2004

The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism, Other Ills

Lawrence A. Cunningham
George Washington University Law School, lacunningham@law.gwu.edu

[29 J. CORP. L. (forthcoming 2004)] [Draft: October 2003]

The Appeal and Limits of Internal Controls To Fight Fraud, Terrorism, Other Ills

LAWRENCE A. CUNNINGHAM*

TABLE OF CONTENTS

* Professor of Law and Business, Boston College; Visiting Professor of Law, Vanderbilt University Law School. Thanks to Laura Ford, John Garvey, Robert Hamilton, Arthur Jacobson, Simon Lorne, Richard Nagareda, Richard Painter, Alan Palmiter and Robert Thompson.

INTRODUCTION

Corporate internal controls have become a first-order policy option to respond to a wide variety of national problems. In response to early 2001's financial scandals,1 Congress adopted the Sarbanes-Oxley Act ("SOX"),2 to bolster controls over financial reporting and mandated audits of them; in response to 9/11's terrorism, Congress adopted the USA PATRIOT Act ("PATRIOT"),3 with provisions expanding controls in the financial services industry to interdict terrorist financing and calling for audits of those controls. These two statutes continue a 30-year trend of Congressional and regulatory strengthening of corporate internal controls to address policies from antitrust, to worker safety, to environmental protection. These responses show internal controls as appealing. This Article raises questions concerning their limits.

Corporate internal controls began as internal processes with the positive goal of helping a corporation meet its objectives, a conception creating modest expectations of results. In using them as a leading policy option, controls assume a negative dimension. They become processes designed to prevent certain undesired events from occurring, a conception creating greater expectations. Controls are inherently limited in what they can do, however, making the modest expectations associated with positive controls sensible but increasing the likelihood of disappointed expectations associated with the more ambitious efforts of preventive controls.

Accompanying the proliferation of corporate internal controls to address various policy objectives has been a rise of audits to test those controls. But audits are also limited in what they can do. Auditors cannot guarantee that controls they test are in fact effective, though they can offer some assurance about that. More important, as audit proliferates as a way to test control effectiveness, pressure builds to create controls that can be audited. This means that controls are increasingly designed according to whether they can be audited, not according to whether they are likely to be effective. The proliferation of controls and auditing of them creates so many controls that by sheer volume it becomes more difficult to determine which controls are likely to be effective.

Numerous systemic forces make controls appealing as a policy option. The movements for deregulation and cooperative compliance make controls appealing as alternatives to direct regulation. Resistance to overt federal preemption of state corporate law makes controls attractive as an alternative way to inject federal policy into internal corporate affairs. The rise of the monitoring

---

1 I offer a capsule history of the era's financial context and salient shenanigans as well as a detailed analysis of every provision of the Sarbanes-Oxley Act in Lawrence A. Cunningham, The Sarbanes-Oxley Yawn: Heavy Rhetoric, Light Reform (And It Might Just Work), 35 U. CONN. L. REV. 915 (2003) [hereinafter Cunningham, SOX Yawn].

2 Public Company Accounting Reform and Investor Protection Act of 2002, 107 Pub. L. No. 204, 116 Stat. 745. The Act is popularly known as the Sarbanes-Oxley Act, SOX here for short.

3 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. The Act is known as the USA PATRIOT Act, PATRIOT here for short.

model of the board of directors in corporate governance makes controls essential tools to enable this indirect supervision of corporate affairs. The corporate social responsibility movement calls for greater corporate accountability; controls addressing interests of particular corporate constituencies seem tailor-made for the purpose.

Backing these powerful systemic forces making controls appealing are two professional groups most-closely involved with internal control design and administration: the auditing and legal professions. In the case of auditors, controls are an appealing way to diversify the profession's services. Auditors can both design and test controls. The profession encourages control proliferation and auditing of controls as part of its business strategy. In their marketing, however, auditors oversell what controls can accomplish, and also oversell how auditing of controls can help make controls more effective.

Lawyers like processes, including controls and audits, and this taste can lead them to believe auditor advertisements. An expectations-gap arises. Lawyers focusing on process encourage controls and audits of them and then expect results to follow. In the case of preventive controls, the expected result is preventing some undesirable outcome such as fraud or terrorism. When fraud, terrorism or other undesirable events occur, legal instincts are to assign blame. The failure of internal controls to prevent the undesirable event can thus create legal liability, despite failure's inevitability given that controls are inherently leaky.

These systemic and professional forces put pressure on having controls and having them audited, rather than having controls that are likely to be effective. Controls to prevent become ends in themselves. Legislators and regulators can adopt or encourage controls in the name of doing something in response to crises. Corporations adopt them as a way to defend against liability claims when undesired events occur despite conscientious controls. Auditors test controls to provide comfort. These pressures produce controls for controls' sake. The paradoxical upshot of control and audit proliferation is the more controls there are, the less actual control exists.

This Article's thesis is thus that we expect too much from corporate internal controls. Its burden is to demonstrate their evident appeal, contrasted with their detectable limits. Part I reviews the empirical appeal of internal controls. It attempts to define internal controls, showing some difficulty in doing so because of the blurry lines between what is internal and external in the case of a corporation. It documents the tool's proliferation, dating from the price-fixing, hijacking-terrorism and overseas-bribery scandals of the late 1960s and early 1970s and continuing through to SOX and PATRIOT in 2001. This history shows a move from controls bearing positive goals to controls promising preventive capability. This Part also discusses the pressures mentioned above that make controls a first-order policy option, including systemic and professional forces.

Part II introduces the strong incentives law has created for corporations to adopt internal control systems. These include the federal Organization Sentencing Guidelines and state law fiduciary-duty cases. Both contemplate controls designed to prevent undesirable outcomes. This discussion shows that internal control directives and incentive-regimes rarely specify required substantive content. They favor frameworks consisting of abstract protocols concerning employee

training, supervision, procedure manuals and violation-reporting systems. The abstract nature of these characteristics contribute to the appeal of controls because they are easy to describe and contribute to the limits of controls because they are so general.

Parts III and IV illuminate the limits of internal controls by considering the different approaches to them taken by the auditing profession on the one hand and legal culture on the other.4 An abbreviated account of this contrast is: auditors know controls and audits are inherently limited processes while lawyers invest more confidence that these processes can assure substantive results. The resulting expectations gap adds pressure to use more controls and audits that simultaneously promote the appearance of control and reduce actual control.

When auditors conduct general audits they understand that they may fail to detect misstatements despite the best controls. In their work, auditors examine controls to assess their bearing on this risk. They understand not only that controls are leaky and limited, but that controls can both reduce risk and increase it. Auditors approach their task using professional skepticism. This means probing the judgments management makes concerning all managerial assertions auditors are asked to attest to. Applying this professional skepticism to both the process and results, auditors are willing to second-guess managerial decisions of every kind without deference.

Auditors honed these professional attitudes in their historical work involving audits of financial statements. Auditors increasingly apply these tools to audit a wide range of other matters. These new engagements include the auditing of control systems intended to prevent a variety of undesirable events. Auditors assess the integrity of controls designed to prevent violations of worker safety regulations and environmental standards, for example. Under SOX, they are also required to audit controls over financial reporting and under PATRIOT to audit controls designed to thwart terrorist financing. There is reason to doubt whether the tools auditors apply to old-fashioned financial statement audits work as well when applied in these non-traditional exercises.

Part IV contrasts the audit view of controls and related risk with the legal view. Whereas auditors take steps to reduce the risk that they will fail to detect misstatements to a maximum statistically-acceptable level and then tolerate the residual as inevitable, the legal perspective is preoccupied with liability risk and the design of compliance systems to mediate or allocate it. The focus is on process. This illustrates a key difference in professional attitude between auditing culture and legal culture concerning corporate internal controls.

---

4 A critique of internal control effectiveness cannot rely upon an assessment of the frequency of internal control failure because internal control success cannot be measured (*i.e.*, the absence of fraud, terrorist attack or other aim of internal controls may be attributable to factors other than internal controls). Comparing deviation rates from established norms in pre-and post-control environments is perhaps the best means for assessment, but testing and interpretation remain difficult at best. *See generally* David P. Farrington, *Assessing Systematic Evidence in Crime and Justice: Methodological Concerns and Empirical Outcomes*, 49 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL AND SOCIAL SCIENCE 587 (2003).

Lawyers invest substantial confidence in processes to promote substantive results. In corporate law, for example, the business judgment rule expresses deference to managerial decisions by examining the process of decision-making rather than the result. This belief in process leads lawyers to imagine that controls and audits of them can neutralize risk more fully than is possible.5 Other professional differences between auditing and legal culture reinforce this difference in expectations. These include the fact that auditors confront controls directly and *ex ante* and must opine on them prospectively; lawyers tend to confront controls *ex poste*, after some event has occurred and wonder why effective controls were not in place.

In summary, the appeal and limits of internal controls to fight fraud, terrorism and other ills is a process moving from positive controls recognized as leaky-but-useful to negative controls with high expectations and more limited capability of delivering. Seduced by the appeal of controls as a first-order policy option, distinctions between control, audit and evaluation blur, and what is auditable is more important than what must be valued by judgment. At the extreme, this emphasis on controls can lead controls to take on the character of ends in themselves, rather than means of achieving ultimate goals. By expecting so much of controls and directing so much attention and auditing power on them, we get less effective controls; were we to expect less from internal controls, and shower less attention and auditing power on them, we would actually end up getting more out of them.

Changing expectations concerning controls and audits of them is difficult. The structure of the control-and-audit regime hides the fact that it revives an old problem of agents watching agents. That is, control seeks to govern behavior and is deemed necessary due to lack of trust. Audits of control seek to test those controls to assure behavior is being controlled. But why should the auditor be trusted any more than the agent in the first place? In the control-and-audit regime, they are vested with infallibility that isn't real. And it is not so much that auditors are not trustworthy but that the tools of their craft are inherently limited and the controls they test inherently limited.

Auditors monitoring controls can only test certain kinds of controls. There is a difference between control effectiveness and control audit-ability. A corporation can have controls that are more effective but less audit-able and controls that are less effective but more audit-able. The less we trust those whose behavior we use controls to influence by increasing audit, the more controls will be produced that can be audited. But the infallibility complex concerning auditing

---

5 The tools lawyers confront in the controls process reinforce the conclusion that ambitions are too high; examples in Appendix B show they may become quixotic for controls extending beyond pure internal functionality and toward outward-directed public policy objective such as fighting terrorism. Three illustrations of alternative control templates suggest associated limits. The first considers the relationship between regulation and control, a difficult interpretive bridge to gap yet one that played a role in the bankrupting of PanAm Airways after terrorists blew up one of the company's planes over Lockerbie, Scotland. The second considers how even informal control practices can lead to liability and suggests how this result is likely to degrade rather than enhance the quality and probable effectiveness of internal controls. The third evaluates PATRIOT's internal control directives to suggest highly uncertain payoffs given clearly substantial costs.

systematically biases us to controls that can be audited rather than controls that are effective. In this cycle, the end point undercuts the goal: we seek control because we do not trust the agent and then add a monitor who can only monitor certain controls and those controls may be less effective in controlling the agent's behavior than controls that can't be audited.

The historical solution to this conundrum was the team production theory of organizational behavior and an economic model that explained how workers coordinate activity in ways beneficial to the organization in lieu of either controls (which can be leaky) or audit (which may not be able to test control effectiveness). We have been on an experimental ride since the mid-1970s using controls and audits as tools to overcome what may not be possible to overcome. One way to reduce the false expectations of the control-and-audit regime is to reemphasize the old-fashioned model—and its own limits. Necessary to doing so are for auditors to temper the advertisements of their products, for legal culture to resist allowing control failure to generate liability, and for both to emphasize the limits of controls when articulating applicable standards which influence expectations.

I. CONTROL APPEAL: ROOTS

Internal controls embrace a variety of mechanisms operating as tentacles in the corporate web, connecting external activity to internal operations and reporting, and connecting these back to external reporting. It is useful to begin with some specification of internal controls by type. This furnishes a basis for considering the history of modern internal controls, a history best characterized as proliferation through mandates and incentives, with limited specification of their required content, but irresistible appeal.

A. Classification

Defining corporate internal controls is difficult. A fully-encompassing definition treats as internal controls all the processes or mechanisms an organization uses to promote the achievement and reporting of its objectives.6 Beyond such generalities, specific classifications are elusive. Part of the difficulty is that internal controls have proliferated in the past three decades.

1. Seeking a Definition

Internal controls have adorned management, accounting and financial auditing since the 19th century.7 Traditional controls are mechanisms intended to assure achievement of corporate objectives. Examples are budgeting processes that define project goals and provide cost-benefit exercises to determine whether particular corporate projects should be pursued. Specific examples are duty-segregation practices such as providing that one work group prepares a project proposal and a different group decides whether to pursue it. Controls intended to help a company achieve its

---

6 *See* SECURITIES AND EXCHANGE COMMISSION, COMMENTARY ACCOMPANYING PROPOSED RULES IMPLEMENTING SECTION 404 OF THE SARBANES-OXLEY ACT.

7 *See* MICHAEL POWER, THE AUDIT SOCIETY: RITUALS OF VERIFICATION (1997), at 19-20.

objectives can be called administrative or operational controls.

In the 1920s, controls expanded to include a set of protocols and systems specifically directed at financial reporting and safeguarding assets. Developed principally as a way to enable auditors to efficiently review a company in order to furnish assurance, these can be called accounting or financial controls. Examples are the practice of filing customer orders or invoices in triplicate with various departments from shipping to billing to collections.

In the late 1950s, attempts to define internal controls distinguished between "administrative controls" and "accounting controls."8 The former entailed implementing managerial policy, as through training programs and quality controls; the latter related directly to safeguarding assets and producing reliable financial records, such as duty-sharing among bookkeepers and maintaining adequate record-keeping systems.

Auditors regularly confront internal controls in their audit work. Their experience with internal controls gradually led auditing standard-setters to expand the category of accounting controls to include mechanisms previously in the category of administrative controls. By the early 1970s, standards denominated administrative controls as the mechanisms governing managerial authorization of transactions, while accounting controls were mechanisms intended to safeguard assets and records to accord with managerial policies that would permit preparing fairly-presented financial statements, promote accountability for asset protection, and periodically compare recorded assets with actual assets to resolve any discrepancies.9

Since the 1970s, controls have exploded in numerous directions to include protocols and systems intended to prevent bribery, protect consumers and workers from harm, preserve environmental resources, and combat terrorism. These can be called policy controls or compliance controls.

A comprehensive study of internal controls in the early 1990s led auditing standard-setters to jettison older distinctions between administrative and accounting controls and to incorporate these new policy and compliance controls. The Committee of Sponsoring Organizations (COSO) collapsed the categories under a single heading called simply internal controls.10 COSO thus functionally re-designated all previously-defined administrative controls as accounting controls**.** In

---

8 STATEMENT OF AUDITING PROCEDURES (SAP) No. 29 (1958).

9 STATEMENT OF AUDITING PROCEDURES (SAP) No. 54 (1972).

10 COMMITTEE OF SPONSORING ORGANIZATIONS (1992). Numerous professional bodies, most in the accounting and auditing professions, have expended substantial effort since 1975 refining and developing internal controls. These include the National Commission on Fraudulent Financial Reporting (the "Treadway Commission"), jointly sponsored by the AICPA, the American Accounting Association, the Financial Executives Institute, the Institute of Internal Auditors, and the National Association of Accountants (these organizations are, in turn, collectively called the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission and operate a separate internal control project). *See* www.coso.org.

part this shift reflected the view that all controls were factors auditors needed to understand when designing a general financial audit. Under the COSO classification, as well as formal auditing standards adopted in the mid-1990s,11 corporate internal controls are processes designed to promote achieving all corporate objectives, including those relating to operations, financial reporting and compliance with law.12

In rules implementing SOX, the SEC hazards return to the older classifications by distinguishing a category of internal controls "over financial reporting."13 It defines these as mechanisms intended to safeguard assets and assure that transactions are properly authorized, recorded and reported to enable preparing fairly-presented financial statements.14 This formal definition of controls "over financial reporting" denotes mechanisms that "pertain to the preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles."15 Implicit in this distinguishing definition is that a recognized category of non-financial controls endures, just as they have since the 1950s when they were denominated as administrative controls. Today these include both operational (or administrative) controls and compliance (or policy) controls.

The SEC's revival of the classical distinction among control types is not intended to suggest that financial auditors need not concern themselves with non-financial controls. It does, however, emphasize that auditors conducting financial audits are more concerned with financial than with operational or compliance controls. The SEC further mints and distinguishes a category of controls called "disclosure controls and procedures." It defends the distinction between internal controls over financial reporting from disclosure controls and procedures by saying that the two overlap but each covers ground the other does not.

2. Positive versus Negative Goals

The struggle to classify controls underscores the difficulty of distinguishing control types. The SEC's distinction between financial controls and compliance controls is one possibility. Another is between inward-directed versus public-policy. But all such categories are difficult to

---

11 STATEMENT OF AUDITING STANDARDS (SAS) No. 78 (Am. Inst. of Certified Pub. Accountants) (1995).

12 For a complete history of corporate internal control systems, see STEVEN J. ROOT, BEYOND COSO: INTERNAL CONTROL TO ENHANCE CORPORATE GOVERNANCE (1998).

13 *See* SECURITIES AND EXCHANGE COMMISSION, FINAL RULE: MANAGEMENT'S REPORTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND CERTIFICATION OF DISCLOSURE IN EXCHANGE ACT REPORTS, 17 C.F.R. 210 (June 5, 2003), at 9.

14 *Id.* (citing as consonant with this view CODIFICATION OF ACCOUNTING STANDARDS AND PROCEDURES (Am. Inst. of Certified Pub. Accountants) § 319, Sarbanes-Oxley Act § 103, and the Foreign Corrupt Practices Act, Securities Exchange Act § 13(b)(2)(B)).

15 *Id.*

sustain. The SEC's attempt to distinguish a category of disclosure controls and procedures illustrates the point. It partakes of portions of both financial controls and compliance controls.

The difficulties of distinguishing between internal and policy controls are due to the complex nature of the corporation. Corporations have multiple roles and constituencies. Even proponents of shareholder-centric corporations pursuing shareholder wealth maximization must recognize that corporations also affect the interests of non-shareholder constituencies. Devotees of corporate social responsibility make this stance explicit. While attempting to arrange control types along a continuum for purposes of tying controls to particular interests may be possible in theory, it is difficult in practice.

A more fruitful possible distinction between controls are those designed to achieve positive or aspirational ends and those designed to achieve negative or preventive goals. These may operate on a continuum as well, but locations are a bit more transparent and certainly less controversial.16 The history of internal controls supports this conception.

Administrative or operational controls originated as mechanisms intended to help produce positive ends consisting of the achievement of corporate objectives. Amid proliferation, controls have assumed a strong negative dimension. Policy/compliance controls in particular are conceived as devices intended to prevent negative events from occurring. A common theme of internal control development in the past decade has been a diminution of the significance of the positive purposes of traditional administrative or operational controls and an increasing accentuation of the negative purposes of contemporary policy/compliance controls.17

The change of purpose appears in SOX. Financial controls are traditionally intended to promote the positive result of fairly presented financial statements. In SOX, they appear to be aimed at least as much at the negative goal of preventing fraud.18 Contemporary classification of controls

---

16 The positive-negative distinction is imperfect but captures important differentiating characteristics. Traditionally financial controls were intended to help produce fair financial reporting. In that positive sense they were akin to traditional operational controls, with the goal of promoting corporate objectives. Compliance controls are primarily intended to meet governmental policies, without that first priority of achieving corporate objectives. Though particular governmental policies may be written in positive terms, from the corporation's viewpoint the goals are not principally about meeting its objectives (a primary, positive aspiration) but about meeting the government's with the corporation's principal interest being to avoid violating laws or exposing itself to liability (a negative objective). *See infra* Part II.C.1.

17 *See* ROOT, *supra* note 12 (explaining that while the COSO framework notes the positive dimension in early sections defining controls as mechanisms intended to help with the "achievement of objectives" and the "effectiveness and efficiency of operations," later detailed discussion of applications mutes this significant characteristic).

18 *See, e.g.*, PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD, PROPOSED STANDARD: AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING PERFORMED IN CONJUNCTION WITH AN AUIT [SIC] OF FINANCIAL STATEMENTS (Oct. 7, 2003).

does not formally embrace this characterization of controls as positive- or negative-directed. But the various struggles to define and classify internal controls suggest it is possibly a more accurate and useful way of thinking about them.

