officer from participating in the investigation, and even from asking questions, although the compliance officer was regarded as one of the best in-house compliance persons at any United States bank. 43 The Justice Department is now investigating whether Citicorp violated federal money-laundering laws in its dealings with Raul Salinas. 44

Also in 1996, the New York Times reported a drastic failure of internal control at Bankers Trust, due to the actions of senior managers. A number of Bankers Trust clients had experienced large losses from dealings with Bankers Trust in derivatives, and some had charged Bankers Trust with improprieties. According to an investigation by independent counsel, ordered by regulatory agencies:

Bankers Trust’s “derivatives business was not well managed or controlled in certain important respects and certain individuals at B.T. . . . exploited these weaknesses for their own purposes,”

---

Government investigations and civil suits uncovered instances in which Bankers Trust employees misled their clients about the risk of derivatives deals. In recorded conversations disclosed in civil trials, salesmen boasted how little their clients understood about the risks they were taking and how much money the salesmen were making as a result.

Moreover, attempts by the bank's internal control departments to enforce appropriate standards—such as determining if a transaction was suitable for a customer—were suppressed by Bankers Trust's senior management.

The report criticized the bank's internal controls, noting that existing policies were not strictly enforced. In some cases, attempts by officials involved in internal control to look more closely at derivatives deals were rebuffed.

"When the credit department sought an expanded role in 'appropriateness-suitability' decisions, this effort was successfully resisted by marketers with the support of senior management," the report said.

As these examples show, the use of internal control to limit managerial opportunism, like the use of such control to provide the board with a competitive source of information, would be subverted if ultimate responsibility for internal control was vested in the managers. Accordingly, the problem of managerial opportunism provides a second reason why ultimate responsibility for internal control needs to be vested in the board. In contrast to managers, directors are not angling for promotion, are normally not judged on the basis of short-term profits, do not have much to lose if they are not renewed, and are charged with the welfare of the entire corporation, rather than with the welfare of a single unit in the corporation.

III. WHAT BOARD RESPONSIBILITY FOR INTERNAL CONTROL ENTAILS

The next question is, how should the board execute its responsibility for internal control? It is especially important to distinguish internal control from specific controls. Certainly, the board cannot be expected to design or administer specific controls. Design of specific controls would be beyond the board's competence, and administration of specific controls would be beyond both the board's competence and its resources. The board does, however, have an

---

important role to play in the design and administration of the internal control structure.

A. Design

In the area of design, the board's role is to use due care to assure itself that an internal control structure is in existence, is appropriate, and is effective. The board's responsibility in these matters is not to ensure that specific controls never fail. Accordingly, a breakdown in a specific control does not in itself establish that the board has not discharged its responsibility. Furthermore, the board need not ensure that every conceivable control is in place. In determining whether any given control should be installed, and the extent and contours of a control, the risk of failure if the control is not in place must be balanced with the control's costs.\footnote{See COSO REPORT, supra note 26, at 77; Reports on Internal Control, supra note 13, at 912-13.}

The board should, however, be responsible for using due care to assure itself that the five components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring—are in place in such a way as to provide reasonable assurance regarding the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with corporate policies and legal rules.\footnote{See COSO REPORT, supra note 26, at 12-14.}

To this end, the board should be especially concerned with overseeing the design and integrity of appropriate systems for producing reliable financial and operational information, and for assessing the likelihood or frequency of significant risks and considering how such risks should be managed.

The board should also be especially concerned to assure that appropriate compliance programs are in place. These programs should include the creation and distribution of substantive codes of conduct based on corporate policies and legal rules, procedures for ensuring that the substantive rules are complied with, and methods for effectively disseminating the programs. The board should monitor the remedial actions taken in response to departures from compliance programs and, more generally, the remedial actions taken in response to violations of established corporate policies and legal rules, whether or not embodied in corporate codes of conduct. In addition, the board should regulate management interventions to override compliance programs, either by prohibiting...
such interventions without board approval, or by requiring documentation and reports to the board if such interventions occur.

Also of special importance is the design and integrity of protocols for reporting on deficiencies and reportable conditions in internal control. A deficiency is a condition in the internal control structure that is "worthy of attention." A deficiency "may represent a perceived, potential, or real shortcoming, or an opportunity to strengthen the internal control system to provide a greater likelihood that the entity's objectives will be achieved." A reportable condition is a "significant deficiency in the design or operation of the internal control structure, which could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements." The board should assure itself that protocols are in place for reporting deficiencies to appropriate persons and for reporting reportable conditions to both senior executives and the board.