The SEC's definitional efforts, as well as those of COSO, imply a further broad distinction between operational or administrative controls and all others. Corporations continue to adopt a variety of operational controls for their own internal purposes. These are intended specifically to achieve objectives relating to the business as an operating entity. Controls promulgated by the SEC or required or encouraged by other governmental entities are the stuff of public policy options. This is increasingly the case even for financial controls under SOX.

3. Practical Specification

Despite classification difficulties, a distinction between financial and compliance controls retains utility. In addition to operating controls, all companies maintain financial controls designed to assure the adequacy of financial reporting. For public companies, these controls have been required by federal securities laws since the 1970s19 and under SOX officers must certify their integrity and auditors must attest to the certification's assertions.20 The content and operation of financial controls can be general, but all are tailored to particular companies. General mechanisms include systems promoting security and redundancy, programming to adhere to specified standards and constraints on subjective judgment as through cross-checking.21

Compliance programs are a species of internal controls, typically a tailored set of devices to meet externally-imposed non-financial mandates. Examples are protocols designed to assure meeting federal workplace regulations promulgated by the Occupational Safety and Health Administration and standards of environmental control promulgated by the Environmental Protection Agency. Many companies adopt a range of standards promulgated by the International Standards Organization, from environmental guidelines to quality control, based on detailed procedures, documentation and testing. Specific industries adopt particular programs to comply with regulatory law, including industries such as securities, insurance, and medicine. PATRIOT imposes a variety of compliance controls on businesses in the financial services industry—from banks to casinos to card clubs—including programs designed to identify suspicious activity among

---

19 The fountainhead of modern internal control regulation is 1977's Foreign Corrupt Practices Act ("FCPA"), Title I, Pub. L. No. 95-213 (1977), codified in scattered sections of 15 U.S.C., which in turn codified various provisions of professional auditing standards, including SAS No. 1. *See* SECURITIES AND EXCHANGE COMMISSION, FINAL RULE: MANAGEMENT'S REPORTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND CERTIFICATION OF DISCLOSURE IN EXCHANGE ACT REPORTS, 17 C.F.R. 210 (June 5, 2003), at 7.

20 *Id*.

21 Controls thus consciously seek to prevent the need for judgment and this reveals a systemic limit and danger of such systems. Judgments must be made. Controls constraining judgment deny this reality. *See infra* Part IV.

customers that could indicate involvement in terrorist financing.22

The distinction between financial and compliance controls is reflected in the allocation of responsibility for controls within a corporation. Boards of directors and managers jointly define, implement and evaluate internal controls, both financial and compliance. In principle, however, chief responsibility for internal controls rests with the board of directors, for controls are intended to radiate throughout the corporation. A board's leadership obligation entails supervising the design of internal controls and supporting their administration. Teams of internal managers implement and review internal controls, teams including both internal auditors and lawyers, and this is where function supports the classical distinction between financial and compliance controls.

A financial department typically administers financial controls, headed by a chief accounting officer, chief financial officer, director of internal audit or, more recently, a new position called chief risk officer. Historically, financial controls were intended to promote fair financial reporting, though after SOX they increasingly are intended to prevent fraud. Financial controls are reviewed by the firm's outside auditor in connection with its annual examination of the financial statements, and SOX requires separate testing of internal financial controls beyond that undertaken to audit the financial statements.23 The board as a whole is directly responsible for the production of general purpose financial statements depicting overall performance. Board oversight of financial controls and external audit is thus direct, typically exercised through a board audit committee seen as one of the most important board committees.

The general counsel's office traditionally administers compliance controls. Contemporary proliferation of these controls uses them as tools to promote governmental policies, as ways to prevent the corporation from violating laws. Board oversight of compliance controls tends to be more attenuated than for financial controls. Responsibility for non-financial controls is not ordinarily assigned to particular board committees. Corporate reporting concerning these matters is not typically part of the annual reporting process concerning overall corporate performance. Any annual reporting that is required concerns discrete matters targeted to particular audiences, such as the EPA or OSHA. They can be audited but are not routinely audited in the same way or to the full extent that internal financial controls are audited. Examples of unusual cases where such reporting and auditing has been undertaken on a par with financial reporting are so-called corporate social responsibility reports and audits, made famous by companies such as Ben & Jerry's Ice Cream and The Body Shop.24

B. Proliferation

---

22 *See* Appendix C.

23 *See* Part III.C.

24 *See* David Hess, *Social Reporting: A Reflexive Law Approach to Corporate Social Responsiveness*, 25 IOWA J. CORP. L. 41 (1999); Lewis D. Solomon, *Implementation of Humanomics by Modern Publicly Held Corporations: A Critical Assessment*, 50 WASH. & LEE L. REV. 1625 (1993); see also Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197 (1999).

The modern history of internal controls has been their proliferation and expansion as a policy option, commonly in response to pending crises.25 Before the 1960s in corporate America, internal controls for financial reporting were common if limited in scope and those for non-financial matters such as preventing violations of law were rare.26 Both began to proliferate following the electrical equipment industry's antitrust scandal of the early 1960s, hijacking-terrorism of the late 1960s and early 1970s, and the foreign-bribery scandals of the early 1970s.

1. Thirty Years of Controls

A leading corporate figure in the antitrust scandals was Allis-Chalmers Co., whose executives agreed to testify for the government against other conspirators in a price-fixing ring. The immediate result was the prosecution of 29 corporations and 45 people pleading guilty or *nolo contendre* to a variety of criminal antitrust violations. Of these, seven went to jail and another 24 received suspended sentences.27 A shareholder lawsuit against Allis-Chalmers executives and board members was dismissed on the grounds that these individuals had no obligation to implement a corporate "system of espionage" to detect the antitrust violations.28 Despite the court's disparaging characterization, the specter of espionage evolved shortly into the concept of compliance programs.

Interest in internal financial controls accelerated the next decade, in the wake of the overseas bribery scandals of the early 1970s. Leading US companies such as Lockheed Aircraft, Exxon, Mobil, Gulf, and United Brands bribed foreign officials and failed to record the bribes accurately on their corporate financial statements. So severe was the resulting crisis that the CEO of United

---

25 A parallel history runs through corporate criminal liability, with a historical aversion to the concept due to the absence of a corporate *mens rea*, though there is fairly wide use and acceptance of it today. For a dissent from the current prevalence of corporate criminal liability chiefly using economic analysis, see Daniel R. Fischel & Alan O. Sykes, *Corporate Crime*, 25 J. LEG. STUD. 319 (1996).

26 *See, e.g., Bates v. Dresser*, 251 U.S. 524, 530 (1920) (Holmes, J.) (bank's outside directors not liable for failure to maintain adequate controls or examine underlying ledgers to detect fraud effected by head cashier that essentially depleted entire assets of the bank, though holding attributed in part to semi-annual audit of bank regulators and validation of cashier's reports by bank president).

27 John D. Copeland, *The Tyson Story: Building an Effective Ethics and Compliance Program*, 5 DRAKE J. AGRIC. L. 305 (2000) (highlighting *Allis-Chalmers* and kindred cases in context of detailed study of poultry-industry leader Tyson).

28 *Graham v. Allis–Chalmers Manufacturing Co.*, 188 A.2d 125 (Del. Ch. 1963) (corporate "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 on directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists.").

Brands committed suicide by jumping 44 stories off the PanAm Building in New York City.29 So broad was the scandal's scope that it led to the toppling of various governments around the world, including in Bolivia, Honduras and Japan. The national mood compelled Congress to "do something." The upshot was the Foreign Corrupt Practices Act (FCPA), an ambitious piece of legislation intended to prevent offshore bribery and false financial reporting obscuring its use. The FCPA laid the foundation for a corporate mandate to develop and implement a wide range of internal financial controls.30

Compliance controls relating to terrorism arose after a spate of hijackings to Cuba and in the Middle East in the late 1960s and early 1970s.31 As aircraft traveling range increased, hijackings assumed greater appeal. On February 21, 1968, Lawrence Wilson Rhodes became the first of 37 hijackers of US commercial aircraft over the next two years demanding to be taken to Cuba.32 In the 1970s, hijackings by the Arab terrorist group Popular Front for the Liberation of Palestine (PFLP) escalated, featuring the spectacular 1970 Labor Day weekend simultaneous commandeering of four commercial jets from various European capitals to Dawson's Field in Jordan.33 In a rush to respond to crisis, Congress enacted a series of laws imposing internal control mandates on airlines aimed at improving security at airports and aboard planes to prevent terrorism.

Other examples of industry-specific crises that resulted in prescribing increased internal controls abound. They include:

• The early 1980's defense contractor scandals, famously featuring $10,000 wrenches and $7,000 coffee machines, led ultimately to the Packard Commission's reports and recommendations for enhanced internal controls adopted by executive branch agencies and subsequently embraced by many industries.34

---

29 Copeland, *supra* note 27 (*citing* Eleanor J. Tracy, How United Brands Survived the Banana War, *Fortune*, July 1976, at 145).

30 After the FCPA was passed, the SEC proposed regulations requiring certification and attestation of internal controls systems but shelved them in response to corporate pressure. *See* SEC COMMENTARY ACCOMPANYING PROPOSED RULES IMPLEMENTING SECTION 404 OF SOX. It repeated the same proposal-withdrawal pattern in 1988 after the Treadway Commission (COSO) report was published. *Id*.

31 Earlier isolated incidents involving threats in the aviation industry elicited no such response. The first hijacking ever seems to have occurred in Peru in 1930, conducted by military officers attempting a coup. In the 1950s, US bank robbers used hijackings to make escapes.

32 DAVID FRUM, HOW WE GOT HERE: THE 70S–THE DECADE THAT BROUGHT YOU MODERN LIFE, FOR BETTER OR WORSE (2000).

33 A copious and insightful opinion concerning insurance law but dwelling on the Arab-Israeli conflict, penned by Judge Marvin E. Frankel (1921-2002), addresses this case. *Pan American World Airways, Inc. v. Aetna Casualty & Surety Co.*, 368 F. Supp. 1098 (S.D.N.Y. 1972), *aff'd* 505 F.2d 989 (2d Cir. 1974).

34 Among the statutes adopted in response to the defense contractor scandals were 1986 Amendments to the False Claims Act, the Anti-Kickback Enforcement Act of 1986, and the Major

• In the mid-to-late 1980s, the financial services industry was engulfed by the insider trading scandals starring Dennis Levine, Ivan Boesky, and Michael Milken, which led to the Insider Trading and Securities Fraud Enforcement Act of 1988's imposition of compliance codes on broker-dealers and investment advisers to prevent insider trading.35

• Evolving environmental concerns throughout the 1980s produced an array of regulatory requirements on business that contain substantial internal control and compliance mandates (in addition to various criminal penalties).36

• In the 1990s, the internal control pressure valve increasingly opened up in the health care industry in response to a rising incidence of fraud in Medicare billing and related areas.37

2. Contemporary Responses

Contemporary accounting scandals and terrorism prompted Congress to adopt new laws imposing internal controls, both financial and compliance. On the terrorism-compliance side, Congress determined that the terrorist attacks on the US of September 11, 2001 were financed using funds transmitted throughout the US financial system. The attacks were a wake-up call in Congress to the reality that our financial system is a conduit for funding dozens of terrorist organizations and thousands of terrorists here and abroad. Congress responded to this awakening with PATRIOT, an act of sweeping breadth containing several specific sections mandating that financial services businesses impose compliance controls to interdict money laundering and identify suspicious activities of customers who may be involved in terrorist activities.

On the accounting-financial controls side, a series of accounting debacles unraveling from the end of 2001 through mid-2002 exposed cracks in the US financial reporting and governance systems.38 Policy analysts advocated a variety of measures. Virtually all embraced some way to improve internal financial controls, increasing the layers of checks and balances within corporations and among audit staff. SOX encapsulated a dozen such controls, the most salient of which require (1) CEO/CFO certification of the design and integrity of internal controls over financial reporting and (2) external auditors to test and opine on such control design and effectiveness, including management's certifications.

PATRIOT and SOX show internal controls as an appealing Congressional policy response to pending crises. As with other such impulses to strengthen internal controls—financial and compliance—however, they are based far less on a calculated cost-benefit assessment of the

---

Fraud Act of 1988.

35 Pub. L. No. 100-174, 102 Stat. 4677 (codified in scattered sections of 15 U.S.C.).

36 Major environmental statutes amended during the 1980s included the Resource Conservation and Recovery Act, CERCLA, the Clean Water Act, and the Clean Air Act.

37 .*E.g.*, Medicare Mediaid Anti-Kickback Act (1972, with amendments since); Medicare and Medicaid Protection Act of 1987. Also applicable are the False Claims Act and the False Statements Act. Relevant case law includes *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996), discussed *infra*

38 *See* Cunningham, *SOX Yawn*, *supra* note 1.

likelihood of their effectiveness, than a populist need to exhibit taking control.39 After all, PATRIOT was adopted in less than 45 days from drafting and SOX within a few months. The motivation for such legislative "reform"—from the Lockheed scandals to hijackings, terrorism and corporate power abuse—is public revulsion. A variety of pressures combine to make controls appealing to Congress amid such crises, as well as in the wide range of more routine areas in which legislators and regulators have looked for controls as a solution to various social problems.

C. Pressure

Two broad phenomena contribute to increasing pressure to make internal controls a first-order policy option. The first is a series of systemic forces percolating beginning in the 1970s and escalating since the 1980s. The second are professional, principally from the auditing profession, with some reinforcement from the legal profession.

---

39 When administrative agencies propose regulations directing or encouraging internal controls, they must satisfy various requirements including assessing the costs and benefits, an exercise Congress does not face. On the other hand, substantial control-spawning federal legislation originates with administrative agencies lobbying Congress for passage and those agencies subsequently analyze the costs-and-benefits of the schemes once passed.

A precise cost-benefit analysis is elusive. SOX responded to what I've called the Big Four Frauds: WorldCom, Enron, Qwest and Global Crossing. *See* Cunningham, *SOX Yawn*, *supra* note 1. The intended benefit is preventing recurrence, making associated losses a good proxy for estimated benefits. The aggregate equity capitalization of the Big Four Frauds at the peak of the 1990s stock market bubble approximated $300 billion (WorldCom $115 billion, Enron $80 billion, Qwest $68 billion, and Global Crossing $40 billion). A substantial portion of the peak levels was due to irrationally-elevated valuation estimates, making far lower this proxy for the benefit from scandals-to-be-prevented controls regulation. The actual benefits given inherently leaky controls are some fraction yet again of that total. To be generous, benefits might be $100 billion over the next five or so years. Additional benefits may accrue from greater reliability of financial data that drives more optimal capital allocation, but these benefits are impossible to measure even roughly.

The costs of complying with SOX include fees paid to the new auditing oversight board (the PCAOB), expenses for control systems and related audits and certifications, insurance premiums and incalculable costs of foregone opportunities driven by risk-aversion deepened by the culture of control. Estimated additional average annual compliance costs are approximately $1.2 million per mid-level SEC registrant, more and less for companies larger or smaller. *See, e.g,* LANCE JON KIMMEL & STEVEN W. VAZQUEZ, THE INCREASED FINANCIAL AND NON-FINANCIAL COST OF STAYING PUBLIC, 2003 NATIONAL DIRECTORS INSTITUTE (Foley & Lardner 2003). With these costs applicable to some 10,000 SEC registrants, that is approximately $12 billion in direct costs per year, meaning direct costs in absolute terms of approximately $60 billion over five years. The cost-benefit calculus becomes a close call when you add some immeasurable costs of undue risk aversion or false confidence in control effectiveness (the latter is discussed further in Part III.C).

For a cost-benefit assessment of internal controls under PATRIOT, see discussion in Appendix C.

1. Systemic

While exact cause-and-effect cannot be determined or measured, the rise of internal controls corresponds with the deregulatory atmosphere spawned during the early 1980s under President Ronald Reagan. That movement was simply an incrementally-stronger manifestation of broader traditional American attitudes generally favoring private industry to state ownership. Legislative and regulatory responses to private sector crises using internal controls enable the state to reach into the private sector to exert power while preserving the essentially private character of its organizations and their operation.40 Controls can also be a vehicle for federal governmental influence on corporate behavior without formal preemption of state corporate law, skirting a longstanding debate.41

Pressures driving control proliferation include evolving conceptions of corporate governance.42 The rising significance of internal controls paralleled the rise of the monitoring model of the corporate board of directors.43 Internal controls moved from an incident of audit practice to a tool to implement indirect board supervision of corporate performance. The tools address problems of asymmetric information in hierarchical organizations (individual employees have incentives to skew information to their benefit at the expense of the organization's) and risks of managerial opportunism (managers with short tenures or compensation tied to short-term performance have interests in conflict with those of the corporation as a whole).44 The monitoring model's impact on internal controls is akin to deregulation's impact: they trade direct for indirect

---

40 Theorists since that period have pushed for a strategy marrying market and regulatory accountability mechanisms that seem to reflect this strand of regulatory philosophy, variously called deregulation, cooperative compliance, interactive compliance, responsive regulation, collaborative governance, cooperative implementation and so on. *E.g.,* STEPHEN BREYER, REGULATION AND ITS REFORM (1982); JAY A. SIGLER & JOSEPH E. MURPHY. INTERACTIVE CORPORATE COMPLIANCE (1988); IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE (1992).

41 Classics in this voluminous debate include William L. Cary, *Federalism and Corporate Law: Reflections Upon Delaware*, 83 YALE L. J. 663 (1974); Ralph K. Winter, Jr., *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251 (1977); Roberta Romano, *The State Competition Debate in Corporate Law*, 8 CARDOZO L. REV. 709 (1987); Joel Seligman, *The New Corporate Law*, 59 BROOK. L. REV. 1 (1993). Important current contributions include Robert B. Thompson & Hillary A. Sale, *Securities Fraud as Corporate Governance: Reflections upon Federalism*, 56 VAND. L. REV. 859 (2003); Mark J. Roe, *Delaware's Competition*, 117 HARV. L. REV. ___ (forthcoming 2003).

42 This is the case of for-profit corporations. Yet internal control proliferation is more widespread. *See infra* note 124.

43 *See* Melvin A. Eisenberg, *The Board of Directors and Internal Control*, 19 CARDOZO L. REV. 237 (1997); Michael P. Dooley, *Two Models of Corporate Governance*, 47 BUS. LAW. 461 (1992).

44 *See generally* John C. Coffee, Jr., *Beyond the Shut-Eyed Sentry: Toward a Theorectial View of Corporate Misconduct and an Effective Legal Response*, 63 MICH. L. REV. 1099 (1977).

power.

The monitoring model led to the universal use of audit committees for large public corporations. Audit committees were not common until the late 1970s, after the New York Stock Exchange adopted rules in 1978 requiring them (though the SEC encouraged audit committee use as early as 1940).45 Audit committees are supervisors of controls. Auditors work with audit committees to conduct financial audits. Both are functionally reliant upon internal controls to aid in the processes intended to enable preparation of fair financial statements. While control and audit are thus distinct exercises, both have grown in parallel fashion since the 1970s and they tend to reinforce each other. Many regulatory directives promoting controls simultaneously promote audits of them.46

Self-observation capabilities developed along with this monitoring model and audit committee reliance upon controls. As pressure mounted on boards to assume responsibility for designing and administering financial and compliance controls, the corporate internal auditing function blossomed. The evolutionary history of the internal audit function parallels the proliferation of controls generally. Internal audit began as an analogue to external auditing. As controls evolved to include non-financial systems elements, the internal audit function grew to encompass their design, administration and testing.47

Another corporate governance development driving control proliferation is the corporate social responsibility movement.48 More is demanded of corporations. Beneficiaries of these demands extend beyond shareholders to numerous non-owner constituencies. Among these are employees, customers, even communities. Laws relating to workplace safety, antitrust and environmental preservation may be seen to protect such constituencies. Imposing or encouraging related internal controls signals addressing these interests without overtly displacing the conventional conception of the corporation as owned by shareholders and managed for them by their agents.

2. Professional

A second force behind the rise and appeal of internal controls—and reinforcing each of these

---

45 N.Y. STOCK EXCHANGE, LISTED COMPANY MANUAL, 303.01(A); NASD By-Laws, Art. 9, Sec. 5; NASD Marketplace Rules, Sec. 4350(d)(1)-(2)); s*ee* DAVID N. RICCHIUTE, AUDITING AND ASSURANCE SERVICES (7th ed. 2003), at 151.

46 *See infra* Part II.

47 *See* Eisenberg, *supra* note 43, at 253 ("as the principle of internal controls has evolved, the internal auditing function has evolved in a parallel way").

48 *See* C. A. Harwell Wells, *The Cycles of Corporate Social Responsibility: An Historical Retrospective for the Twenty-first Century*, 51 KAN. L. REV. 77 (2002); *compare* William W. Bratton, *Confronting the Ethical case Against the Ethical Case for Constituency Rights*, 50 WASH. & LEE L. REV. 1449 (1993) *with* Stephen M. Bainbridge, *Corporate Decisionmaking and the Moral Rights of Employees: Participatory Management and Natural Law*, 43 VILL. L. REV. 741 (1998).

systemic forces—are the professionals involved in selling them.49 Chief among these are auditors. The auditing profession's business interest is to promote such controls, though somewhat indirectly. Its principal interest is to promote the need for testing and offering assurances with respect to controls.50 For example, the auditing profession for at least four decades made the case that it is necessary for internal financial controls to be formally and publicly audited,51 an aspiration finally granted for financial audits of SEC registrants in SOX.

The auditing profession diversified its activities substantially beginning in the mid-1980s, conducting far more attestation services apart from traditional financial audits. 52 The apotheosis of this expansion that emerged since the late 1980s is the ethics audit. This audit reports on management's performance in monitoring the risk of unethical behavior throughout a company.53

KPMG's trademark version of this exercise was advertised as "ethics process management," a service related to six risks that bear on corporate ethics: sexual harassment, environmental contamination, antitrust infractions, improper foreign payments, fraudulent financial reporting, and race discrimination.54 In other words: the service is addressed to preventing all the hot-button ills of our time. There is no doubt this will routinely include anti-terrorism and anti-money laundering policies, at least for the financial services industry.55

The AICPA's Special Committee on Assurance Services (known as the Elliott Committee) in 1995 argued for expanding the profession's scope of assurance services, leading many public accounting firms to redesignate their auditing departments as assurance departments.56 The Elliott Committee emphasized that risk assessment services, a strong growth segment, could rise to 10-20% of annual financial audit fees.

The attestation profession, of which auditing is a part, engages in a wide variety of assurance services. Apart from financial audits, the wide range of examples includes attestations relating to balloting for the Academy Awards, claims of test improvement results at instructional companies such as Stanley Kaplan, counts of the number of equivalent subscribers magazine publishers boast, verification of claims made by the company that publishes *Consumer Reports* concerning its testing

---

49 *Cf.* Fischel & Sykes, *supra* note22, at 346-348.

50 *See* RICCHIUTE, AUDITING, *supra* note 45, at 640-641 ("public accounting firms have compelling economic incentives to enter—rather than ignore—the assurance services market.").

51 *Id*., at 200.

52 RICCHIUTE, AUDITING, *supra* note 45, at 711.

53 Many commentators promote such ethics audits. *E.g.*, Lynn Sharp Paine, *Managing for Organizational Integrity*, HARV. BUS. REV., Mar.-Apr. 1994, at 106; Linda Klebe Trevino et al., *Managing Ethics and Legal Compliance: What Works and What Hurts*, 41 CAL. MGMT. REV. 131 (Winter 1999).

54 RICCHIUTE, AUDITING, *supra* note 45, at 711.

55 *See infra* Part III.C.

56 SPECIAL COMMITTEE ON ASSURANCE SERVICES, AICPA, REPORT OF THE SPECIAL COMMITTEE ON ASSURANCE SERVICES (1997).

and reporting methods and even the claim by a sporting goods company concerning how its golf balls outdistance competitors by so many yards per drive. 57 Whole new fields include privacy audits and data security assurances.58 On the horizon are audits relating to controls governing anti-money laundering policies and anti-terrorism policies generally.59

Auditors boast of their product's value.60 The attestation profession encourages expectations concerning what controls can do and how the profession can help. This is true even though these professionals know that inflated expectations may come back to haunt them.61 In fact, auditors stoke this business. When internal controls are recommended or required, for example, they conduct surveys and report results on who has what level of controls and who does not.62 This stimulates market growth in the public assurance business, boosting revenue.

Lawyers also benefit from mandates for designing and implementing controls. In SOX's wake, for example, law firms produced scores of client memos advertising products ranging from ethics codes to compliance manuals.63 Plaintiffs' lawyers benefit from the additional theory of

---

57 These examples are sprinkled throughout the college textbook on auditing, RICCHIUTE, AUDITING, note 45.

58 *Id*. at 198.

59 *See infra* Part III.C.

60 The Web sites of each of the largest public accounting firms show eager advertising skills at work; description emphasizes all the benefits it produces, never mentioning inherent limits. *E.g*., KPMG, ASSURANCE (the firm's "Business Measurement Process (BMP)" is the first fully risk-based system, a proprietary product powered by state-of-the-art technology focused on key business risks on a year-round basis; such tools when used for internal audit will "provide you with a greater return on your internal audit investment."); PRICEWATERHOUSECOOPERS, AUDIT & COMPLIANCE (we help make everyone "feel confident that both the hazards and opportunities of risk are effectively addressed across the organization"; "Our Internal Audit Technology Solution is TeamMate™"; we "boost confidence and trust in your web business"; we provide assurance that web processes comply with "policy statements (assertions) made by management"; "we provide independent assessments of the adequacy of controls within the processes and systems that ensure the integrity of management information"); PRICEWATERHOUSECOOPERS, SAS NO. 70 SERVICES (when third parties ask for a report on internal control "A SAS No. 70 audit will be your solution," a "formal report on the design, implementation, and operating effectiveness of controls," and you can get such a report on other parties too); DELOITTE & TOUCHE, CONTROL REVIEWS ("We perform a wide range of control reviews;" "Not only do we seek to highlight significant exposures, but we go the extra mile to recommend potential solutions").

61 *See* POWER, *supra* note 7,at 144 (auditors "talk up expectations at the very same time as [they] may suffer from so doing").

62 *See* POWER, *supra* note 7, at 57.

63 *See* Anthony Lin, *Corporate Governance Practice Groups Spawn From Troubled Waters*, N.Y.L.J., Aug. 12, 2002 (noting common practice among law firms in SOX's wake to write client memos outlining issues and inviting clients to call and noting this is "hardly surprising" given that SOX "promise law firms something for just about everyone, and for a long time to come").

liability controls create. Whereas traditional tort principles of causation and foreseeability can defeat claims victims make when damaged by a supervening cause such as a terrorist attack, the additional claim that internal controls failed lowers these barriers.64

II. CONTROL APPEAL: MANIFESTATIONS

The roots of internal control proliferation have grown into an elaborate forest of controls. The forest is manifested in important legal incentives to adopt them. Control appeal is also evident in both the generality of what control incentives and directives provide as well as the increasing harmonization of the general devices that comprise their content.

A. Incentives

The appeal of internal controls is evident in the extensive array of incentives offered to organizations to adopt them. Bestowed benefits of adopting corporate internal controls include (a) limiting legal liability of public companies under the Foreign Corrupt Practices Act, which can otherwise expose businesses to violations of federal securities laws for failing to maintain adequate accounting records; (b) sentencing reductions for organizational wrongdoing under the federal government's Organization Sentencing Guidelines (OSGs) and from prosecutorial grace pursuant to the Department of Justice's guidance for US attorneys; and (c) helping a corporate board of directors discharge its fiduciary duties as articulated in major corporate law cases relating to the duty of care.65

1. Federal

The Foreign Corrupt Practices Act (FCPA) requires SEC registrants to create and maintain a system of internal accounting control that provides reasonable assurance that transactions are authorized and properly recorded.66 "Reasonable assurance" connotes a level of comfort that would satisfy prudent persons when conducting their own affairs. Administration of the FCPA falls on the SEC.67 Factors the SEC deems relevant in assessing a system's adequacy include: board and audit

---

64 *See infra* Parts IV.B-C & Appendix B. It doesn't always take control failure to reduce these barriers. *See In re September 11 Litigation*, (21 MC 97, S.D.N.Y. Sept. 9, 2003) (denying motions to dismiss of airlines, property managers and aircraft manufacturer at pre-discovery stage on grounds that they owed duties to passengers and victims "on the ground" and that proximate causation defenses were premature given state of the record).

65 In some cases, incentives to use controls also hint at an awareness of their limits. Many incentives encourage controls by offering rewards for using them, not solely exposure to liability for their failure. Such provisions suggest some value in the carrot of reward over the stick of liability, an important feature of these incentives that can help enhance control effectiveness. Still, a key implication of the proliferation of incentives to use controls is a strong sense of their appeal as a policy option.

66 15 U.S.C. § 78m(b).

67 *E.g., SEC v. Montedison, S.p.A.*, 3 FCPA REP. 699.450, 699.450 (Nov. 1996) (alleging

committee involvement; policy communication throughout the organization; assigning authority and responsibility; investing competent compliance personnel with integrity and accountability; and objectivity and effectiveness of internal audits.68

Executive branch agencies, including the SEC, encourage internal control use in additional ways. The SEC, for example, announced in late 2001 a framework for evaluating cooperation by companies that could lead the SEC to refrain from taking enforcement action.69 The framework is built on cooperation such as providing information and directing remediation; but it also emphasizes self-policing in the form of compliance procedures, establishing proper tones at the top, conducting internal investigations of noncompliance, and promptly correcting and disclosing misconduct when discovered. It is a deal to exchange state involvement for control promises, a deal indulging the pressure to prefer in principle internal corporate controls to direct governmental supervision or management.70

The federal Organization Sentencing Guidelines (OSGs) furnish specific ways for corporations to reduce their culpability rating for various offenses. These include maintaining a corporate compliance program and system of internal control.71 To be eligible for lower penalties and sanctions, a company must establish programs and controls calculated to reduce criminal conduct. They must appoint a senior compliance officer, restrict awarding discretion to employees with criminal tendencies, convey corporate policy to staff and respond quickly to violations.72 In addition, illustrating the policy habit of trying to enhance control by also imposing audit, the OSGs require the monitoring and auditing of employees to promote compliance.

The Justice Department's Attorney's Manual directs prosecutors to consider internal controls and corporate compliance programs when deciding whether to prosecute and in recommending

---

FCPA violations in misrepresenting financial condition by concealing hundreds of millions of dollars in bribes to Italian officials); *SEC v. Marlene Indus. Corp.*, 17 SEC Docket 406, Litigation Release No. 8733, 1979 WL 22175, at *1 (SEC Apr. 26, 1979) (alleging FCPA violations due to creation of false and inaccurate cash allowance vouchers and use of improper and inaccurate corporate records).

68 *See* SEC NOTICE OF WITHDRAWAL OF PROPOSED RULES REGARDING STATEMENT OF MANAGEMENT ON INTERNAL ACCOUNTING CONTROLS, 45 FED. REG. 40,135, 40,139-40,143 (1980).

69 *See* REPORT OF INVESTIGATION AND STATEMENT SETTING FORTH FRAMEWORK FOR EVALUATING COOPERATION IN EXERCISING PROSECUTORIAL DISCRETION, SEC RELEASE NO. 44969 (Oct. 23, 2001), and accompanying Press Release No. 2001-117.

70 Indulging the pressure may be an alternative description to embracing the disguise of state control by cloaking it in the garments of free enterprise. A fully-developed position on that subject is beyond the scope of this Article.

71 U.S. SENTENCING COMMISSION, AN OVERVIEW OF THE FEDERAL SENTENCING GUIDELINES (Nov. 1998); *see* JEFFREY KAPLAN ET AL., COMPLIANCE PROGRAMS AND THE CORPORATE SENTENCING GUIDELINES: PREVENTING CRIMINAL AND CIVIL LIABILITY (1993).

72 SENTENCING GUIDELINES FOR CORPORATIONS, § 8C2.5(f).

sentences.73 This Manual does not specify what constitutes sufficient controls or programs, a common characteristic of legal materials concerning internal control.74 It does, however, furnish two critical attributes used in determining whether to recognize a program in exercising prosecutorial discretion: (1) the program's design integrity as a directive force in preventing or detecting violations and (2) the program's enforcement by the corporation.

2. State

State law also seems to encourage some corporate internal controls. The early case arising from the price-fixing scandals in the electrical equipment industry in the 1970s, *Graham v. Allis Chalmers,75* defined a limited scope of a corporation's or board's obligations to employ internal controls, mooting any incentive effect. The price-fixing shenanigans were engineered by middle-managers in one of the company's numerous divisions. No system of corporate espionage was required, the court famously declared, except where information comes to a board's attention, giving directors notice of criminal activity afoot within the corporation.

With internal controls now functionally required by federal securities laws, there is reason to believe a state court would call for corporations to maintain at least some degree of surveillance. Having such systems comfort a board that its decisions will survive judicial scrutiny, constituting incentives to develop controls. The widely-publicized *Caremark* case involving widespread violations of Medicare rules supports this assessment.76

Caremark provided patient-care and managed-care services, generating substantial revenues from third-party payment schemes such as Medicaid and Medicare. Payments were subject to the Anti-Referral Payments Law (ARPL) prohibiting health-care providers from exchange arrangements designed to induce referrals of Medicaid or Medicare patients. Caremark had numerous agreements with providers for consulting and grant-making and these providers in exchange recommended Caremark services to such patients, violating the ARPL.

Caremark pled guilty to violations, paid criminal fines, and made civil restitution. Shareholder derivative suits followed against directors, who proposed a settlement. Reviewing it, Chancellor Allen discounted the continuing vitality of *Graham*. He concluded that boards have 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 cause by non-compliance with applicable legal

---

73 U.S. DEPARTMENT OF JUSTICE, U.S. ATTORNEY'S MANUAL, Title 9, Criminal Resource Manual, 162 Federal Prosecution of Corporations.

74 *See infra* Part II.B.

75 188 A.2d 125 (Del. 1963).

76 *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996). *Caremark* may be seen as a response to the federalization of corporate law through the backdoor of internal controls. *Cf*. Renee Jones, *Rethinking the Federalism Debate in Corporate Law*, 29 J. CORP. L. ___ (forthcoming 2004).

standards."77

The court's statement of the law is tougher than the *Graham* standard, requiring some affirmative board monitoring for compliance even absent notice of potential wrongdoing. On the other hand, based on the alleged facts, the court thought it was unlikely that the Caremark board had violated even the higher standard.78 In the case's aftermath, however, internal controls became an essential means of making boards comfortable that they had met their monitoring-for-compliance duties, whatever they are.79

Some legal materials distinguish between internal controls and compliance programs (for example, both the OSGs and US Attorney's Manuals do so). But the distinction is not always followed when questions of liability arise. Controls and compliance are treated as an integrated information system of some kind and boards responsible for maintaining the integrated whole. This treatment follows from a combination of COSO's collapsing of the categories and the development of the board-monitoring model of corporate governance which envisions general obligations on boards to maintain both internal financial controls as well as compliance programs.80 Failure exposes corporate boards and sometimes corporations to liability to shareholders and non-owners, furnishing powerful incentives to adopt them all.81

The Caremark opinion exemplifies the point.82 It makes no distinction between financial controls and compliance controls. In fact, it classifies a broad category expressly including both, treating financial compliance in a string along with environmental, employee and product safety.83

---

77 *Caremark*, 698 A.2d at 970.

78 Leading corporate law codifiers increasingly see these developments driving creation of a separate "duty of oversight" as part of the general duty of care. *E.g.,* JEFFREY D. BAUMAN, ELLIOTT J. WEISS & ALAN R. PALMITER, CORPORATIONS: LAW AND POLICY (5th ed. 2003), at 612-637.

79 *See* H. Lowell Brown, *The Corporate Director's Compliance Oversight Responsibility in the Post* Caremark *Era*, 26 DEL. J. CORP. L. 1 (2001). For an analysis of what they are, see *infra* Part IV.A.

80 Professor Dooley provides a detailed history of the drafting process through which the ALI Corporate Governance Project of the late 1980s and early 1990s sought precisely this result, an effort to functionally overrule *Graham* and to require boards, as an integral part of their duty of care, to establish legal compliance systems "of the same rank as accounting and auditing systems." Dooley, *supra* note 43, at 485.

81 The distinctions are useful at every level, however, from who should design what controls, test them, audit them, and what liability should follow, if any, and to whom. *See infra* Parts IV.B-C and Appendix B.

82 The opinion's precedent value may be limited since it arose in the narrow procedural context of approval of a proposed settlement, on alleged facts the court indicated would have been susceptible to a motion to dismiss. But it is a characteristically thoughtful opinion of Chancellor Allen's and understood to represent a significant statement of current law.

83 *Caremark*, 698 A.2d at 969 (noting a prevalent tendency of criminal law enforcement "to assure corporate compliance with external legal requirements, including environmental, *financial*,

The opinion emphasizes an integrated "information and reporting system" directed toward "*both* the corporation's compliance with law and its business performance."84 The proposed settlement was triggered by an alleged compliance failure, so collapsing it into a framework that includes financial controls is significant, providing coextensive incentives for all control types.

B. Limited Substantive Content

Despite substantial mandates and incentives to use internal controls, there is little specification of their required content, either for financial or compliance controls. A unifying thread of many control regimes, however, is the development of employee handbooks and appointment of chief compliance officers. The availability of these broad-brushed mandates in control prescriptions reinforces the appeal of this response to particular crises. The simplicity of the directive makes it easier to impose.85

1. Controls

State law cases furnish no directives on control content, sticking to the reticent common law tradition of refraining from blueprinting fiduciary action.86 The OSGs and US Attorney's Manuals speak in general terms of effectiveness, integrity, and enforcement. Even SEC rules don't detail the content of required controls but state broad mandates. For example, SEC rules require registrants to maintain adequate controls to enable registrants to prepare financial statements in accordance with generally accepted accounting principles.87 The SEC followed a similar reticent practice in establishing rules under SOX, citing deference to the unique needs of various business types and the broad range of legitimate corporate culture.88

---

employee and product safety regulations as well as assorted other health and safety regulations") (emphasis added).

84 *Id*. at 970 (emphasis added); *see also id*. at 971 (repeating the phrase "information and reporting system"); *see also Dellastatious v. Williams*, 242 F.3d 191 (4th Cir. 2001) (citing *Caremark* and holding directors satisfy their duty by showing a good faith attempt to create "an adequate corporate information-gathering and reporting system");

85 *See* POWER, *supra* note 7, at 84 (a key appeal of many internal-control protocols, voluntary or mandatory, is their general "lack of organizational specificity").

86 *E.g.*, *Dellastatious v. Williams*, 242 F.3d 191 (4th Cir. 2001) (citing *Caremark* and holding directors satisfy their duty by showing a good faith attempt to create "an adequate corporate information-gathering and reporting system"); *In re Baxter Int'l Inc. Shareholders Litig*., 654 A.2d 1268 (Del. Ch. 1995) (pre-*Caremark* case) (dismissing a complaint on grounds its claims of director culpability were conclusory).

87 Securities Exchange Act, Rule 13(b)(2)(B).

88 *See* SECURITIES AND EXCHANGE COMMISSION, FINAL RULE: MANAGEMENT'S REPORTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND CERTIFICATION OF DISCLOSURE IN EXCHANGE ACT REPORTS, 17 C.F.R. 210 (June 5, 2003), at 9.

Other administrative agency guidance on compliance controls is likewise general. Consider, for example, the Occupational Safety and Health Administration (OSHA)'s "Star Program." Businesses adopting safety and compliance systems exceeding minimum standards set by OSHA qualify for reduced levels of OSHA oversight.89 To be admitted to this deference-for-controls deal, businesses must (1) adopt workplace safety programs that include hazard assessment and control; (2) furnish OSHA with reports detailing self-inspections, accidents and employee hazards; and (3) complete an onsite OSHA inspection.

International standard-setters have developed more detailed guidance concerning environmental controls. The relative detail compared to US control materials may be due to the comparatively weaker deregulatory philosophy in most other countries. Even at this level, however, standards show deference. One standard promulgated by the International Standards Organization (ISO) provides guidance on designing environmental management systems.90 It demands that senior management commit to environmental performance standards.

Emphasized are periodic reviews of operations, products, and services to identify significant environmental impacts, as well as legal and contractual obligations that shape environmental practices. The standard prescribes documenting and setting measurable performance targets and objectives, establishing a management program and resources to pursue these objectives. It also calls for employee training protocols, defines individual employee roles, and details consequences for violations. The protocol emphasizes the need for communication and monitoring procedures, as well as periodic management reviews.91

2. Audits

Regulatory guidance routinely addresses the testing of internal controls, increasingly calling on outside auditors to verify system integrity. While intended to promote the effectiveness of control, one risk of such control-plus-audit programs is to encourage creation of controls than can be tested rather than controls more likely to be effective. These are not necessarily the same controls.