Finally, the board should assure itself that periodic evaluations of internal control are conducted. This responsibility includes determining that appropriate portions of the internal control structure are reevaluated by personnel with the requisite skills, that the reevaluations have adequate scope and depth of coverage and are conducted with adequate frequency, and that the methodology for evaluating internal control is logical and appropriate.

B. Administration

In addition to being responsible for assuring itself that the design of the internal control structure is appropriate and effective, the board is responsible for assuring itself of the proper administration of internal control. The most significant instrument for executing this responsibility, at least in large publicly held corporations, is an internal auditing function, consisting of a senior internal auditing executive, an internal auditing staff, and in some cases, outsourcing. The important and influential Treadway Report recommended an internal auditing function for all such corporations. A 1993 study by Curtis C. Verschoor, based on the

48 Id. at 70.
49 Id.
50 Id. at 72; see also Auditing Standards Board, AICPA, Statement on Auditing Standards No. 60, Communication of Internal Control Structure Related Matters Noted in an Audit (1988).
51 Treadway Report, supra note 23, at 37.
management reports that were included in the 1992 annual reports of very large publicly held corporations, found that most of the surveyed corporations made such reports, and 95% of corporations that made such reports referred to an internal auditing function.\textsuperscript{52} Similarly, the \textit{Corporate Director's Guidebook} reports that most large publicly held corporations have an internal audit department.\textsuperscript{53}

At one time, internal auditing was analogous to external auditing, and consisted primarily of financial auditing and attesting to the accuracy and completeness of financial statements. Today, internal auditors also evaluate controls, check compliance with policies and procedures, and test reporting systems in non-financial areas of corporate operations. In effect, as the principle of internal control has evolved, the internal auditing function has evolved in a parallel way. Under best practice, the responsibility of the internal auditor parallels the board's responsibility for internal control. For example, the Institute of Internal Auditors' \textit{Standards for the Professional Practice of Internal Auditing} states that internal auditors should:

\begin{itemize}
  \item Review the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.
  \item Review the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on operations and reports, and should determine whether the organization is in compliance.
  \item Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
  \item Appraise the economy and efficiency with which resources are employed.
  \item Review operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.\textsuperscript{54}
\end{itemize}

Therefore, where an internal auditing function is in place, it provides the board with an organ that can administer internal control on the board's behalf. To this end, the board of a publicly held corporation should implement the recommendations of the Treadway Report by maintaining an effective internal auditing function.


\textsuperscript{53} \textit{Corporate Director's Guidebook}, supra note 6, at 1266.

\textsuperscript{54} \textit{Standards of Internal Auditing}, supra note 21, at 95-96 (Statement of Responsibilities of Internal Auditors); see also id. at 34-36.
Accordingly, the board should assure itself that the charter of the internal auditing function is as broad as that specified by the Institute of Internal Auditors and that the internal auditing function has adequate resources to carry out its charter. In addition, the board should require the senior internal auditing executive to report to the board, or to the audit committee, as well as to an executive. The audit committee, in turn, following the recommendations of Principles of Corporate Governance section 3A.02, should: (1) Review the appointment and replacement of the senior internal auditing executive, to enhance the objectivity of the internal auditing function. (2) Serve as a channel of communication between that executive and the board, to reenforce the objectivity of internal auditing and to help ensure that significant internal control issues will reach the board's attention. (3) Review all material internal audit reports with the internal auditors, outside the presence of management. And (4) Meet periodically with the senior internal auditing executive outside the presence of management; encourage that executive to raise potentially troublesome problems at a relatively early stage and to broach sensitive problems in an uninhibited and private fashion; and give that executive assurance of an objective hearing in the event of a disagreement with management.55

Even in publicly held corporations that do not have an internal auditing function, the corporation's outside independent accountant has a limited, but crucial and mandatory role in internal control under section 10A of the Securities Exchange Act,56 adopted as part of the Private Securities Litigation Reform Act of 1995.

Under section 10A(a), the independent public accountant is required to include in each audit two special procedures: First, procedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material effect on the determination of financial statement amounts; second, procedures designed to identify related-party transactions that are material to the financial statements, or otherwise require disclosure therein.