The EPA offers its version of a high-quality audit program that calls for explicit top management support for auditing and commitment to follow-up on audit findings, coupled with an

---

89 Richard S. Gruner, *General Counsel in an Era of Compliance Programs and Corporate Self-Policing*, 46 EMORY L.J. 1113, 1131-32 (1997).

90 INTERNATIONAL STANDARDS ORGANIZATION, ENVIRONMENTAL MANAGEMENT SYSTEMS SPECIFICATION WITH GUIDANCE FOR USE (ISO 14001) (1996) ("ISO 14001"); *see* Donald A. Carr & William L. Thomas, *Devising a Compliance Strategy Under the ISO 14000 International Environmental Management Standards*, 15 PACE ENVT'L L. REV. 85 (1997).

91 Numerous companies publish statements relating to such matters, often emphasizing environmental policy but extending to a broad range of social responsibility issues. *See, e.g.*, STATEMENT OF FORD MOTOR CO. (Aug, 2002).

auditor operating independently of the internal auditing department.92 These professionals are to be supported by adequate team staffing and have proper audit training. Also required are explicit definitions of the audit program's objectives, scope, resources, and frequency; a process which collects, analyzes, interprets, and documents information sufficient to achieve audit objectives; and a process which includes specific procedures to promptly prepare candid, clear, and appropriate written reports on audit findings, corrective actions, and schedules for implementation.

In the case of the Medicare program, the Office of Inspector General (OIG) for the Department of Health and Human Services plays a leading role in articulating internal control and audit guidelines. It became particularly active in the 1990s in the wake of health-care fraud scandals like those at the heart of the *Caremark* case.93 Among the initiatives were corporate integrity audits (CIAs), mandatory exercises imposed on non-compliant companies reminiscent in content of the voluntary private ethics audit pioneered by KPMG in the 1980s. Ordained by the OIG beginning in 1994, these remedial programs impose integrity obligations on corporate health care providers. Several hundred hospitals and other health care providers participate.

As with most compliance programs, health care CIAs have grown with age. Compliance measures now routinely mandate designation of a compliance officer and/or committee; developing written standards and policies; implementing comprehensive employee training and screening programs; and preparing periodic reports. Tailoring to special entity needs is common, as is establishing mechanisms to conduct independent audits of the program. Enforcement and penalties result from noncompliance, including exclusion from the Medicare program.94

3. Cycles

Articulations of the required content of internal control and audits of them become a feedback loop. The occasional variations in articulated requirements most often simply extend the loop in slightly different directions. For example, interpretations of the FCPA suggest that it is necessary to conduct due diligence checks of "agents, partners, or consultants of the company,"95

---

92 ENVIRONMENTAL PROTECTION AGENCY, ENVIRONMENTAL AUDITING POLICY STATEMENT, 51 FED. REG. 25,004 (July 9, 1986).

93 *See* Lewis Morris & Gary W. Thompson, *Reflections on the Government's Stick and Carrot Approach to Fighting Health Care Fraud*, 51 ALA. L. REV. 319, 341-344 (1999).

94 The OIG also recommends compliance guidelines for health-care service providers. It publishes compliance guidance notices in the Federal Register, tailoring them for various industry segments, such as hospitals, clinical laboratories, home health agencies, third-party medical billing companies, hospice providers, medical equipment suppliers, nursing homes and Medicare+Choice organizations. The guidance draws on the OSGs and suggests: (1) written policies, (2) compliance officers, (3) employee training and education, (4) effective lines of communication, (5) enforcement through discipline, (6) audits to monitor compliance, and (7) curative procedures. *Id*., at 346-348.

95 *See, e.g.,* Gary Eisenberg*, Foreign Corrupt Practices Act*, 37 AM. CRIM. L. REV. 595 (2000); Kari Lynn Diersen, *Foreign Corrupt Practices Act*, 36 AM. CRIM. L. REV. 753 (1999); Lynne Baum, *Foreign Corrupt Practices Act*, 35 AM. CRIM. L. REV. 823 (1998).

suggestions echoed in the ISO guidelines.

In turn, the OSGs draw on the FCPA, which specifies the standard content for a corporate compliance program: a code of conduct, a protected means for employees to report violations, employee training and screening, and penalties for violations. All these examples show the standard internal control specification theme: broad, abstract mandates covering similar general ground intended mainly to promote cultural and psychological awareness of corporate policy and effectiveness.

SOX follows the tradition of articulating broad abstract principles that substantially replicate existing standards. SOX requires CEO/CFO certification of internal financial control system design, testing and integrity, but never says what those things mean or require. Auditors are required to test the design and effectiveness of internal controls over financial reporting, but details are not given.96

Guidance subsequently promulgated by auditing standard-setters concerns the methodology of the examination and attestation rather than a specification of the required controls.97 The SEC extends the mandate to its newly-created category of "disclosure controls and procedures" but likewise leaves registrants to interpret platitudes rather than adopt particular procedures.98 SOX requires disclosure of assessments of internal controls and an internal control report, again without saying what controls mean or require.

PATRIOT's regulations are somewhat more directive.99 Whereas most primary legal materials spawning internal controls are regulations whose administration encourages or implicitly requires controls, many PATRIOT provisions specifically instruct entities to adopt specified controls. Many of these internal-control mandates copy and extend existing special rules traditionally applicable to banks. Controls mandated under the Bank Secrecy Act require reporting currency transactions exceeding $10,000 and suspicious activities (those that tip an informed banking employee to the possibility of illegal activity, especially money laundering).100 PATRIOT extends like requirements to other members of the financial services industry.

PATRIOT imposes compliance controls on the financial services industry akin to the additional layers of external audit traditionally imposed on banks by banking regulators. Imposed controls include "know your customer" rules, mandatory screening for suspicious ones, and

---

96 The regulations contain broad statements of standards that echo those found in elementary accounts of auditing practice. This is unsurprising, since professional auditing standards were the primary source of the FCPA. *See supra* note 19. For discussion of standards articulated by the Public Company Accounting Oversight Board (PCAOB) under SOX, *see infra* Part III.C.

97 *See infra* Part III.C.

98 SEC, FINAL RULE: MANAGEMENT'S REPORTS ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND CERTIFICATION OF DISCLOSURE IN EXCHANGE ACT REPORTS, 17 C.F.R. 210 (June 5, 2003).

99 *See infra* Appendix C.

100 *See, e.g.*, 12 C.F.R. § 208.62, 31 C.F.R. § 103.22; 31 U.S.C. § 5313.

reporting on them. Examination audits include testing of compliance procedures and internal controls. Examiners identify areas of compliance or control vulnerability and banks respond by making remedial recommendations. Since 1999, federal bank regulators have included anti-money laundering compliance and examination procedures in their reviews,101 practices PATRIOT extends to non-bank members of the broadly-defined financial services industry.

C. Procedural Shape

Corporations may find legally-mandated controls appealing. Internal controls can be designed to mediate the tension between the need to repose trust and discretion in employees on the one hand, and the imperative to supervise and impose checks-and-balances on the other, a method the Soviets and Ronald Reagan famously characterized as "trust but verify."102 Mandatory controls serve a sanitizing function for modulating the trust-suspicion trade-off. Controls mandated by law may be imposed by the corporation on employees without expressing a particularized mistrust of them.

1. Abstract Accountability

Uniting the forces that make internal controls appealing, especially as responses to pending crises, is a quest for accountability. Perceived balance indicates more need for verification and less room for trust. If everyone could be counted on to do the right thing, no controls would be necessary. Entire markets are operated on this premise, participants relying on the spontaneous coordination of self-interested actors for the production, distribution and exchange of goods and services. Some companies rely on comparable forces. The deep mechanism at work in such settings is trust (competition operates as well). One party can count on the other to do what is called for, implicitly or explicitly.

When doubt arises concerning the reliability of participants, checks must be imposed to permit interaction to proceed. The mediation is a characteristic of governance mechanisms in a wide range of settings. Lenders lend but require borrowers to maintain designated financial performance ratios and accept periodic monitoring. The structure of the U.S. Constitution is anchored in rational skepticism of those wielding political and juridical power. The entire field of corporate governance is devoted to addressing the risk that owners face when reposing trust in managers possessing corporate control. Internal controls are a sub-species of that governance structure.

In a perfect world, a corporation could count on all employees to follow policy and leave

---

101 U.S. DEPARTMENTS OF JUSTICE & TREASURY, 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 46. Bank compliance systems are required by various provisions of Title 12 of the U.S. Code.

102 Reagan often said in the context of brokering arms talks with the Soviet Union, "trust but verify" (a translation of the Russian equivalent, *doveryai no proveryai*). *See The Summit*, N.Y. TIMES, Dec. 9, 1987, at A21 (transcript of remarks of President Reagan and Soviet Union General Secretary Mikhail Gorbachev at signing of nuclear non-proliferation treaty).

everything to trust. In the actual world, employees stray, become careless or larcenous, and the corporation needs some mechanism to curtail departures. The mechanism calls for checks that achieve the goal of compliance without destroying the benefits of trust that drive achievement of corporate objectives such as product innovation, market expansion, and profit generation.

The unique character of internal controls is thus the injection of suspicion into the trust relationship. The company extends to the employee a measure of trust, but is accompanied by some suspicion that the trust is misplaced. Suspicion becomes the central feature of internal controls, a view that explains why the 1960s court in *Graham* derided such systems as constituting corporate espionage. One difference between the pre-*Graham* era and that prevalent today is a difference in the mix of trust and suspicion in corporate culture.103 A key difference is how contemporary controls bear negative or preventive goals rather than positive qualities of achieving corporate objectives.

In theory this justifies internal controls that are designed to kick in when suspicion is aroused—exactly what the *Graham* court held. More weakly, this view of internal controls justifies triggering controls when suspicion is merely justified—pretty much the *Caremark* stance. Contemporary financial and compliance controls work the *Caremark* way. Both stiffen when temptation increases, as where employees must obtain multiple approvals for disbursements greater than certain amounts or where enhanced scrutiny is applied by airlines to passengers buying one-way tickets with cash and carrying no luggage or by banks to depositors rapidly moving recently deposited cash to different accounts. They bear a preventive quality.

2. Cooperation by Procedure

A wonderful mechanism for inserting controls without straining the trust relationship unduly is to characterize the programs as cooperation protocols rather than command models. Mandatory and voluntary controls can both be designated in this way. Publishing ethics codes, appointing compliance officers, and producing a battery of manuals and training programs put employees on the same page as the organization. Employees become leaders in a process, rather than subordinates bending to the will of the corporate hierarchy.104

These mechanisms are deliberate reorientations of the trust-suspicion model of internal controls. They dispel concern about employee backlash from lack of employer trust. The approach replaces suspicion with cooperation. It is akin to parallel theories of regulation envisioning the corporation as a cooperator with regulatory authorities. The strategy enhances the probable power of the employee in the program substantially.

These strategies are most likely to be effective in those areas where employees naturally

---

103 Others include those noted in Part I.C., including deregulatory drives, corporate governance evolution and auditing profession diversification.

104 *See* Stephen C. Hansen, *Designing Internal Controls: The Interaction between Efficiency Wages and Monitoring*, 14 COTEMP. ACCTNG. RES. (Spring 1997).

share the employer goal. Employee sympathy is most likely greatest in the case of extreme public policy functions. Leading examples are anti-money laundering and anti-terrorist financing protocols. They enable the employee to believe in the program and share a sense that "we" are the employee-employer and "they" are the outsiders bent on doing it and its constituents harm.

Presenting controls in this cooperative spirit is increasingly popular, and explains the increasing appeal of this sort of internal control to solve a range of problems. This explains OSHA's Star Program, for example, as well as the embrace of employee training protocols by the ISO, the HHS and others.

Employees see themselves as members of a team working together to assure integrity and compliance. This theory emphasizes the culture of compliance as a company-wide characteristic, not merely a tone at the top but the tone all around. Boards can use such devices as a way to coordinate the effort of labor to balance its interests with those of shareholders.105 This spirit of cooperation is ultimately what makes internal controls acceptable as a norm in regulatory circles, what enables Congress to pass legislation without upsetting the regulated.

These employee-sensitive controls also suggest inherent limits on controls. The traditional team production model of employee cooperation is strong though nothing in it guarantees that employees will not fail or cheat. Adding layers of controls to the model does not change that fact, though it can lead people to believe it does. This is particularly so when the controls are designed in ways that can be audited, as the procedural shape of controls tend to be—auditors can read manuals, attend training program sessions and review proceedings triggered by whistleblower reporting. Control audit-ability promotes control appeal to the auditing profession. It advocates these tools despite their professional emphasis and recognition of their inherent limits—matters discussed next.

III. CONTROL LIMITS: AUDIT VIEWS

The auditing profession is sprawling and the place of internal controls concerning financial and non-financial matters within it requires a preliminary contextual note. Standard treatments of the auditing profession distinguish between two broad types of services it renders. One is consulting, two-party arrangements exemplified by services rendered directly for clients such as business valuation, litigation support, system design, actuarial, and tax.

The other type is assurance engagements. These are three-party arrangements offering comfort as to the quality of certain information. They include a range of matters, from verifying assertions a business makes about itself to consumers (such as testing products) to data a company makes about its financial reporting (such as comfort letters to underwriters of its securities and other services involving such "agreed-upon procedures"). These general attestation services are governed by standards set forth in the auditing profession's Statement of Standards and Attestation

105 *Compare* Margaret M. Blair & Lynn A. Stout, *A Team Production Theory of Corporate Law*, 85 VA. L. REV. 247 (1999); *with* Alan J. Meese, *The Team Production Theory of Corporate Law*, 43 WM. & MARY L. REV. 1629 (2002).

Engagements (SSAE) No. 1.106

The family of attestation services includes audits, which in turn are typically distinguished into three sub-categories. The most common are financial audits, the practice of which is governed by specific standards articulated as generally accepted auditing standards (GAAS) geared toward stating an opinion as to the fair presentation of financial statements and their compliance with generally accepted accounting principles (GAAP). Another category is operational auditing, typically conducted by an organization's internal auditors, and addressing matters relating to the effectiveness of the organization's operations. The third are compliance audits, traditionally performed mostly for non-profit organizations and governmental entities, but increasingly being undertaken in a broad range of areas for a variety of client types.

SOX requires auditors to attest to assertions management now must make concerning the effectiveness of a company's controls over financial reporting. Auditors have greatest experience with such financial controls. These were created in part to enable them to provide assurance concerning financial statement assertions without need for verifying every transaction. Though even in this exercise controls have limited efficacy, auditor experience with them provides ability to assess these limits with some degree of reliability. When auditors extend their traditional audit tools to investigate and attest to assertions relating to policy controls, limits multiply.107

A. Audit Risk

All attestation engagements are designed to provide reasonable assurance as to the covered assertions. None provides absolute assurance. In other words, risk cannot be eliminated. The best a practitioner can do is to hold risk to a relatively-low but statistically-acceptable level. Auditors divide risk into various classifications.

1. Attestations

At the broadest level, attestation risk is "the probability that an attestor may unknowingly fail to modify a written conclusion about an assertion that is materially misstated."108 More focused is the definition of audit risk when applied to a financial audit: "the probability that an auditor may

---

106 CODIFICATION OF ACCOUNTING STANDARDS AND PROCEDURES, STATEMENT OF STANDARDS AND ATTESTATION ENGAGEMENTS (SSAE) No. 1 (Am. Inst. Of Certified Pub. Accountants). A foundational principle of this and other attestation standards is the concept of independence. The principle usually means that an auditor engaged to perform three-party attestation services may not also be engaged by the same client to render two-party consulting services. *See* SOX, § 201 (amending 15 U.S.C. § 78j-1); 17 C.F.R. § 210.2-01(c)(4)(i)-(ix) (2002).

107 Auditors increasingly rely upon the opinions of experts in the new fields they audit, such as actuaries, land surveyors, engineers and others. In an environmental audit, for example, the auditor's job may entail checking the credentials of and procedures used by an emissions expert, rather than testing emissions directly.

108 RICCHIUTE, AUDITING, *supra* note 45, at 45.

unknowingly fail to modify an opinion on financial statements that are materially misstated."109 Within each category, practitioners distinguish between three types of risk:110

- Inherent risk is the susceptibility of an assertion (such as an account balance in a financial audit) to error that could be material, assuming there are no related internal controls.
- Control risk is the likelihood that error could occur and not be prevented or detected by internal controls.111
- Detection risk is the likelihood that error could occur and not be detected by the auditor's procedures.

Audit or attestation risk is the product of the three risk types. The relationship among these distinctive sorts of risk can be expressed in a formal model:

$$AR = IR \times CR \times DR$$

Audit practitioners evaluate inherent risk (*IR*) and control risk (*CR*) and then solve this equation for an acceptable level of detection risk (*DR*). Rewriting the equation in these terms yields:

$$DR = AR / (IR \times CR)$$

This expression reflects detection risk (*DR*) as the dependent variable. Controlling for it entails mastering inherent risk and control risk. Viewed this way the issue is how to establish and interpret what an acceptable level of detection risk (*DR*) is. Its key function is to drive the scope of an audit plan measured by the amount of evidence required to express an opinion.

The opinion is a function of the level of confidence one requires to give it. That confidence level (*CL*) can also be formalized, as:

$$CL = 1 - DR$$

The confidence level is the likelihood that the audit procedures did not fail. The requisite confidence level in turn hinges on concepts of materiality. The standard of materiality used in the auditing profession bears a similarity to the standards used in both securities law and financial accounting. All treat as material matters that a reasonable person would consider important in

---

109 *Id*.

110 These definitions of risk and the accompanying formula expressing relations among them are set forth in *id*. at 46-48.

111 The general attestation standards set forth in SSAE 1 do not focus on internal controls, though in practice any attestation exercise considers them relevant to the engagement. On the other hand, GAAS is explicit with respect to internal controls. These standards require an auditor to understand an organization's internal controls and to use that understanding in planning the audit.

making a decision based on some information base.112

Planning an engagement requires a preliminary estimate of materiality (for example, the maximum amount by which financials could be misstated and still not make the auditor decide reasonable people would find it important). The auditing profession publishes decision aids relating audit risk to materiality and implied requisite audit effort. It also invokes various rules of thumb.

The commonest quantitative rule of thumb in financial auditing relates to an item's effect on net income. Effects less than 5% are seen as unlikely to be material and those greater than 10% are seen as likely to be material. This rule of thumb is not taken to reveal bright lines, however, and instead is seen simply as a starting point for more textured, qualitative analysis.113 Examples of qualitative factors are loan-covenant compliance which on their own may not trigger a percentage-of-income effect but could spell risks of default, cross-default and related financial difficulties.

In the preliminary stage of an engagement, auditors design tests of controls. These are audit procedures to assess the efficacy of internal controls to prevent or detect material misstatements. They address control risk (discussed further in the next section). Evidence from these tests defining control risk is in turn used to set an acceptable level of detection risk. This is done by executing substantive tests.

Substantive tests are audit procedures designed to detect material misstatements or to identify assertions likely to contain material misstatements. They address detection risk. Substantive tests are of two types: (1) tests of detail are designed to detect material misstatements in accounts and (2) analytical procedures are evaluations of data drawing on comparisons such as in relevant trends, baselines or forecasts.

2. Audit Limits and Auditor Skepticism

Not only are audits imperfect in detecting all error or misstatement, they are not invariably capable of distinguishing between errors and deception. Corporations are exposed to varying risks of error and managers have varying incentives to cheat. Managers have principal responsibility for designing internal controls and varying abilities to override them, with consequent implications for the probable error rate in audits. Auditors must decide whether to investigate for deception, using

---

112 *E.g.*, SEC Regulation S-X (average prudent investor ought reasonably to be informed of); *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438 (1976) (reasonable person would have attached importance in deciding); Financial Accounting Standards Board (reasonable person relying would have changed mind or been influenced). Practitioners posit an inverse relationship between audit risk and materiality (for example, the risk of sizable misstatements is low while the risk of small misstatements is high). RICCHIUTE, AUDITING, *supra* note 45, at 50. Put otherwise, broader definitions of materiality or less toleration for audit risk indicates an expanded audit plan (more or better procedures).

113 *E.g.*, SEC Release 1999 (cautioning financial auditors of SEC registrants against undue reliance on such rules of thumb).

strategic decision-making triggered by the presence of evidence that discrepancies are too high to be attributable to error alone.114

Assessing the risk environment driven by factors of materiality and risk sets the stage for gauging the scope of evidence required to justify opining on an assertion. Deep epistemological challenges round out the environment auditors face in certifying client assertions. Acquiring requisite evidentiary quantity and quality in turn entails a host of judgments. Many sources of knowledge are available to support achieving desired confidence levels. Each contributes in different ways. Examples are the examination and practical results of testing and review, managerial testimony, reasoning from recognized principles and relationships, and intuition. These sources of knowledge complement each other, but none is perfect and even taken together risks of knowledge gaps remain.

Auditors seek to seal the potential gaps in assembling requisite knowledge bases by adopting the fundamental auditing standard of professional skepticism. Auditors approach the assessment and investigation process by probing. They ask questions of managers and employees, seek verification from multiple sources, and willingly engage in a second-guessing of managerial judgments on a variety of matters. The skepticism applies to both the processes and the outputs.

B. Control Risk

Auditors see internal controls as a factor in assessing attestation risk. They posit an inverse relationship between control quality and audit scope: superior controls demand an audit of lesser scope and intensity; weaker controls demand a more intense and expansive audit. For example, a high-quality internal financial control system can reduce the required scope of an audit while low-quality systems indicate a broader audit plan (all other things being equal). But while audit planning thus requires an understanding of controls as a source of measuring and minimizing attestation risk, control quality cannot be measured by volume. More controls are not necessarily better or more effective.

Consider the audit risk formula described in the previous section. The model separates the risks but they are in fact related to one another.115 Suppose two companies embracing identical internal control systems but bearing different inherent risks (one sells only ice cream in the US and the other sells a range of consumer products in 100 countries). Control risk in isolation appears to be the same. But given the different inherent risk, the identical control systems indicate greater control risk in the complex company than in the simple company.

Until SOX, reports on internal controls for SEC registrants were required only when tests of

---

114 *See* Dennis H. Caplan, *Internal Controls and the Detection of Management Fraud*, 37 J. ACCT. RES. (Spring 1999).

115 *See* Richard Dusenbury, Jane Reimers & Stephen Wheeler, *Inherent Risk and Control Assessments: Evidence on the Effect of Pervasive and Specific Risk Factors*, 19 AUDITING: A JOURNAL OF PRACTICE & THEORY (2000).

controls revealed significant deficiencies (called reportable conditions). This reporting remains the case for non-SEC registrant reviews of internal controls. Thus there remain two different types of reports on internal control: audit (reportable conditions) and attestation (full test of all controls and opinion on management's assertions concerning control effectiveness, discussed in the next section). Either way, the standard auditor's opinion letter on these matters emphasizes the "inherent limitations" of the exercise.116

These limitations are revealed in the emphasis auditors place on the complex definition of internal controls. Auditors particularize the sorts of definitions drawn in Part I.A from sources such as the 1992 COSO report. They emphasize limiting elements.117 Internal controls are *processes* not events and are performed by *people* organization-wide. Both elements imply the possibility of control leakage. This is reemphasized by repeating the ultimate purpose of controls: they are intended to meet designated objectives in ways offering *reasonable* (not absolute) assurance.

Factors influencing the success of these elements of control are environmental and procedural. Environmental factors concern employee attitudes towards and awareness of controls, as well as their actions in light of those perceptions. Procedural matters refer to rules governing authorization/execution of transactions, duty segregation, documentation and recordkeeping, and limiting access to assets and records.

1. Tests of Controls

Tests of controls are performed using attributes sampling plans that test the rate of deviation (or rate of occurrence) from a control characteristic. They therefore differ from the analogous statistical sampling performed in substantive tests which are intended to determine whether particular assertions (such as recorded account balances) are fair.

Either form of sampling in tests of controls (or other tests) creates an additional risk: sampling risk. This can be reduced by increasing sample size. But as with all other risks associated with auditing, sampling risk cannot be eliminated. The best one can do is to invoke recognized procedures of statistical sampling governed by the laws of probability theory.

Apart from these methodological limits to auditor interpretation of control risk, behavioral factors in both internal control design and testing guarantee residual risk. From a control-design perspective behavioral factors add difficulties to designing optimal internal control levels, yielding tendencies that overproduce controls.118 Excessive controls not only raise direct costs, they also complicate control risk assessment.

---

116 *E.g.*, RICCHIUTE, AUDITING, *supra* note 45, at 200.

117 *See generally* AICPA, PROFESSIONAL STANDARDS § 36 (1990), Standard 53 (SAS 53).

118 *See* Donald C. Langevoort, *The Behavioral Economics of Corporate Compliance with Law*, 2002 COLUM. BUS. L. REV. 71; Robert Prentice, *The Case of the Irrational Auditor: A Behavioral Insight into Securities Fraud Litigation*, 95 NW. L. REV. 133 (2000).

Control benefits are probably lower than managers routinely think due to biases extending from the moment supervisors hire new employees to the period when they test control systems. For example, supervisors believe they are better at making hiring decisions than they really are. They become more motivated to believe this after a hiring has been made. Managerial evaluations of internal controls relating to employee qualities and training therefore likely overrate the systems due to the bias of self-review.

Behavioral factors also suggest that the costs of controls are likely to be under-estimated. Some costs can be measured directly, such as the salaries paid to compliance officers and the production costs of training programs and manuals. Harder to measure are the time spent consulting those manuals and codes, their effect on employee decision-making and risk-taking, and the overall costs of a culture incrementally weighted more towards suspicion and less towards trust.

The auditing perspective on control risk may lead to excessive controls. Among systematic audit biases are order effects, including saliency bias. This refers to the meanings assigned to different sorts of information as a function of when during a process they are received. Auditors often address this bias using conservatism. 119 Auditors insist on greater controls, more control testing, or other exercises that attempt to wrestle with control risk to a fuller extent than warranted under the established confidence level. But while such conservatism trained on control levels may produce more controls, the combination of biases does not necessarily equate to reducing control risk.

2. Inherently Leaky Controls

While all internal controls complicate assessing audit risk, automated controls amplify the challenge. Where substantial information supporting financial statement assertions is in electronic form, for example, it may not be feasible to limit detection risk to acceptable levels by conducting substantive tests of the assertion. It may be necessary to obtain evidence about the effectiveness of the design and operation of the controls to reduce the level of assessed control risk.120

Internal controls enhanced by information technology thus do not reduce audit risk, but potentially increase it. Understanding the environment requires understanding the automated systems used to generate results. For financial controls, this encompasses procedures relating to

---

119 *See, e.g.,* Gary S. Monroe & Juliana Ng, *An Examination of Order Effects in Auditors' Inherent Risk Assessments* (SSRN.COM); Brenda H. Anderson & Mario J. Maletta, *Primacy Effects and the Role of Risk in Auditor Belief-Revision Processes*, 18 AUDITING: A JOURNAL OF PRACTICE & THEORY (Spring 1999).

120 STATEMENT OF AUDITING STANDARDS (SAS) NO. 94, THE EFFECT OF INFORMATION TECHNOLOGY ON THE AUDITOR'S CONSIDERATION OF INTERNAL CONTROL IN A FINANCIAL STATEMENT AUDIT. This amends Statement of Auditing Standards (SAS) No. 55, Consideration of Internal Control in a Financial Statement Audit (incorporating and expanding SAS No. 80, Amendment to Statement on Auditing Standards No. 31, Evidential Matter (AICPA, Professional Standards, vol. 1, AU § 326.14)).

entries made to the general ledger, particular journals for standard and nonrecurring items, and adjustments relating to consolidation, reclassifications and the like. For compliance controls, similar exercises include testing baggage screening protocols in the aviation industry, emissions measurements for environmental controls, and reporting systems within financial institutions designed to capture suspicious transactions.

For both types of controls, special expertise may be necessary to achieve requisite understanding.121 As a result, testing controls in an audit does not displace need to conduct substantive tests in various areas where controls are unlikely to work. These include areas involving estimation and valuation, where controls simply cannot be well-designed to prevent leakage.

Such additional substantive testing is often applied to high-risk areas, such as receivables/sales and inventory/cost-of-goods-sold for financial audits or security at nuclear power plants in compliance audits. General audits in these areas are subject to substantive testing including analytical procedures whatever level or quality of controls governs them. Thus customers are called to confirm receivables balances and warehouses are inspected to confirm inventory levels. These are typically superior tests than testing related controls. A clean audit, whether of financial or compliance matters, is not and cannot be a confirmation that controls are effective, though discovered misstatements can suggest control deficiencies.

Consider the inherently leaky controls in *Caremark*. Caremark's internal controls appear to have been state-of-the-art. It published an employee guide governing contractual relationships with clients, reviewed it annually, and published numerous revised editions. The policy prohibited what relevant law prohibited. Internal controls to prevent violations included policies requiring regional officers to approve contracts arranged by employees under their supervision. It used an internal audit plan to promote compliance and ethics. Its outside auditor tested these and found no material weaknesses in the controls. It had an Audit and Ethics Committee, a compliance officer, and other policies requiring various home office approvals of field employee disbursements and agreements.

Despite all this, two company employees along with various third parties were indicted for violating the law and engaged in other acts in violation of company policy and eventually settled their cases. Contributing to the cracks these people slipped through were ambiguities in both the law and the employee manuals, making it somewhat unclear whether some sorts of arrangements were covered.122 But since the controls were state of the art, the court rightly concluded that there was

---

121 Consider Electronic Data Interchange (EDI) systems that automate erstwhile manual processes to manage and control a corporation's transactions through computerized systems. EDIs have proliferated throughout the global business world, becoming a standard practice. Specialized internal controls are necessary to assure EDI integrity and specialized audit techniques are necessary to test those controls and thus verify EDI system integrity. Catherine Hardy & Robert Reeve, *Electronic Data Interchange (EDI) and CIS Audit: A Study of the Impact of EDI on CIS Audit Procedures* (SSRN.COM).

122 *See infra* Appendix B.

"no substantial evidentiary support in the record" to hold directors personally liable.123

C. Auditing Control

Auditing of assertions by navigating an internal control environment is complicated but entails only a partial encounter with all controls. This is an additional limit on auditors' ability to confidently attest to assertions with 100% conviction. As if to overcome this limit of internal controls, accompanying their expansion in the past few decades has been an expansion of auditing to test them fully.

Auditing is increasingly used to generate comfort in a wide variety of activities, such as environmental operations, employee relations, and compliance with regulatory requirements.124 Under pressure due to periodic series of heavily-covered corporate scandals, from the 1970s to today, corporations have been forced to enhance their internal governance systems.

These changes in governance have not only led to the creation of a wide variety of internal controls, they have increased the need for independent parties to audit their effectiveness and integrity. The increasing appeal of internal controls as a policy option is thus accompanied by an increasing appeal of audit as a policy option. The paradox here is that the appeal of audit as a policy option is stoked by the decline of internal controls as a failsafe.

1. Financial Control Audits

This is the story of SOX. In the 1970s, the SEC persuaded Congress in response to crisis to pass the FCPA requiring companies to have internal financial controls. In the early 2000s, in response to crisis perceived to originate in internal control failure, the SEC persuaded Congress to pass SOX requiring auditors to audit those internal controls.

In this cycle of control mandates followed by audit mandates, pressure builds on audit to create controls that can be audited. But we just saw that controls do not automatically reduce audit risk and may increase it. For many contexts direct-testing rather than control-testing is necessary. Accordingly, attestations concerning overall control systems tell only a partial story. They cannot speak to the effectiveness of underlying substance over which controls offer no reliable assurance.

---

123 *Caremark*, 698 A.2d at 971. Legal perspectives on control risk discernable from *Caremark* are discussed further in Part IV.A below.

124 The proliferation of internal controls and auditing extends beyond corporations to include many types of organizations, including governmental agencies, hospitals, and universities, and many different types of activities. Public agencies, from rail lines such as Amtrak to schools under competitive pressure from firms such as Edison, have been forced to reinvent themselves along more entrepreneurial lines. Control and audit expansion is the product of heightened calls for accountability throughout society, a broad gauged illustration of suspicion creeping into once trusted institutions.

SOX nevertheless places enormous confidence in controls, requiring officers to certify them and auditors to attest to that certification. This means auditors must fully assess financial controls, not merely test them as part of a general financial audit.

SOX requires officer certifications of the design and effectiveness of internal controls. This move is only a partial sealant. These officer certifications require attestation by those officers *both* that they designed the control systems *and* tested them and found them effective. The risk of self-review bias is self-evident.

To seal this crack, SOX requires auditors to issue a report on an entity's internal control over financial reporting in conjunction with the entity's financial statement audit.125 Preliminary standards for this work were promulgated by the Public Company Accounting Oversight Board (PCAOB). It contemplates two separate audit opinions: a new one on internal control over financial reporting and the traditional one on financial statements.126

The Proposed Standard treats these exercises as integrated. The Proposed Standard also indicates it is possible to give a qualified opinion on one while giving an unqualified opinion on the other.127 This correctly implies that effective controls are neither necessary nor sufficient

---

125 In SOX's wake, audit standard-setters endorsed standards governing this procedure previously established. Both official and unofficial auditing standard-setters did so. The AICPA, the official standard-setter until SOX terminated that status, published a draft proposal in late December 2002, substantially embracing SSAE 10 but adding guidance. The PCAOB, the official standard-setter created by SOX, published its formal endorsement of SSAE 10 in April 2003, and the SEC promptly approved this action. In October 2003, the PCAOB released an elaborate proposed standard articulating governing principles. PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING PERFORMED IN CONJUNCTION WITH AN AUIT [SIC] OF FINANCIAL STATEMENTS (Oct. 7, 2003) (the "PCAOB PROPOSED STANDARD").

Standards applicable to the SOX financial-control-audit are substantially those applicable to any other attestation engagement as articulated in Statement SSAE 10. These may be supplemented by the criteria established by COSO for assessing internal controls. In the case of SOX's financial-control-audit, these requirements include that the auditor of the controls also be the auditor of the client's underlying financial statements. Throughout, directives require planning the engagement, understanding controls, evaluating their design, testing their effectiveness, and opining on them. They also require identifying material weaknesses and deviations.

126 These paragraphs concerning the PCAOB Proposed Standard appear in a different form in the author's public letter to the PCAOB commenting on the Proposed Standard.

127 The seeming incongruity of a qualified control opinion with an unqualified financial statement opinion is possible because a material weakness discovered in internal control can be overcome in a financial statement audit by substantive tests that do not rely upon the control bearing the material weakness. The opposite incongruity of an unqualified control opinion with a qualified financial statement opinion is possible because controls cannot control judgment—controls are processes that may assure following required procedures but cannot assure managers make fair judgments. This is a critical point concerning the limits of controls that is obscured in the control

conditions for accurate financial reporting. If a company can have ineffective controls and fairly-presented financial statements, then effective controls are not necessary; if a company can have effective controls but materially-misstated financial statements, then effective controls are not sufficient.128

The possibility of effective controls producing inadequate financial statements is recognition that controls cannot guarantee accurate reporting. This is inevitable but obscured in both SOX and the PCAOB's Proposed Standard. The Proposed Standard correctly emphasizes inherent limitations of internal controls and the contrast between reasonable assurance, which is possible, and absolute assurance, which is not.129 The Proposed Standard also rightly describes these limits as known features of the financial reporting process and expresses the hope that installing safeguards will "reduce, though not eliminate, the risk" of material misstatements.130 But the particular context of providing an adverse financial audit opinion despite furnishing an unqualified control audit opinion is never mentioned in the Proposed Standard.

It may be true as matters of logic and probability that it is more likely that a company will boast ineffective controls and yet be in a position to present adequate financial statements. But the situation in which effective controls nevertheless yield inadequate financial statements is of greater concern. After all, this is the situation plaguing WorldCom Inc. and other catalysts of SOX.131 The Proposed Standard makes this point in saying that "many frauds resulting in financial statement restatements relied upon the ability of management to exploit weaknesses in internal control" and inferring from this that one goal of improving controls is to reduce the incidence of fraud.132

The possibility that effective controls may nevertheless yield materially inaccurate financial statements is critical to emphasize. To the extent it is deemphasized—as it was in the Proposed Standard—two key points arise. These apply to the SOX-style audit of financial controls as well as audits of all other types of controls.

First, de-emphasis risks inducing users of control-audit opinions into a false sense of complacency that controls assure outcomes, whether preventing fraud, producing fairly-presented financial statements, or other goals. That raises false expectations, an error that will create costs, not benefits, from any control-enhancement regime.

Second, de-emphasis on the possibility that effective controls don't guarantee substantive results is a signal of elevating the concept of control as an end in itself—control for control's sake, without regard to what controls can do. Controls as ends in themselves are logically less probably

---

culture.

128 Neither point negates the possibility that some level of control is necessary nor that in certain discrete contexts some level of control is sufficient.

129 PCAOB PROPOSED STANDARD, *supra* note 125, at ¶¶ 15-17.

130 *Id.*

131 *See* Appendix A.

132 PCAOB PROPOSED STANDARD, *supra* note 125, at ¶ 15.

effective than controls consciously designed for instrumental purposes.

A non-corporate parallel illustrates.133 A university internal-control proposal called for academics given research grants to prepare time-sheets. Part of the motivation was to create a control that was auditable. While the scheme would achieve that objective, it would have skewed incentives toward reading and away from writing or teaching. And it would not accurately measure the effectiveness of the researcher's performance, as it would simply abstract one aspect from the vast complexities of the underlying activity.

No audit is capable of measuring effective performance, however, for audits seek only to verify data or systems. The point renders audits of controls fractionally valuable compared to audits of assertions. An opinion that time-sheets are being completed (control system checks out) or even that they accurately reflect reading hours (output certified) says nothing about the value of the research (which is ultimately what all the controls and audits are supposed to be worried about). Controls attempt to prevent the need to exercise judgment. But judgments cannot be avoided.

2. Auditor Advertising and the Expectations Gap

While properly disclaiming capabilities when conducting audits and giving attestation opinions, auditors promote their services when lobbying for regulations or advertising their services.134 Good examples are the anti-terrorism audits widely peddled following 9/11. There are several varieties. They range from business continuity audits to those prescribed by PATRIOT concerning anti-money laundering systems.135 The potential variety of such audits and associated controls is limitless. Intermediate illustrations would be anti-terrorism audits bearing the tenor of the social responsibility audits made famous by Ben & Jerry's and the Body Shop or ethics audit of the type pioneered by KPMG.

Key controls to adopt and test in each case are akin to those catalogued in Part II. Order-of-the-day requisites are: written policies, compliance officers, employee training, self-enforcement, and of course outside auditing. For PATRIOT-compliance, data tracking systems and information filing protocols are necessary in addition to these features. For business continuity, duplicate back-up systems are in order. For broader certifications, particular industries that are likely targets would

---

133 POWER, *supra* note 7, at 98-99.

134 *See supra* note 58.

135 *E.g.*, PricewaterhouseCoopers, Data Quality Case Study: Ensuring Compliance with Anti-Money Laundering Laws (touting services related to systems to enhance a company's know-your-customer capabilities) (available from www.pwcglobal.com); Deloitte & Touche, Business Continuity Management (advertising products to address "political and economic instability, acts of terrorism both cyber and physical and third-party critical dependencies to name a few" and calling for a shift from "business continuity planning" to "business resiliency") (available from www.deloitte.com); Ernst & Young, Technology and Risk Services ("Companies don't get a second chance today. . . .Everyone you do business with needs to know that your business systems are secure, reliable, available and properly controlled.") (available from www.ey.com).

adopt requisite procedures: aviation, power, landmark real estate operators, and so on.

These controls, including audits of them, can serve several functions. They can help a company assure it is in compliance with regulatory requirements, particularly the case for companies subject to PATRIOT. They can enable a company to continue to operate despite a terrorist attack striking its operational centers. Some might even help address the underlying substantive concern: helping to prevent terrorist attacks, directly or through helping to disrupt funding.

They are not cost-free. In addition to direct costs are the costs associated with creating false complacency. The comfort-sense of systems, controls, and audits obscures the real underlying risks. Doing these things may help but risks remain. Audit certifications, both financial and otherwise, direct or of controls, always have offered more than they give. The auditing literature refers to this as the expectations gap.136

Some auditors wonder about its source. One factor may be the expectations the profession creates, compared to the known limits of its craft. The gap widens when auditors advertise products incapable of delivering the promise. Auditors could help close it by aligning their advertisements, and especially lobbying, with the reality they face. After all, this is what they will argue when internal control failures go undetected and victims of fraud or terrorism sue them.137

The expectations gap typically refers to the difference between what a financial auditor can do and what investors using financial statements expect. Amid control and audit proliferation this expectations gap assumes larger dimensions. There is an expectations gap between what auditors and controls can do concerning a wide range of policy matters and what the public, lawmakers, and legal culture expects them to accomplish.

One reason for this expansion of the expectations gap is that controls have been transformed from bearing a traditional positive function of meeting corporate objectives in administrative controls toward a more negative function of preventing unwanted social effects in policy/compliance controls.138 This difference between positive and negative control functions is a key difference between how auditors and other businesspeople understand controls versus how legal culture—legislators, lawyers, judges—sees them.