Under section 10A(b), if, in the course of conducting an audit pursuant to the statute, an independent public accountant detects or otherwise becomes aware of information indicating that an illegal act has or may have occurred—even an act that would not have

55 See Principles of Corporate Governance, supra note 5, § 3A.02.
a material effect on the financial statements—the accountant is required to determine whether it is likely that an illegal act has occurred. If so, the accountant must assure that the board or the audit committee is adequately informed with respect to the act, unless the act is clearly inconsequential. If the accountant thereafter determines that senior management has not taken timely and appropriate remedial action with respect to the illegal act, and certain other conditions are met, the accountant is required to report that conclusion to the board.

IV. THE LEGAL FRAMEWORK

The principle that the board should be responsible for internal control is primarily based on considerations of efficiency. However, this principle is also supported by a legal framework. One element of this framework, already considered, is the Foreign Corrupt Practices Act. Other elements include the Federal Criminal Sentencing Guidelines, official pronouncements concerning risk management, and the duty of care.

A. The Sentencing Guidelines

A corporation can be found guilty of a crime by imputing to the corporation the acts and intent of agents who acted within the scope of their authority. The imposition of corporate criminal liability has become increasingly common.

Under federal law, a corporation that is found guilty of a federal crime may be sentenced to a fine within a range determined under the Federal Sentencing Guidelines. Under the Sentencing Guidelines, the base fine that would otherwise be payable is dramatically reduced if the corporation had an effective compliance program in place prior to the crime. For example, if a corporation has such a program in place, cooperates with the government investigation, and accepts responsibility for its criminal conduct, the corporation may be required to pay as little as 5% of its base fine.

57 See supra note 20 and accompanying text.
62 See id.; see also Dan K. Webb et al., Understanding and Avoiding Corporate and Executive Criminal Liability, 49 BUS. LAW. 617, 644-63 (1993).
Accordingly, the Sentencing Guidelines provide a corporation with enormous incentives to have an effective compliance program. The Guidelines provide that to constitute an effective program, a compliance program must be reasonably designed, implemented, and enforced. At a minimum, the corporation must take the following steps: (1) establish standards and procedures, reasonably capable of reducing the prospect of criminal conduct, to be followed by employees and other agents of the corporation; (2) assign to specific high-level individuals overall responsibility to oversee compliance with the standards and procedures; (3) exercise due care not to delegate substantial discretionary authority to those individuals whom the corporation knows or should know have a propensity to engage in illegal activities; (4) effectively communicate corporate standards and procedures to all employees and other agents through training programs or dissemination of written information; (5) attempt to achieve compliance by the use of monitoring and auditing systems to detect criminal conduct of employees and agents, and by having in place and publicizing a reporting system whereby employees and agents can report criminal conduct by others within the organization without fear of retribution; (6) enforce standards to achieve compliance through appropriate disciplinary mechanisms; and (7) respond appropriately if an offense is detected, and take steps to prevent additional similar offenses.

Although the Sentencing Guidelines do not explicitly require the board to be responsible for compliance programs, it is widely understood that the board has that responsibility. For example, the Corporate Director’s Guidebook states that a director should be particularly concerned that the corporation has established and implemented law-compliance programs.

B. Risk Management

A second element of the legal framework concerning the board’s responsibility for internal control concerns risk management. The SEC and the Federal Reserve Bank have both weighed in on this issue. In In the Matter of Gibson Greetings, Inc., Gibson got in over its head in trading derivatives, took substantial

---

63 U.S.S.G., supra note 61, § 8A1.2 cmt. 3(k).
65 Corporate Director’s Guidebook, supra note 6, at 1250-51.
losses, and failed to report them properly. In an order against Gibson and two of its executives, the SEC stated:

Gibson . . . lacked adequate . . . controls for ascertaining whether derivatives transactions were consistent with corporate derivatives objectives established by Gibson's Board of Directors. The board had approved a resolution on April 15, 1992 authorizing the Vice President, Finance or his designee to "take such actions as he may deem appropriate from time to time to effectuate interest rate swap transactions relating to the Corporation's obligations on such terms as he may approve." This resolution did not authorize transactions beyond interest rate swap transactions relating to the corporation's debt. No specific procedures were put in place to implement that resolution, such as procedures to place limits on the amounts, types or nature of derivatives transactions, or to assess the risks of derivatives transactions.67

Dennis Dumas, senior counsel at the Bank of New York, has commented on the order in Gibson as follows:

In the discussion, the commission . . . raises three possible duties:

1. a board duty to enunciate risk objectives;
2. a duty to establish internal control and procedures to determine compliance with board-enunciated objectives; and
3. a duty to implement the internal controls and procedures.