IV. CONTROL LIMITS: LEGAL VIEWS

Lost in contemporary legal apprehension of internal controls is their original purpose.

---

136 *E.g.,* Joseph I. Goldstein & Catherine Dixon, *New Teeth for the Public's Watchdog: The Expanded Role of the Independent Accountant in Detecting, Preventing, and Reporting Financial Fraud*, 44 BUS. LAW. 439 (1989); Marc J. Epstein & Marshall Geiger, *Investor Views of Audit Assurance: Recent Evidence of the Expectation Gap* , J. ACCOUNTANCY, Jan. 1994, at 60; Erica B. Baird, *Legal Liability Under the Expectation Gap Statements on Auditing Standards, in* ACCOUNTANTS' LIABILITY 67 (PLI 1991).

137 *See Monroe v. Hughes*, 31 F.3d 772 (9th Cir. 1994).

138 *See supra* note 16 and accompanying text.

Internal controls were originally and fundamentally mechanisms intended to help the organization get to where it is trying to go, whether in terms of product development, customer satisfaction or other fundamental business goals. The business perspective emphasizes the positive aspirations of controls more strongly and fully as a matter of history and practice than the legal side which emphasizes the negative, compliance dimension.139 The business practice of internal controls suggests they are tailored tools for internal objective achievement; the legal view tends to see them as attaching norm-attributes to control-functions they weren't intended to bear.

A. Comparative Control Risk

A focused comparative assessment of how legal views of control risk differ from audit views of control risk shows limits of internal controls. While a full theory of legal views of risk is beyond the scope of this Article, the next section also pursues this more abstract level of insight on law's attitudes towards internal control risk.

1. Analytical Differences

Comparing relative professional perspectives on control risk suggests that the legal view's ambition tends to move more towards closure. That is, compared to residual risk audit tolerates, law allows for less. Law does not seek to address risk 100%, but it is closer to that ambition than audit is. It is neither necessary nor possible to quantify differences and none of the factors discussed below clearly compels the conclusion that law's attitude towards controls is more ambitious than audit practice suggests is sensible. But taken together the comparative tendencies provide strong support for the inference.140

Audit begins with a precise context in which to evaluate internal control risk. It is the formal concept of audit risk. No such equivalent focused framework exists for law. The legal context begins at a more abstract level of risk conception. It is the broad risk of disappointed expectations or adverse outcomes. And legal culture seeks to protect the former (epitomized in contract law) and compensate for the latter (epitomized in tort law). These orientations point in the opposite direction of audit's formal model of control risk inevitability.

Audit presents a formal definition of internal control risk. It is a component of the audit risk model. Law provides no such formal definition. Legal mandates or incentives address themselves

---

139 *E.g.*, Linda Klebe Trevino et al., *Managing Ethics and Legal Compliance: What Works and What Hurts*, 41 CAL. MGMT. REV. 131 (Winter 1999) (lawyers trained on legal problems produce compliance protocols that emphasize "a compliance approach, not a values approach"). In other words, lawyers see controls as bearing negative purchase, as showing norms, not as bearing a positive dimension, as promoting particular corporate objectives.

140 There is also empirical evidence that law expects more than audit can deliver. *See* Marianne M. Jennings, Phillip M .J. Reckers & Daniel C. Kneer, *The Auditor's Dilemma: The Incongruous Judicial Notions of the Auditing Profession and Actual Auditor Practice*, 29 AM BUS. L. J. 99 (1991) (studies showing that judicial expectations of audit are unrealistic).

to negating risk, not dealing formally with the residual, indicating a bias towards risk elimination rather than risk toleration.

Auditors measure control risk.141 There is likewise no equivalent measure in law. The nearest equivalent is inquiry concerning who among potentially blameworthy parties was the least-cost-avoider of a risk realized.142 This is a broad principle from the general legal toolkit, not tailored for internal controls. And it involves a comparative-cost measure between parties, not a direct measure of the risk itself.

Auditors use formal context, definition and measurement to minimize control risk. Apart from the inferred tendencies, law's lack of them does not logically compel any conclusion about law's relative assessment. Informal legal intuition could rate risk higher or lower. But the informalities tend to lead to ranges. Ranges open up possibilities to treat reality as occurring at the extremes. Given legal culture's devotion to assigning responsibility, a temptation arises to treat control risk as at the lower end of the perceived range.

Offsetting this bias could be law's tendency to try to understand particular contexts and incorporate them. When assessing performance of professionals in particular disciplines, law tends to draw on the relevant professional literature. Doing so for internal control risks would lead law to examine the same literature and standards auditors draw upon in practice. To that extent, law's attitude toward control risk should be congruent with that of auditors. Law would follow audit standards in determining whether, for example, an auditor comported with professional obligations for defining and minimizing control risk and planning and conducting an audit accordingly.143

That congruence may be more apparent than real, however, when auditor advertisements concerning their craft capabilities exceed what they can do in fact. Those pronouncements raise expectations, can influence what is seen as reasonable, and thus form part of the legal framework for evaluating claims of negligence when controls fail and risk is realized. This is what auditing literature calls the expectations gap. So the theoretical congruity between law and formal auditing pronouncements breaks down and law's ambition in allocating internal control risk exceeds that of audit's.

---

141 Auditors do not pretend to measure control risk precisely, of course, but do attempt a rigorous evaluation and assessment. *E.g.*, VINCENT M. O'REILLY, ET AL., MONTGOMERY'S AUDITING (12th ed.), at 6.14 ("Many attempts have been made to develop mathematically based risk assessment models, but there is no requirement that audit risk or its components be quantified. In fact, it may not be practicable to quantify the components of audit risk because of the large number of variables affecting them and the subjective nature of many of those variables.").

142 *E.g., D'Amico v. Christie*, 518 N.E.2d 896, 901 (N.Y. 1987) ("The key in each [case] is that the defendant's relationship with the either the tortfeasor or the plaintiff places the defendant in the best position to protect against the risk of harm").

143 There should be instinct congruence between law's approach to auditing's reality: the earliest legal materials embracing standards for control and audits-of-control audits (such as the FCPA) drew directly on professional auditing literature control. *See supra* notes 17, 94, 95 and 122.

2. The Process Bias of Lawyers

Whereas auditors rely upon the standard of professional skepticism that leads them to question both process and result, the lawyer view emphasizes process. Among corporate lawyers and judges, in particular, the business judgment rule means that process is paramount. Corporate law generally assumes that if the process is properly designed and followed, the results will take care of themselves.144 In the case of control (and audit), however, this is unlikely to be the case. So the result is that law can expect too much from control (and audit).

This discrepancy can be reinforced when audit's emphasis on systems and controls creates false impressions that these reflect likely achievement of underlying objectives. The proliferation of audit and the standard resort to enhancing internal controls in the face of crisis shows social anxieties. 145 Assuaging social anxieties with these tools can create illusions of control and denial of risk.146

Consider the legal attitude discernable from *Caremark*'s establishment of the director duty of oversight through information systems. Specification is required of its content. There are two ways to put it: (1) reasonable effort at absolute assurance or (2) absolute effort at reasonable assurance. In Delaware this distinction is not mere semantics.

In (1), reasonable effort signifies the Delaware focus on process;147 in (2) reasonable assurance emphasizes the limits of systems. The former commands less from actors but expects more from systems. The latter commands more of actors but expects less from systems. Chancellor Allen's statement of the duty partakes of version (1), a duty to "attempt in good faith to assure."148

---

144 *See* Lawrence E. Mitchell, *Fairness and Trust in Corporate Law*, 43 DUKE L. J. 425, 434-36 (1993); *infra* note 147.

145 POWER, AUDIT SOCIETY, *supra* note 7 (auditing as a response to systemic challenges "reflects wider social anxieties and a need to create images of control in the face of risk.").

146 *Compare* ERNEST BECKER, THE DENIAL OF DEATH (1973).

147 Evaluating directorial liability for breach of the duty of care is analytically identical to other tort cases, though Delaware judges like to emphasize subtle differences that make usual negligence analytics ill-suited. *See Caremark*, 698 A.2d at 969, note. The chief difference is that the reasonable person standard is jettisoned and business judgment rule deference installed. But otherwise, the elements are duty, breach, causation and damages. The differences lead judges to avoid second-guessing the quality of decisions (whether they are stupid or irrational is irrelevant, for example) and focus on good faith and process. *See* Mitchell, *supra* note 144.

148 *Caremark*, 698 A.2d at 970. To be fair and complete, other language in the opinion supports this emphasis, though some does not. One says the duty can be discharged "by assurance of adequate information flows." Another says that a breach would require no "attempt to assure a reasonable" system. A third requires boards to assure themselves of systems reasonably designed to produce requisite information. But all these phrases appear outside the court's integrated statement of the duty, where one may suppose greatest attention to detail was applied.

Suppose there are two types of systems, Control A+ and Control B-. Control A+ is designed for absolute assurance and Control B- is known to have some leaks but is pretty good. Under standard (1), the board must take reasonable steps to install Control A+. Under standard (2) the board must buy one of them, but buying Control B- is clearly okay.

The legal culture is telling managers to take steps to buy Control A+; the audit culture is happy to sell it; the truth is, there is no Control A+. No system provides absolute assurance. The gap is significant between (1) what systems can deliver (something like Control B-) versus (2) what legal culture expects and what auditors advertise they can deliver (Control A+).149

3. Perspective Differences

Hindsight bias tends to result in assigning higher probabilities to actual outcomes than would have been assigned based on expected outcomes. From this view, it would be likely that auditors apprehend a greater measure of control risk than lawyers would.

Auditors assess internal control risk at the outset. It is generally an *ex ante* perspective (forensic auditing is the exception, but this has more of a legal than an audit context). The legal view tends to be *ex poste* (except where lawyers participate in the design and evaluation of controls, which likewise characterizes more of an audit than a legal context). After some risk is realized, the issues of how and why it arose and who is responsible are investigated after-the-fact.

Similarly, auditors sign off on risk ahead of time. Lawyers give no such certification. Auditors opine concerning assertions made, based on evidence they've gathered, tests they've conducted, in light of risks they understand and have tried to define, measure and minimize. Lawyers are not in this business of opining on internal controls.

Auditing exhibits relative literalism compared to law. Auditing is populated by descriptive language intended and believed to have relatively stationery meanings and significations. Auditors measure and express results in quantities. Lawyers are more inclined to linguistic interpretation. They understand words to have uses more than meanings and that meanings vary with context. They are less inclined toward quantitative measures, at least as ultimate answers, compared to auditors.

A good example of these comparative differences concerns loss contingencies and associated

---

149 Again to be fair and complete, the *Caremark* opinion states that there is no way that a "rationally designed" system will "remove all possibility" of violations. But this may only mean there is a difference between formal articulations of legal duty, with ambitious aspirations, and what such common sense views acknowledge. *See* PHILIP K. HOWARD, THE DEATH OF COMMON SENSE: HOW LAW IS SUFFOCATING AMERICA (1995). In the same spirit, note that the FCPA contemplates systems designed to obtain "reasonable assurance." *See supra* Part II.A. But that statute originated by copying standards directly from the professional auditing literature, *see supra* 19, constituting an expression of audit culture whereas *Caremark* is more distinctly an expression of legal culture.

risk. Though this is a non-control context, it is an intersection directly raising risk assessments where auditors meet lawyers routinely. Both professions use the concepts of remote, possible, and probable to assess risk of loss contingencies. But each defines the levels differently, both in terms of content and metrics. Auditors attempt a numerical specification; lawyers approach the meanings conceptually, as existing in ranges. Sometimes the two overlap but often they do not.

Reasons for the gap include the different professional obligations implicated in assessing loss contingencies.150 Auditors seek disclosure, implying a bias towards perceiving higher risk; lawyers seek confidentiality, implying a bias towards perceiving lesser risk. Those associated characteristics may also contribute to stances on control risk. If so, auditors see risk as higher compared to lawyers.

Audit's ultimate view of risk may be equated to an old principle of the common law that allowed losses to lay where they fell.151 The modern legal mind rejects this approach permitting happenstance to dictate outcomes. Legal culture seeks to understand risk of loss and allocate it in some way, whether by contract or by non-contractual defaults such as using least-cost-avoider analytics.152 Auditors embrace the concept in action, facing it every day, conducting tests and interacting with management to achieve risk-reduction at least cost. But in the end they live with it based on their judgments.

4. Generality versus Specificity

Auditors classify controls according to particular tasks. Financial controls relate to attestations concerning financial statements. These are tested during a financial audit. Compliance controls are tested when auditors are engaged to do so. Specific tests are conducted and opinions given that define the steps and scope of an attestation. Direct testing of financial controls is a consciously more involved process intended to yield different levels of risk minimization and comfort.

Law does not meaningfully embrace such distinctions. Instead broad legal mandates direct the establishment and testing of internal controls. The clearest examples are state law fiduciary

---

150 *See* Richard W. Painter, *Lawyers' Rules, Auditors' Rules and the Psychology of Concealment*, 84 MINN. L. REV. 1399 (2000).

151 This disposition is discernable in the hallowed line of English impossibility cases in contract law, including *Paradine v. Jane*, 82 Eng. Rep. 1897 & 82 Eng. Rep. 519 (K.B. 1647); *Taylor v. Caldwell*, 122 Eng. Rep. 309 (Q.B. 1863); *Krell v. Henry*, 2 K.B. 740 (C.A. 1903). *See generally* John D. Wladis, *Common Law and Uncommon Events: The Development of the Doctrine of Impossibility of Performance in English Contract Law*, 75 GEO. L.J. 1575 (1987).

152 The variety of strategies trace their roots to the Coase Theorem's proposition that initial legal distributions of entitlements in a world of no transactions costs don't matter, because parties will trade to the efficient allocation. *See* Ronald H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1 (1960). *See generally* John Elofson, *The Dilemma of Changed Circumstances in Contract Law: An Economic Analysis of the Foreseeability and Superior Risk Bearer Tests*, 30 COLUM. J. L. & SOC. PROBS. 1 (1996).

duties imposed on directors, epitomized by *Caremark*. It embraced the broad concept of an "information and reporting system" that seemed to encompass without distinction financial and compliance matters.153

When controls fail, the existence of control norms, directives, or practices are relevant to evaluating the standard of care exercised with little or no regard to the particular control at issue or its underlying substantive purpose. Their existence helps plaintiffs meet case elements such as foreseeability and causation. These factors tend to produce a legal attitude toward internal controls that expects more from them than audit suggests it should.

The content of internal controls is invariably filled with a set of best practices. These come to define expected standards of behavior, which in turn furnish the texture of legal standards of liability. Industry practices are copied and instantiated as norms. Failure to follow leaders creates liability risks. This occurs without regard to whether the standards warrant copying.154

In novel contexts such as contemporary cyber-crime, for example, limited experience prevents a reliable knowledge base concerning how to defeat hackers. This matters little for law. If other corporations have installed firewalls and redundancies but one hapless corporation did not, a negligence claim buds even if there is no other basis for believing that the standards were preventive.155

B. Liability Risk

American political culture is non-fatalistic. For every harmful effect, there is causal blame; damage requires compensation. Cultural belief in systemic failure and blameless accident are foreign, un-American.156 Legal culture is an expression of political culture. American legal culture

---

153 *See supra* Part II.A. COSO collapsed the distinction. Even when official pronouncements nod at the distinction between types—such as in the DOJ's U.S. Attorneys' Manual and the federal Organizational Sentencing Guidelines and the SEC's SOX regulations—operational significance is limited. The SEC's revival of the classical distinction is a promising sign.

154 *See* POWER, *supra* note 7, at 143 ("audits may turn organizations on their heads and generate excessive preoccupations with, often costly, auditable process. At the extreme, performance and quality are in danger of being defined largely in terms of conformity to such process.").

155 *See* Jenny B. Davis, *Cybercrime Fighters*, ABA JOURNAL.COM (July 31, 2003). Led by the U.S. Department of Homeland Security's June 2003 creation of the National Cyber Security Division to address threats to computer systems, companies began following, and thus creating, emerging standards and best practices for computer security. One expert notes that these standards once articulated form the basis for gauging corporate behavior and that "class action lawyers will start salivating if you didn't take the actions recommended by this or that organization."

156 *See* John C. P. Goldberg, *Unloved: Tort in the Modern Legal Academy*, 55 VAND. L. REV. 1501, 1510 (2002). In discussing the evolution of the concept of negligence in tort law, Professor Goldberg explains:

finds plaintiffs in every catastrophe, defendants behind every tragedy. Internal control is a device law uses to create responsibility and assign blame.

1. Assigning Blame

Directors faced personal liability in *Caremark*, avoided through a settlement. Chancellor Allens's opinion suggested to many practicing lawyers that corporate boards needed to assure adequate controls across the corporation.157 Control failures allegedly responsible for the bombing of a PanAm flight over Lockerbie, Scotland, yielded corporate liability that helped send the airline into bankruptcy and ultimate oblivion; TWA faced similar liability risk when passengers on board one of its terrorized jets lodged similar complaints concerning internal control failure.158

Control failure producing legal liability risks arises in the most unlikely settings. Take terrorism. Apart from Acts of God, terrorist assaults such as 9/11's would seem to qualify as blameless or unavoidable, at least insofar as corporate America or its controls are concerned. But emblematic of legal culture, immediate reaction to 9/11 was to ask how victims would be compensated and how the civil litigation system would facilitate doing so.159 There seemed little question that compensation was due and that some corporate deep-pockets would pay.160

> Lots of behavior . . . might be described as negligent, particularly in hindsight, after someone's been hurt. This realization not only stemmed from the tractability of the concepts of fault and reasonableness, but also was predicated upon an important fact about American political culture, which is that we simply do not cotton to notions of fate. To us, every accident has an explanation, every bad outcome a responsible party. Europeans and other strange peoples might think in terms of systemic failures and unavoidable accidents. Not so for us.

157 On the other hand, Chancellor Allen's *Caremark* opinion indicates that director liability for control failure would require an "utter", "sustained," and "systematic" failure of controls. These adjectives carve back on liability risk. Nevertheless, corporate advisors viewed the opinion more cautiously. Also, these adjectives rightly suggest an apprehension of controls as bearing negative dimensions. They insightfully imply that controls intended to prevent harms set high ambitions, the failure of which would produce liability only in very extreme cases of abdication. The insight is a useful way of understanding the opinion and provides a way to align what law expects from internal controls with what is reasonable to expect from them. *See infra* text accompanying note 188.

158 *See infra* Appendix B.

159 *E.g.*, Georgene Vairo, *Remedies for Victims of Terrorism*, 35 LOY. L.A. L. REV. 1265, 1267 (2002) ("I was curious to see how the victims of the World Trade Center (WTC) and Pentagon bombings would be compensated."); *see also id*. at 1268 (reporting teaching Civil Procedure and Complex Litigation students about how to sue and what the issues would be (claims and liability theories), without mentioning prior question of whether anyone should even think about suing anyone at all).

160 *See id.* at 1268 (after noting that lawyers should not "get rich off this disaster," declares

These legal instincts are reflected in the fund Congress created as an alternative to civil litigation for 9/11's direct victims. Though the fund also sought to limit damages faced by various putative defendants, this and the direct compensation motive both reflect a prevalent expectation that payment must be made. Some fund critics complained that creating it and providing incentives for victims to partake was "tantamount to denying the rights of victims to sue the airlines for damages."161 The claimed right is overstated if airline internal control failure may not be to blame, suggesting a legal right to bring a claim for control failure that audit indicates is unfounded.162

Which of these two methods will provide ultimate compensation is uncertain. To the extent the special fund provides the lion's share of the remedy, this neutralizes concern that internal control failure is seized upon to allocate responsibility to corporations not in any direct way culpable. On the other hand, to the extent the private litigation generates liability in those defendants this concern remains real.

2. Creating Expectations

Legal culture's greater ambition for internal controls compared to audit may be partly explained by evolution of controls from positive internal mechanisms to achieve objectives to negative preventive mechanisms imposed or encouraged through regulation. Corporate governance codes and best practices templates are good examples. They began as professional efforts to retain authority to promote corporate objectives while limiting regulatory intervention.163 Regulators increasingly rely on them. When these devices are adopted internally they embrace the positive quality of achieving objectives, but when functionally required or encouraged by regulators they embrace the negative dimension of preventing deviance.

Legislators using controls as a crisis-response mechanism both embrace an ambitious role for controls and create high expectations. Controls bearing positive qualities of objective achievement are relatively modest and create proportionately modest expectations. Controls bearing negative qualities of deviance-prevention are more ambitious and can create proportionately greater expectations.

It is plausible to believe that a system of control can reduce associated risk. But legislation accompanied by political rhetoric advertising it as the solution to prevent recurrence of the crisis promises to do more than that. It creates the stronger but false sense of risk control. Expectations arise that unwanted events can be prevented. The audit view confirms that this is impossible to achieve in fact but such legislation is law that makes it appear plausible to embrace in attitude.

---

that "All victims should receive reasonable compensation within a short time frame," without explaining why).

161 *See* Noah H. Kushlefsky, *Practice Tips: Choice between the Victim Compensation Fund and Litigation*, 25 L. A. LAW. 13 (Sept. 2002).

162 The same lawyer admitted that "liability of domestic defendants is uncertain." *Id*.

163 *See* POWER, *supra* note 7, at at 54.

Such legislation appears to solve problems, and it may solve some.164 But symbolic control regimes also produce symbolic rituals of comfort.165 When legal culture takes these legislative expressions seriously, second-order pathologies follow. Controls assume perceived qualities they can't bear, as reliable aids in preventing failures not possible to prevent. When controls turn out to fail, not only does liability follow, but legislators or regulators indulge an addiction to creating more of them.166

3. Auditor Liability

A further consequence follows from this discrepancy between law's ambition for controls and the audit understanding of them. Liability for corporate control failure extends beyond the corporation to include the auditors having furnished attestation opinions. The Enron and WorldCom debacles, along with others, led to Arthur Andersen's demise.167 The lawyer's view of risk that supports liability is not invisible to auditors. They recognize personal liability risks when the audit comfort they have given turns out to have been misplaced. For auditors, legal risk is liability exposure.

The perception affects audit practice. Audit exercises are conducted in a legally defensible way. Formal attestation expressions are hedged with representation limitations and capability qualifications. The gap between what auditors advertise and what they deliver widens. It becomes difficult to discern what is reasonable to expect. Auditors face pressure to adhere to recognized best practices more than assuring that those practices are in fact best. The result retards evolution of substantively-best in favor of practice-best. What is done is more important than what it does.

4. Limiting Effects

Law's comparatively greater ambition for internal controls can also further limit controls' possibilities. When systems create false images of control, they proliferate along with audit certificates of comfort. But the result is not necessarily justifiable comfort.168 The more society relies on controls seeking risk elimination, audit that appears to attest the capability, and liability for respective failures, the more pressure arises for controls that make the audit function possible (and

---

164 I make this assessment and prognosis concerning Sarbanes-Oxley in Cunningham, SOX Yawn, *supra* note 1.

165 *See* POWER, *supra* note 7, at 138 (symbolic legislation invariably "generates its own pathologies in the form of equally symbolic enforcement practices oriented towards the production of comforting labels").

166 *Id*. at 139 ("Audit cannot be permitted to fail systematically and must be immunized from radical doubt; if audit is to function credibly in the processing of risk then trust in audit must be constantly affirmed and supported").

167 *See* Cunningham, SOX Yawn, *supra* note 1, at 926 (Andersen audited Enron, WorldCom, Global Crossing and Qwest, the "Big Four Frauds" that catalyzed SOX).

168 *See* POWER, *supra* note 7, at 140.

more auditing of those controls). The paradoxical upshot: installing more controls produces less actual control.169

The legal view of internal controls encourages their use as devices to assign blame and promote accountability. This promotes their value as liability risk management tools or forms of insurance. But this creates moral hazard problems that can skew control design.

If controls enable a corporation to shift liability down the ranks or expose leaders such as boards to liability for control failure, corporations will invest less in controls authentically designed to meet objectives, and more in methods to shift liability away from the corporation or board and onto employees. Producing manuals and conducting training programs at the organizational level enables corporations to assign blame to employees who failed to follow the lessons. This can occur even if the manuals and programs are weakly calibrated to promote actual substantive performance.

The use of internal controls to simultaneously promote compliance and accountability can produce two forms of departure above optimal internal controls. The first is window dressing. These are controls deliberately designed to bear nominal significance but carry no functional bite. When window dressing is equally rewarded, corporations will produce more of it. Neither the OSGs, nor *Caremark* nor other incentives for controls are systematically equipped to distinguish window dressing from optimal controls.170

The other form of excessive controls can arise by accident. Internal controls may be conscientiously designed but be overdrawn, futilely attempting to overcome the reality that no internal control system will deter or catch all adversity. The result is likely over-investment in perfectly good controls. If you give credit for internal controls, you risk getting not only window dressing but valid controls that won't likely yield commensurate benefit.

The expectations gap, and audit and law's roles in sustaining it, create another downside. The paradox of control's appeal-and-limits floods corporate America with controls throughout its operations, reinforced by periodic deepening and broadening in response to crises. It becomes impossible to know which controls really work and which are doomed to artificial confidence boosting. When law takes auditing's image-making seriously it treats the system as more of a risk neutralizer than as simply a factor in assessing risk's magnitude.

Control proliferation and generality also complicate foreseeability analysis in tort contexts. If controls were used only in particular settings with defined functions, they could be useful indicia that related risk realization was foreseeable. They might be useful in assessing difficult pragmatic questions of causation when losses arise after controls fail. But when every aspect of corporate affairs is layered with elaborate controls, and most are abstract recitations of good-governance

---

169 *Cf. id*. at 141 ("At worst auditing tends to become an organizational ritual, a dramaturgical performance.").

170 *See* John C. Coffee, Jr., *Does Unlawful Mean Criminal? Reflections on the Disappearing of the Tort/Crime Distinction in American Law*, 71 B.U. L. REV. 193, 229 (1991).

platitudes,171 there is no credible basis for drawing such inferences. Control signifies nothing special, so offers no insight concerning foreseeability or causation. This has not, however, prevented using control failures in exactly this mistaken way.172

C. Control Liability

The role of internal controls in assigning blame is not unique. It is a symptom of broader stress the American tort system has been suffering for some decades.173 Old-fashioned tort law provided a civil remedy for a private wrong, invoking the state's judicial system in the redress. Twentieth-century tort law, led by Cardozo, reworked tort to meet the novel civil wrongs wrought by mechanized industrial society.

Tort moved in numerous directions but the central artery viewed the enterprise as an open-textured drawing board on which to chart blame assignment.174 Negligence remained the chief doctrinal tool, anchored somewhat by traditional concepts of duty, breach and causation, including foreseeability. But these doctrinal constraints never provided clear boundaries and as tort was put to use in solving a wide range of modern tensions, judges and juries used these as fluid instruments of social policy.175

1. Controls and Torts

Internal controls became an ingredient in the enterprise of judicial policymaking, a tool to assign blame or to exonerate, depending on the facts (as well as the cut of the judge's robe). Commentators examine the judicial output using analytical tools of deterrence and compensation: how are sanction threats and penalty levels calibrated to discouraging undesirable activity? Internal controls enter the equation as compliance promotion devices with the threat of liability backstopping their presumed efficacy.

Suppose a statute prohibits a certain act, say certain kinds of political contributions. Suppose further that best practice, industry standards, and regulatory encouragement indicate the desirability of internal controls to prevent such contributions. And suppose finally that a company makes a prohibited contribution, internal controls notwithstanding.

---

171 *See supra* Part II.B.

172 *See infra* Appendix B; *see also* Langevoort, *supra*, note 118 ("it would obviously be foolish for the law to test the reasonableness of a system simply by reference to what are common practices in the industry, which is exactly what we see happening in many fields").

173 *See* PHILIP K. HOWARD, THE DEATH OF COMMON SENSE: HOW LAW IS SUFFOCATING AMERICA (1995).

174 *E.g., Hamilton v. Beretta U.S.A. Corp*., 750 N.E.2d 1055, 1056 (N.Y. 2001) (question of duty in tort is a "legal, policy-laden declaration reserved for judges"); *532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Center, Inc*., 750 N.E.2d 1097, 1101 (N.Y. 2001) (tort duties are areas of "policy" creating "a legal question for the courts").

175 *See generally* Goldberg, Unloved, *supra* note 156.

Making the contribution violates the statute. The company is liable for the statutory breach, as is the employee responsible for causing it to be made. If it is a criminal statute, no private citizens would be entitled to enforce it by recovering against the corporation. Any claim against it by third parties or claims by shareholders against its board, officers, or other employees would face an uphill battle on the basis of the statutory violation alone. Issues of duty, breach, causation and damage are formidable.176

But the contribution also represents an internal control failure. This changes the picture for each of these claims. Now third parties somehow damaged—say opposing political parties—as well as shareholders whose corporation has been harmed have an alternative ground for their claim, whether against boards, managers, or employees. The presence of the control culture brings down the otherwise-formidable barriers associated with the elements of duty, breach and causation. Internal controls ease the burden of all potential plaintiffs and also enlarge their potential number.

Consider the real case of PanAm.177 Rules required baggage screening by physical inspection. The company developed internal controls to train employees in the technique and to use x-ray technology to meet the obligation. In doing this, the company sought but never obtained an FAA interpretation that its controls—using x-ray to meet the physical inspection requirement—satisfied the legal requirements. The controls failed. Terrorists smuggled a bomb aboard a plane which exploded over Lockerbie, Scotland, killing nearly 300 people.

Passengers' survivors sued PanAm. The thrust of their case was simple. FAA rules required physical baggage-inspection. Employee training was inadequate. Physical inspection was not met by x-ray examination. The case was about the failure of internal controls. The plaintiffs won. Were internal control failures to blame? Were culprits inadequate training and inadequate internal control responses to assure that FAA physical inspection directives were met? Or were terrorists the cause?

The tort claim yielded a multi-million dollar jury verdict for the passengers' victims and contributed to the corporate death of an already-beleaguered airline. Worse, that airline was the unofficial US flag carrier overseas. As awful as the death toll was, terrorist payback multiplied enormously when the company, socked with this liability, went bankrupt.

2. Curtailing Ambitions

---

176 Liability is more likely if the board knowingly engaged in the illegal act. *See Miller v. American Tel. & Teleg.*, 507 F.2d 759 (3d Cir. 1974) (denying defendants' motion to dismiss shareholder derivative action alleging knowing violation of federal prohibition on corporate campaign spending, holding while business judgment rule protects ordinary director decisions it does not protect a decision alleged to constitute an illegal act); *compare Gagliardi v. Trifoods Int'l*, 683 A.2d 1049, at n.2 (Del. Ch. 1996) (disinterested directors acting in good faith not liable for corporation's illegal acts).

177 Appendix B contains a fuller account, context and criticism of the *PanAm* case.

Just as tort as a whole has been asked to do more than it is capable of doing,178 internal controls as a component of this system are asked to do more than they can. When asked to do more than they can, they become capable of doing less. Emphasis on control yields control proliferation that disguises the effective from the ineffective; emphasis on audit of control yields controls that can be tested rather than promoting controls likely to be effective. The controls produced are less likely to be effective.

The foundational paradox of internal controls is the logical opposition between the interior concept of internal and the exterior character of control.179 If this conceptual paradox is foundational, the ultimate operational paradox is the radius of control devices. Internal controls have a positive side lost in the literature, especially the legal literature. These are valuable devices to help direct a corporate operation to achieving its objectives. One characteristic of control proliferation is controls have assumed a negative cast and emphasis.

Accentuating the positive side of controls suggests that if the goal is to achieve x, failure to achieve goal x does not necessarily indicate failure or culpability. Emphasizing the negative side of internal controls changes the logic. If the goal is to prevent x and x occurs, failure and culpability are implied. This re-characterization of controls can increase the risk of liability from perceived control failure. Yet should all control failures be treated alike?

Here it seems instructive to return to the difficult task of arraying controls along a continuum from operational and financial (pure internal) to compliance and policy (somewhat more external).180 In this Article I cannot develop a full model but can sketch some useful outlines. SOX and PATRIOT suggest the extremes. Apart from traditional operational controls, the financial controls of SOX are geared most inward, at preventing fraud (as well as fair financial reporting). PATRIOT is directed more outwardly, at preventing terrorism. In between are controls related to antitrust, environmental, labor, and workplace safety.

Employees are likely more receptive to controls geared towards outward-directed objectives, especially terrorism. These are pursuits of a public policy nature in which the firm is a civic partner and through which employees co-venture in a virtuous enterprise.181 Employees are least likely

---

178 *See* Goldberg, Unloved, *supra* note 156.

179 Characteristics described as internal to an object suggest them as its constitution. Control is essentially a directive force operating from outside an object. The proposition of control from within shows a logical tension. Even for individuals, self-control is a function of the superego at work; for organizations, no basic psychological operations are instinct to the entity. The paradox does not prevent an internally-generated mechanism to impose some directive constraint. It does mean that doing so is full of tension. And it may help explain the numerous additional paradoxes suggested in this Article.

180 *See supra* Part I.A.2.

181 *See* Arthur J. Jacobson, *Hegel's Legal Plenum*, CARDOZO L. REV. (1988); Arthur J. Jacobson, *The Other Path of the Law*, YALE L. J. (1995).

receptive to controls geared towards self-observation to police asset dissipation and inaccurate record-keeping, monitoring themselves or each other.

Two competing models of regulatory theory map onto this range. The deterrence model hypothesizes that target decision-making is conducted by comparing the cost of compliance with the product of enforcement threats and penalty levels. The cooperation model enlarges the framework by recognizing norms of compliance that may be skewed by the simple adjustment of threat and penalty levels.182 In the case of internal controls the relative purchase of these models varies with the tenor of the control.

Pure internal controls, those directed to existing asset preservation and accurate recordkeeping, link to the deterrence model. Dishonest employees benefit by asset-dissipation or reporting-obfuscation and even honest employees are less receptive to the controls as expressions of mistrust. Deterrence is key and the combination of threats and high penalties a device matched to the risks of departure.

Externally-oriented internal controls, those directed to anti-terrorism activities for example, are more congruent with the cooperation model. Dishonest employees do not benefit personally from their failure and have no inherent incentives to cheat. They seek to cooperate in the civic enterprise. The cooperation model is a more accurate account of their decision-making process.

These suppositions of comparative employee receptivity to controls relate directly to the role control failure should play in evaluating corporate or employee liability. For pure internal controls, financial controls, the deterrence model means the combination of threats and penalties is key. Control failure should expose the corporation and its agents to liability—threatened enforcement and penalty size must be real. At a minimum control failure should be an important factor bearing on the culpability, whether under negligence standards or otherwise, of derelict employees and the corporation.

The opposite is the case for externally-oriented internal controls. Cooperation can be more readily assumed. The combination of threats and penalties are not critical drivers, and may backfire. Employees want to help. When they fail, enforcement and penalties are inapposite. At minimum, control failure should not be a factor in evaluating claims of negligence or other theories of liability against employees or corporations.

This theoretical account of the distinction between control types is congruent with the longer history of corporate law. Causation has constituted a formidable barrier to claims by shareholders

---

182 *See* Michael P. Vandenbergh, *Beyond Elegance: A Testable Typology of Social Norms in Environmental Compliance*, 22 STAN. ENVTL. L. J. 55, 61-62 (2003) (noting that one weakness of standard deterrence model is evidence shows monitoring increases compliance but penal severity does not and explaining that compliance is promoted not by more or less deterrence-model emphasis but through tailored enforcement in light of a framework incorporating an understanding of the effects of norms).

against allegedly negligent directors whose major fault was lack of attention.183 But this distinction never insulated directors from negligence liability when their inattention overlooked outright self-dealing down the ranks. This meant maintaining a system of financial control.184 Extending this basic principle to the realm of all compliance controls is radical and revolutionary, transforming not only corporate law but American civil and criminal law.185

It is not too late to arrest the revolution, though some repair work is in order. Every legal institution connected with internal controls should be cautious in allowing them to furnish a substantially new and independent basis of liability. They are unlikely to be as effective as such liability theories would require to be justified; imposing liability discourages development of gold standards of internal controls; and especially in the case of terrorism, imposing liability after attacks promotes the terrorists' goals and is not in the national interest.186

Several ways are available to limit liability expansion based on internal control failure. Traditional tort jurisprudence permits pragmatic and prudential line drawing.187 When internal controls are a factor, they should be treated according to their underlying purpose. For financial controls, they could be credited with some significance; for terrorism controls, none.

---

183 *E.g., Barnes v. Andrews*, 298 Fed. 614 (S.D.N.Y. 1924) (distinguishing between failure to remedy ordinary incompetence from failure to detect outright self-dealing within board's oversight responsibilities).

184 *See* Dooley, *supra* note 43, at 485 ("directors' ignorance of wrongdoing will not be excused if and to the extent that the board has an obligation to assure that the firm maintains adequate internal controls to guard against such wrongdoing. The clearest example of this is accounting controls, where it has long been recognized that the board is obliged to insure the installation of adequate record-keeping and auditing systems.").

185 *Id*. (the quest "to impose secondary liability on directors for the illicit acts of others is truly radical, and the case for such a revolutionary change in existing law is far from being proved"; it amounts to "sweeping changes in the whole corpus of American civil and criminal law"). The defect is the failure to distinguish, as many particular federal statutes had done, between types of illicit acts. Discriminatory judgment should be applied to determine "whether directors should be liable for another's violations of the antitrust, labor, civil rights, product safety, environmental or general criminal laws calls for the application of no less discriminating judgment." *Id*. at 485-86 (footnotes omitted). A related concern was why shareholders should be entitled to wage derivative suits against directors for such violations "when shareholders have no greater interest in corporate lawfulness than any other member of society." *Id*. Well, the floodgates having opened, plaintiff classes are not limited to shareholders. Professor Dooley also noted that compliance programs are more intractable than financial controls: "Determining which corporate assets need to be secured is relatively easy, but deciding which laws directors should be most concerned about is not." *Id.*

186 *See infra* Appendix B.

187 The seminal statement is WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS §31, at 180 (1941) ("duty . . .is only an expression of the sum total of those considerations of policy which lead the law to say that the particular plaintiff is [or is not] entitled to protection.").

This would call for a clarification of the *Caremark* decision. A simple way to do so is to emphasize that while the court rejected *Graham* by announcing directors have duties to monitor through controls, it also noted that liability would only attach when evidence showed an utter, sustained and systematic failure.188

But emphasizing that out is not enough. More particularly, *Caremark* should not be read to treat board obligations to maintain broad "information and reporting systems" to expose boards, or the corporation, to liability when controls fail. Rather, control types should be distinguished.

Again a complete specification of controls calibrated to appropriate liability cannot be made in this Article, but outlines can be mentioned. Control failure could be a factor in the case of financial controls, but should be given no weight in the case of terrorism controls. Any other compliance control failure should be seen as a factor only to the extent calibrated to the underlying purpose of the substantive factors controlled and their link to internal corporate governance.

There is precedent for just a move in Delaware. The Delaware courts flirted with and likewise retreated in a similar manner concerning a duty of candor the Supreme Court of Delaware noticed had "crept into" corporate law.189 Any creeping of the duty of oversight ought to be similarly nipped in the bud.

CONCLUSION

The success of internal controls is manifested in silence—absence of financial scandal or terrorist threat. In the case of internal controls designed to prevent deviance, it is often impossible to prove success, or even notice it. When national intelligence organizations such as the CIA fail publicly in counter-terrorism efforts, as they appear to have done on September 11, embarrassed experts argue: "But you should see how many terrorist attacks we thwarted!" When a company properly reports in accordance with GAAP and no fraud occurred, was it due to internal controls or to independently-conscientious employees?

Despite the difficulty of assessing the effectiveness of internal controls, when failures arise they should not be dismissed on the grounds that the successes cannot be tallied. The CIA argument is not so convincing. Nor should the failure or inaction be seen as an automatic indictment of the control system, however, for the CIA thesis has some validity. Failures should instead be studied for lessons about the weaknesses of controls and the extent to which they can be fixed. Lessons can be applied to improve controls and to reshape expectations about what they can realistically achieve. These views of control from law and auditing and the examples of SOX and PATRIOT point in the same practical direction: controls and audits are helpful but inherently limited and while

188 *See supra* note 157.

189 *See Stroud v. Grace*, 606 A.2d 75, 84 (Del. 1992). The concept had "crept" into Delaware corporate law beginning with the major case of *Lynch v. Vickers Energy Corp.*, 383 A.2d 278 Del. (1977), and including other major cases such as *Mills Acquisition Co. v. McMillan, Inc.*, 559 A.2d 1261 (Del. 1989) and *Citron v. Fairchild Camera & Instr. Corp.*, 569 A.2d 53 (1989).

encouraging sensible use of them is desirable, equally desirable is emphasizing that we should not expect very much from them.