The commission appears to endorse board enunciation of objectives (Duty 1) through its criticism of the failure to establish and implement controls and procedures to determine compliance with these objectives. Moreover, the commission plainly states that the chief financial officer and treasurer were responsible for implementing internal controls and procedures to determine compliance with the board's stated objectives (Duty 3).

Nevertheless, the commission remains silent on who was responsible for establishing internal controls and procedures to determine compliance with board-enunciated objectives (Duty 2). This omission, in light of the SEC statement that the chief financial officer and treasurer were responsible for Duty 3, appears to indicate that the commission may believe that board members have some personal responsibility for Duty 2.68

---

67 Id. at 1406.
Similarly, the Federal Reserve Board’s *Bank Holding Company Supervision Manual* provides that the board of a banking organization “should approve all significant policies relating to the management of risks throughout the organization . . . [and] should be informed regularly of risk exposure and should regularly re-evaluate significant risk-management policies and procedures,”69 and that lines of authority should include an independent system for reporting exposures to the board.

The Federal Reserve guidelines for rating risk-management in banking organizations, issued in 1995, go into more detail:

Boards of directors have ultimate responsibility for the level of risk taken by their institutions. Accordingly, they should approve the overall business strategies and significant policies of their organizations, including those related to managing and taking risks, and should also ensure that senior management is fully capable of managing the activities that their institutions conduct. While all boards of directors are responsible for understanding the nature of the risks significant to their organizations and for ensuring that management is taking the steps necessary to identify, measure, monitor, and control these risks, the level of technical knowledge required of directors may vary depending on the particular circumstances at the institution.

Directors of large banking organizations that conduct a broad range of technically complex activities, for example, cannot be expected to understand the full details of their institutions’ activities or the precise ways risks are measured and controlled. They should, however, have a clear understanding of the types of risks to which their institutions are exposed and should receive reports that identify the size and significance of the risks in terms that are meaningful to them. In fulfilling this responsibility, directors should take steps to develop an appropriate understanding of the risks their institutions face, possibly through briefing from auditors and experts external to the organization. Using this knowledge and information, directors should provide clear guidance regarding the level of exposures acceptable to their institutions and have the responsibility to ensure that senior management implements and procedures and controls necessary to comply with adopted policies. . . .

In assessing the quality of the oversight by boards of directors and senior management, examiners should consider

---

69 *Board of Governors, Federal Reserve Board, Bank Holding Company Supervision Manual* § 2125.0 (1997).
whether the institution follows policies and practices such as those described below:

* The board and senior management have identified and have a clear understanding and working knowledge of the types of risks inherent in the institution’s activities and make appropriate efforts to remain informed about these risks as financial markets, risk management practices, and the institution’s activities evolve.

* The board has reviewed and approved appropriate policies to limit risks inherent in the institution’s lending, investing, trading, trust, fiduciary and other significant activities or products.

* The board and management are sufficiently familiar with and are using adequate record keeping and reporting systems to measure and monitor the major sources of risk to the organization.

* The board periodically reviews and approves risk exposure limits to conform with any changes in the institution’s strategies, addresses new products, and reacts to changes in market conditions.  

Although the SEC and Federal Reserve materials concern financial instruments or institutions, the concepts embodied in those materials can easily be extended, by analogy, to risk-management in general.

C. The Duty of Care

A third element of the legal framework arises out of the director’s duty of care. The duty to monitor has now become a well-established element of the general duty of care. An internal control structure is necessary to properly implement that duty. For example, the Corporate Director’s Guidebook states:

A significant aspect of the board’s responsibility, often referred to the Audit Committee, is oversight of the corporation’s policies and procedures regarding compliance with law and significant corporate policies. Most large, publicly owned corporations have adopted codes of conduct expressing principles of business ethics, legal compliance, and other matters relating to business conduct. Subjects commonly addressed by such codes are legal compliance (antitrust laws and policies, Foreign Cor-

---

70 Division of Banking Supervision and Regulations, Federal Reserve System SR 95-51 (SUP), Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies 3-5 (1995).
rupt Practices Act of 1977, and insider trading, to name a few), conflicts of interest, corporate opportunities, gifts from business associates, misuse of confidential information, and political contributions. The board of directors should be concerned that the corporation have such a code of conduct, that the code is widely circulated to appropriate employees, that adherence to the code is enforced, that the corporation maintain procedures for monitoring and enforcing compliance, and that the support of the CEO and the board is clearly evidenced.71

Similarly, the Comment to Principles of Corporate Governance section 4.01 states: "Today, an ordinarily prudent person serving as the director of a corporation of any significant scale or complexity should recognize the need to be reasonably concerned with the existence and effectiveness of procedures, programs, and other techniques to assist the board in its oversight role."72

In short, the modern authorities point in the direction of requiring active monitoring as a component of a director's due care. Active monitoring, in turn, requires the installation of an internal-control structure that is appropriate for the particular corporation.

The well known case of Graham v. Allis-Chalmers Manufacturing Co.,73 decided by the Delaware Supreme Court in 1963, may seem to point in a different direction. Allis-Chalmers and four of its employees had pled guilty to indictments based on price-fixing and other violations of federal antitrust laws. A derivative action was brought against Allis-Chalmers directors and the four employees for damages to Allis-Chalmers resulting from the conduct that was the subject of the indictments. The plaintiff claimed that the directors were liable under various theories, one of which was that the board should have taken action to learn about and prevent antitrust violations. In holding for the directors, the Delaware court said:

[It] appears that directors are entitled to rely on the honesty and integrity of their subordinates until something occurs to put them on suspicion that something is wrong. If such occurs and goes unheeded, then liability of the directors might well follow, but absent cause for suspicion there is no duty upon the directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists.

71 Corporate Director's Guidebook, supra note 6, at 1267.
72 Principles of Corporate Governance, supra note 5, § 4.01(a)(1)-(2) cmt. c.
73 188 A.2d 125 (Del. 1963).
The duties of the Allis-Chalmers Directors were fixed by the nature of the enterprise which employed in excess of 30,000 persons, and extended over a large geographical area. By force of necessity, the company's Directors could not know personally all the company's employees. The very magnitude of the enterprise required them to confine their control to the broad policy decisions. That they did this is clear from the record. At the meetings of the Board in which all Directors participated, these questions were considered and decided on the basis of summaries, reports and corporate records.74

Allis-Chalmers, although perhaps correctly decided on its facts, envisions a passive role for the board that may have been acceptable in 1963, before the evolution of the monitoring model, but is inconsistent with the modern view of the board's monitoring obligation. As stated by Norman Veasey and William Manning:

[A] comparison of the results of Graham and . . . [the monitoring position reflected in the Business Roundtable Statement] exposes not a philosophical difference between Delaware courts and the Business Roundtable; rather, it shows a natural development in the role of an "ordinarily prudent director" since 1963, the year in which Graham was decided.75

The most comprehensive and authoritative statement on the current status of Graham v. Allis-Chalmers is In re Caremark International,76 decided in 1996 by Chancellor Allen. Caremark conducted a patient-care and a managed-care business. The patient-care business included alternative-site services, and the managed-care business included prescription drug programs and the operation of multi-specialty group practices. A substantial part of Caremark's revenue was derived from third-party payment programs, including Medicare and Medicaid. These payments were subject to the Anti-Referral Payments Law ("ARPL"), which prohibited health-care providers from paying any form of remuneration to induce the referral of Medicare or Medicaid patients.

From its inception, Caremark entered into a variety of agreements with health-care providers, including consultation agreements with, and research grants to, physicians. At least some of these physicians prescribed or recommended Caremark services or

74 Id. at 130.
75 Norman Veasey & William Manning, Codified Standard: Safe Harbor or Uncharted Reef? An Analysis of the Model Act Standard of Care Compared with Delaware Law, 35 Bus. Law. 919, 930 (1979); see also Principles of Corporate Governance, supra note 5, § 4.01(a)(1)-(2) cmt. c: "The Allis-Chalmers case was decided 30 years ago . . . [T]he 'obligation' component of duty of care provisions is a flexible and dynamic concept."
products to Medicare recipients and other patients. Based on these agreements and grants, Caremark was indicted for violating ARPL. Caremark pleaded guilty to mail fraud and agreed to pay civil and criminal fines. Subsequently, it also reimbursed various private and public parties. In all, Caremark was required to make payments of approximately $250 million.

Derivative actions based on these payments were brought against the directors, and settled. The issue in Caremark was whether the settlements should be judicially approved. That issue, in turn, depended in part on the applicable legal principles, which led Chancellor Allen into an extended consideration of the status of *Graham v. Allis-Chalmers*, and, more broadly, the duty of the board in connection with the installation of monitoring systems. Chancellor Allen’s important opinion is worth quoting at length:

> [The shareholders argued that the directors breached their duty of care by reason of their failure to implement a system of watchfulness which would have brought the misconduct to their attention in ample time to have brought it to an end.]

> As the facts of this case graphically demonstrate, ordinary business decisions that are made by officers and employees deeper in the interior of the organization can... vitally affect the welfare of the corporation and its ability to achieve its various strategic and financial goals. If this case did not prove the point itself, recent business history would. Recall for example the displacement of senior management and much of the board of Salomon, Inc.; the replacement of senior management of Kidder, Peabody following the discovery of large trading losses resulting from phantom trades by a highly compensated trader; or the extensive financial loss and reputational injury suffered by Prudential Insurance as a result of its junior officers’ misrepresentations in connection with the distribution of limited partnership interests. Financial and organizational disasters such as these raise the question, what is the board’s responsibility with respect to the organization and monitoring of the enterprise to assure that the corporation functions within the law to achieve its purposes?...

> ... [In *Graham v. Allis-Chalmers*, the Court said in] notably colorful terms, ... that absent cause for suspicion there is no duty upon the directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists. The Court found that there were no grounds for suspicion in that case and, thus, concluded that the
directors were blamelessly unaware of the conduct leading to the corporate liability.

How does one generalize this holding today? Can it be said today that, absent some ground giving rise to suspicion of violation of law, . . . corporate directors have no duty to assure that a corporate information gathering and reporting system exists which represents a good faith attempt to provide senior management and the Board with information respecting material acts, events or conditions within the corporation, including compliance with applicable statutes and regulations? I certainly do not believe so. I doubt that such a broad generalization of the Graham holding would have been accepted by the Supreme Court in 1963. The case can be more narrowly interpreted as standing for the proposition that, absent grounds to suspect deception, neither corporate boards nor senior officers can be charged with wrongdoing simply for assuming the integrity of employees and the honesty of their dealings on the company's behalf.

A broader interpretation of Graham v. Allis Chalmers—that it means that a corporate board has no responsibility to assure that appropriate information and reporting systems are established by management—would not, in any event, be accepted by the Delaware Supreme Court in 1996, in my opinion. In stating the basis for this view, I start with the recognition that in recent years the Delaware Supreme Court has made . . . clear . . . the seriousness with which . . . corporation law views the role of the corporate board. Secondly, I note the elementary fact that relevant and timely information is an essential predicate for satisfaction of the board's supervisory and monitoring role under Section 141 of the Delaware General Corporation Law. Thirdly, I note the potential impact of the federal organizational sentencing guidelines on any business organization. Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account this development and the enhanced penalties and the opportunities for reduced sanctions that it offers.

In light of these developments, it would, in my opinion, be a mistake to conclude that our Supreme Court's statement in Graham concerning "espionage" means that corporate boards may satisfy their obligation to be reasonably informed concerning the corporation, without assuring themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance. . . .
Thus, I am of the view that a director’s obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.\footnote{Id. at 968-70 (internal quotations, citations, and footnotes omitted). Chancellor Allen concluded that the Caremark board had satisfied its monitoring obligation. Inside and outside counsel had advised Caremark’s directors that Caremark’s contracts complied with the law. Caremark had an internal audit plan designed to assure compliance with business and ethics policies. A report by Price Waterhouse, Caremark’s outside auditor, concluded that there were no material weaknesses in Caremark’s control structure. Caremark’s Audit & Ethics Committee adopted a new internal-audit charter which required a comprehensive review of compliance policies and the compilation of an employee ethics handbook concerning such policies. The board had also instituted a policy that required Caremark’s regional officers to approve every contractual relationship entered into with a physician, and had received information from management pertaining to the company’s law-compliance efforts.}

**Conclusion**

To make the board’s monitoring and decisionmaking functions meaningful in publicly held corporations, the board must be vested with ultimate responsibility for internal control. Assigning this responsibility to the board does not require the creation of new corporate institutions; in many, and perhaps most, publicly held corporations, most or all of the elements necessary to carry out that responsibility are already in place. Instead, what is principally required is that responsibility for internal control be made explicit, that the meaning of this responsibility be specified, and that a proper linkage be created between the board and the internal auditing function.