But it is difficult not to raise expectations, particularly when responding to national crises such as 2001's financial scandals and terrorism. The pressure to respond quickly is too great.190 The key, however, is not action but analysis and information. The public should not be led to think there are solutions to these problems but taught to understand the chances of them occurring and how to live with those chances. Politicians responding to crises ought not pass new legislation claiming to prevent assorted ills using controls and audits, but educate the public about associated risks. Politicians generally lack requisite incentives to do this, however, so public education remains the only way to align expectations with probabilities and realities. In the case of internal controls, we are a long way from that alignment, and SOX and PATRIOT widen the distance.

190 *See Something Must (Not) Be Done)*, THE ECONOMIST (Sept. 13, 2003). Examples of quick responses that are suboptimal abound. Relatively infrequent train wrecks produce speed restrictions and track inspections that shift demand from rail to automobiles, a statistically more dangerous place producing a higher probability of fatalities. Rare airplane emergency-water-landings brought us the virtually useless but costly life vests under each seat. 9/11 produced random passenger screening that caught the most innocuous passengers, giving hijackers a greater probability of slipping unnoticed (this system is giving way to more analytical approaches based on risk profiles). The post-Exxon-Valdez oil spill cleanup did more damage than the spill. The control responses of Enron and 9/11 appear to fit this category of misguided reaction. All these responses generate associated public expectations that the fix would somehow work or help to work, though this is invariably mistaken.

APPENDICES

A. Control Failure: WorldCom

To give a practical sense of the limits of internal controls and audit consider the colossal failure of WorldCom Inc., once the nation's second largest long-distance telecommunications carrier (marketed under the MCI brand). WorldCom's internal controls failed because they allowed senior financial executives to jigger ledger entries without immediate detection. On the other hand, they worked because a member of the company's internal audit team discovered the jig. The limit of weakness relates to the time delay, from deception to detection.

The internal audit that uncovered the scam was not a routine and scheduled check-up. Instead, a newly-installed CEO asked the internal auditor to spot check capital expenditure (cap-ex) records. One entry related to "line costs," disbursements made to local telecom networks to make phone calls and other connections, she discovered. These would normally be characterized properly as routine business expenses, as the cost of generating current income. If so, such disbursements should have been recorded as current operating expenses, not as capitalized expenses, or assets to be written down over future periods.

And it wasn't just that the figures were listed in the asset accounts rather than the expense accounts. Apparently the journal entries, the original books, properly recorded the line costs as expenses; but during the account closing process, they were transferred to the asset accounts–and indeed sprinkled across these. Internal controls should have intercepted the deception. Specific protocols in place should have ensured automatic posting of entries from the original journal into the financial statements during the closing process. Allowing managers to override those systems is an internal control failure.

The controller, in charge of the closing process, rationalized that these line charges would contribute reliably to future earnings, and there was some evidence that this belief was shared in the telecom community. But it did not jibe with GAAP. Several billion dollars of these disbursements were recorded in the cap-ex accounts, as assets on the balance sheet (not affecting the income statement), rather than in the expense accounts burdening net income.191

Treating operating expenses as capital expenditures is an age-old move and there is an age old tendency for the abuser to overdo it, festooning the balance sheet with a bright red flag. A cap-ex account increasing by several billion dollars in a year stands out, even in a company WorldCom's size. After the controller made the overriding adjustments during the account closing process, additional internal controls should have raised a question about the size of these items, another case of internal control failure.

For internal controls to work, however, the company's senior management must want them to work. When the CFO and controller, along with the chairman of the board audit committee, wish to evade internal controls, it becomes far easier to do so. Internal controls must be designed to thwart collusion among senior management that could undermine them—a daunting prescription.

Ideally, defects in internal controls should be discovered during a company's external audit,

---

191 As reported in 2001, line costs tallied about $15 billion, but should have been recorded at $22 billion. The result changed a year's worth of large losses into apparent paper profits for 2001 and 1Q 2002. Also of interest was the apparent fact that in prior years line costs were expensed; the change to cap-exing them in 2001 thus also required some explanation.

and the external audit should discover override capabilities and related concealment. WorldCom's external audit, performed by erstwhile Big Five accounting firm Arthur Andersen, did neither. Andersen in February 2002 issued a report to the company's board audit committee pronouncing internal controls impenetrable regarding determinations of whether to expense or capitalize line costs.192 Any such controls proved utterly porous.

Andersen's report concludes that the company's balance sheets and income statements were fairly presented in accordance with US GAAP, which they were not. Concerning internal controls, Andersen informed the committee that it tested the effectiveness of "transaction processes" in "preventing a material misstatement." In each test, the issue was whether "adequate controls" existed to "prevent a material error" in the financials due to failure to capture transactions, process data and record data in the general ledger. In all areas, WorldCom passed these assessment tests.

But this is wrong on its face. The Andersen report organizes "Line Costs" and "Property Plant & Equipment" under separate headings, with a subheading for the former called "Line Cost Accrual" and for the latter "Capitalization of Assets." This organization and designation uniquely and accurately distinguish line costs from capital assets, underscoring that they are operating expenses.

With respect to Andersen's testing internal controls to assess effectiveness, the report withholds a score for the financial reporting process relating to preparing the financial statements and making related SEC filings.193 If it was premature to assess these matters because they were in process, however, then it was probably premature to say in the report's overview that the financial statements were prepared in accordance with GAAP.194

Many audits and internal controls fail. Neither the WorldCom failure nor those others should be taken to mean that all audits or controls are worthless or destined to fail. Indeed, the lesson to take from the WorldCom case may be that it is often the simplest means of deception that are hardest to deter and detect. The contemporaneous scandal at Enron, for example, was far more complex, pervasive, and long-lived, creating more opportunities for discovery and interdiction. The ongoing complex deception could be missed only by dozing or worse, while the quick bookkeeping sleight of hand at WorldCom could be missed by blinking.

Explanations in the case of WorldCom run from negligence to complicity. In between, and most likely, are weaknesses in internal control systems or audit procedures or both. The issue is the contribution internal controls and external audit make in such a cause. While undoubtedly useful allies in financial reporting and deterring employee misappropriation, they are not guarantors. It remains a disgrace when corporate leaders cheat their shareholders and employees, abetted by leaky

---

192 ARTHUR ANDERSEN, REPORT TO THE AUDIT COMMITTEE OF WORLDCOM, Year Ended December 31, 2001 (Feb. 6, 2002) (WorldCom SEC filing, July 8, 2002), reported in Kurt Eichenwald, *Auditor Gave Assurances of Safeguards against Fraud*, NY TIMES, July 9, 2002.

193 ANDERSEN, REPORT, *supra* note 183, at 8.

194 It is possible that financial statements comply with GAAP but not with SEC rules, making the report's logic unassailable as a formal matter. But to withhold the SEC opinion with specific reference to the processes of preparing the financial statements relates too directly to the GAAP opinion for the formal logic to stand up. The prudent stance would hazard a preliminary GAAP opinion, subject to satisfactory determination of the SEC opinion.

control and audit systems.

Worse still is when controls fail in a broader social campaign. It would be a national outrage if those systems invested with such capacity to aid in a war on terrorism, for example, turned out to offer less value than Congress has tried to lead the public to believe. A look at internal controls in this area suggests associated limits.

B. Control Liability

The importance of distinguishing between internal controls related to financial matters and compliance mandates directed externally is clearest in the case of controls that seek to interdict terrorism, from financing to breaches of aviation security. The following pair of examples illustrates. One relates to the problem of general regulations that must be interpreted into particular controls; the other to voluntary development of controls.

Each illustrates a complementary cost of internal control-liability reliance. The first shows the inherent difficulty of defining requisite controls as well as the way control-failure liability defeats the underlying control goal. The second shows the dubious virtue of allowing voluntary controls to establish legal standards of liability. Both suggest limits in counting on internal controls and dangers in expressing confidence in them by imposing liability for control failures.

1. Pan Am and Lockerbie: From Regulation to Control

An exquisite example illustrating the challenge of translating regulation into control arose from the December 1988 bombing of PanAm flight 103 over Lockerbie, Scotland. The case pit internal controls against terrorism, and terror won. It won in two ways: terrorists evaded detection and the blame-assigning process afterwards led to the dissolution of PanAm, the nation's unofficial flag carrier overseas—an enormous terrorist victory.

At 7:03 pm December 21, 1988 PanAm flight 103 fell out of the sky, 33 minutes into its ascent. Killed were all 259 on board the Boeing 747 plus 11 residents of Lockerbie Scotland where the flight's debris crashed to the ground. After the disaster a massive investigation was mounted to recover and study debris to determine the crash's cause and assign requisite responsibility or blame. Of the tens of thousands of items recovered, a few left no doubt that a bomb hidden in a radio/cassette player smuggled in a Samsonite suitcase caused the disaster and that ultimate blame rested with a Libyan national. Penultimate blame—and liability—rested with PanAm.

The internal control issue related to baggage inspection procedures. Forensic evidence indicated that the suitcase containing the explosion-packed radio originated on an Air Malta flight, with a connecting flight in Frankfurt to London, and finally on to New York. Such luggage, originating at a prior airport and transported from one air carrier to another, is called interline transit baggage. Special inspection rules promulgated by the FAA apply, and US carriers such as PanAm needed internal controls to define requirements and promote compliance.

Rules generally require matching passengers to baggage, with no unaccompanied luggage allowed. For interline transit baggage, this matching system is ineffective, calling for physical inspection of such bags. The internal control issue here hinged on the scope of this physical inspection requirement, and the degree to which compliance officers at PanAm had addressed it, as well as the degree to which PanAm employees on the ground at Frankfurt Airport had executed the directives.

The legal framework for resolving this dispute is the Warsaw Convention.195 In addition to

---

195 A concise history of the Warsaw Convention and the aversion of the United States to it

limiting air carrier liability, the Convention authorizes liability for carriers who engage in "willful misconduct." This is an abstract standard because neither compliance nor noncompliance with applicable regulations is definitive (one can commit willful misconduct while complying with rules to the letter and be free from willful misconduct even when committing rule violations).

In a federal jury trial, PanAm was convicted, and the verdict upheld on appeal to the Second Circuit, with one judge dissenting.196 The chief issue concerned physical inspection of interline transit luggage. On the facts, PanAm followed FAA rules, embodied in PanAm's internal control systems, by matching luggage to passengers for non-interline transit luggage. This duty can be discharged by physical or administrative match. Physical match entails tying each passenger to each piece of luggage, standing on the tarmac; administrative match compares the number of passengers and pieces of checked baggage with the number of bags being loaded on board.

In the case of PanAm 103, administrative match was used and airline staff were satisfied that this more or less ruled out the possibility that the bomb was contained in an accompanied bag (with greater awareness of the willingness of terrorists to engage in suicide bombing, today this inference would less likely be so readily made). As to interline transit baggage, the physical inspection requirement can be met by an employee opening baggage and conducting a visual and direct search or, at least theoretically, by less invasive but potentially more perceptive means such as x-ray analysis.197

This theoretical possibility struck to the heart of the case, because all agreed that PanAm had conducted an x-ray inspection. It was also at the heart of what PanAm's internal control compliance officers had been struggling with. The trial court excluded the compliance officers' testimony, however, and objections to this decision were overruled on appeal. As a result, the jury heard the issue framed in terms of a rule requiring the physical searching via opening of bags and noncompliance with that rule.198

---

appears in Larry Moore, *Terrorist Airline Bombings and the Article 20(1) Defense Under the Warsaw Convention: The Lockerbie Air Disaster Reconsidered*, 25 DENVER J. INT'L L. & POL'Y 25, 27-30 (1996). The Warsaw Convention limits the amounts that may be awarded, a limitation US judges have invented numerous ways around. *Id*. at 25, n. 4. One way around the limits is a finding that injury was caused by a defendant's "willful misconduct" as set forth in Article 25(1) of the treaty. *Id*. at 30. Willful misconduct is a "flagrant violation of a duty intended to protect passengers," a concept akin to common law concepts of gross negligence or reckless disregard rather than ordinary negligence. *Id*. at 32.

196 *In re Air Disaster at Locerkbie, Scotland*, 928 F.2d 1267 (2d Cir. 1991).

197 Potentially more effective in the scope of items that might be detected, particularly small quantities of chemicals spread thinly across sewn-in compartments less visible to the naked eye. The x-ray machine PanAm used for flight 103, on the other hand, was a top of the line machine but nevertheless failed to discover the bomb. A direct human examination may have done so. Internal control designers struggle with determinations such as to require one or the other or both such procedures.

198 Numerous other issues concerning admissibility of evidence arose in the case. PanAm sought to admit evidence showing its procedures were the same as those used by British security regulations, but the trial court excluded this evidence and the appeals court treated this as harmless

PanAm's compliance officers offered to testify that they believed that physical inspection included either physical search or x-ray inspection. During the years preceding flight 103's destruction, the company had sought the FAA's views concerning whether x-ray was a satisfactory alternative way to meet the physical inspection requirement. Obtaining an FAA interpretation of the rules was necessary in order for the compliance officers to prepare appropriate training and compliance manuals for airport ground crews.

The trial court by excluding the testimony, and the appeals court by affirming that decision, treated PanAm's position as an offer of proof that it sought an FAA waiver of the physical search requirement, not an FAA interpretation. This move effectively sealed the company's fate in the litigation because waivers are ineffective unless given in accordance with an elaborate procedure all conceded was not met. (Nor could PanAm have won its case using a mistake of law theory relating to what the regulations required.)

A vigorous dissent challenged the exclusion of the compliance officers's testimony because it stacked the deck against PanAm. The dissent complained that the trial and appellate courts had recast PanAm's argument from an issue of rule interpretation that needed to be translated into internal controls, to one of ignoring clear regulatory requirements.

What divided the dissent from the others is a core problem in all efforts to create internal controls. Any regulation–whether from the FAA, SOX, the SEC, or PATRIOT–is potentially subject to competing understandings. Internal controls and compliance programs are the first interface. Those creating them must make judgments concerning the regulatory meaning. Judicial disagreement in the Lockerbie case underscores the difficulty that compliance officers face translating regulations into policy. The majority's view that the language was clear rendered PanAm's inquiries to the FAA as requests for waiver, not interpretation; the dissent's quite plausible position reflected the reality of an ambiguous directive.

Once an interpretation is made, compliance officers must define a framework for promoting a culture, systems and conduct that will meet the requirements. In the *PanAm* case, even granting the dissent's position that x-ray may have been authorized as a means of control, the next issue would be the handling of the x-ray inspection.

In the context of internal controls, proper handling of the x-ray machine depended on the training component of the internal control system. The most faithful and precise manuals are meaningless if not read, understood, and used. Airline x-ray machines are designed to conduct reviews invisible to human beings using the naked eye and pat down techniques. The machines can see through luggage compartments and other walls and detect some explosives and the like.

Despite that basic advantage of machines over humans, PanAm's x-ray technician reported that he relied heavily on intuition and experience in examining luggage, not so much on the machine. The employee's resort to impressionistic detection may have been necessary by default,

---

error. *PanAm* at 821. The trial court excluded PanAm's expert testimony concerning the security risk of unaccompanied luggage, an error the appeals court held was cured by a jury instruction. *PanAm*, at 822. The trial court admitted plaintiffs' evidence concerning unrelated security issues, and the appellate court said while prejudicial, it was proper as it related to causation. *PanAm*, at 824. The appellate court likewise found harmless error in the trial court's allowing plaintiffs' expert to testify that PanAm violated FAA regulations, *id*. at 827, and that PanAm was not permitted to demonstrate the effectiveness of is x-ray since plaintiffs stipulated as to its effectiveness. *Id*. at 828.

however, for the employee had only been on this job for seven weeks.

That short period raises the related internal control matter of employee seasoning. For particularly sensitive tasks, including most concerning airline security, new recruits commonly are designated as trainees during a probation period when senior employees work alongside them. The PanAm103 technician may have lacked training and technical experience that could have shifted his reliance from intuition to technology.

But he makes a more universal and important point in saying he had developed a sort of sixth sense for airline security. That is what effective experts do, and it is something not always possible to define in a manual or include in training procedures. Neither the manual nor training constitutes a compliance program. In short, machines are not the ultimate defense, people are.

Another control in place, but not met in the *PanAm* case, called for crew to notify a plane's pilot when unaccompanied interline baggage is to be placed on board. Reporting up the chain of command is a standard feature of internal controls and compliance programs. It is also one of the most difficult for line employees to meet. This is particularly the case where there is a meaningful risk of management rebuke. Baggage handlers who have x-rayed an unaccompanied interline bag, based on a good faith belief in this technology's reliability (and possibly even superiority), may worry that reporting its presence to a pilot will result in criticism for failing to open and examine its contents.

Additional unfavorable evidence relating to employee recruiting and training aspects of internal controls arose in the *PanAm* case. PanAm's head of security at Frankfurt had a checkered record, having passed bad checks in the US and used a company credit card at a brothel.199 A ground crew member responsible for identifying high-risk passengers for special examination ("selectees" in airline security parlance) could not define what a selectee was.

The majority-dissent disagreement in the PanAm case carries further implications for internal control theory and practice. Suppose, as the majority opinion saw it, the procedures were violated in a willful manner, as the Warsaw Convention requires to impose liability. However, the conviction says nothing about any need to improve the procedural specifications, for the clearest letter and protocol could, and some were, willfully violated. What could be improved under this view were those controls relating to compliance.

Under the dissent's view, greater clarity in internal controls themselves would have helped, as by expressly requiring human direct inspection. Following either view, however, note that both protocols can fail, either due to willful misconduct or ordinary carelessness or flaw. This reality suggests a tougher internal control specification, to require both checks. This is a redundancy protocol, a prominent characteristic of many internal control systems.

Not even redundant systems guarantee 100% compliance, alas, as other PanAm lapses suggest. Proper training must be furnished, employee's backgrounds must be checked, and so on.

---

199 This is the kind of employee background that the OSGs discourage in their internal control guidelines calling for avoiding awarding discretion to staff with criminal tendencies. *See supra* Part II.A.

There can be no assurance that beefing up on any of these fronts would have prevented the PanAm Locerkbie bombing, though having them increases the probability of success.

The issue is the magnitude of the savings versus cost of alternative trade-offs. In the case of airlines, speed and passenger convenience is compared to the cost of guaranteeing no detonated bombs or other instruments of terror put passengers and crew in harm's way. At one extreme, modest incremental costs such as prohibiting unattended cars at airport curbsides would easily pass, while extraordinary measures such as shutting down regional airports would just as easily fail. More subtle measures, such as passenger profiling, are far harder to measure in either the benefit or cost dimensions.

With respect to internal controls, employee screening, training and supervision to assure minimum protection is warranted. But more elusive is specifying the exact content and duration and timing of these techniques. Also to be considered are payback of baggage screening, bomb and chemical detection mechanisms, ranging from personal search to x-rays, dogs, and other controls. Equally elusive is the business of testing these cost-benefits. Common sense, prudence, and judgment become the tools of the internal control designer and compliance officers, not to mention regulator, rather than social science techniques of measurement, weighting, probabilistic calculations and statistical break-even points. This remains the case despite increasing experience with both sides of the equation.

The lawsuit against PanAm in the Lockerbie bombing case resulted in a judgment that sealed the company's demise. The company sold its European routes to Delta and its Latin American routes to American Airlines. Its former world headquarters in New York City, the fabled PanAm building, was also sold. That symbol of PanAm's might reflected other national identify characteristics of the company, including that it served as the unofficial US flag carrier. More than the loss of life, destroying national US symbols is exactly what terrorists seek. Lawsuits against companies used by terrorists thus feed directly into their hands. Surely this is not a role our system of internal controls ought to perform.

Terrorists were to blame. Yet the factor of internal controls enabled our legal system to blame the companies and their employees instead. This is a substantial change of traditional tort principles. Doctrines of causation and foreseeability would have sealed these defendants from liability. Especially under the willful misconduct misconduct standard applied, factors in addition to the baggage screening practices should have been admitted and would have exonerated the company.200

---

200 Comparing the majority and dissenting opinions in *PanAm* suggests a passion crept into the trial judge, jury and appellate court majority. As the dissent points out, the trial court treated it as a criminal case where the defendants flouted clear law. Another avenue of defense uses Article 20(1). Moore, supra note 186, at 44. It absolves defendants of liability when they can prove they took all reasonable and necessary measures to prevent the injury that arose. This section makes it harder for courts to exclude testimony and evidence of the kind excluded in the case. Under this approach all the following testimony would have been admissible:

- PanAm sought and thought it obtained an FAA interpretation that x-ray was acceptable to meet the physical inspection requirement;
- the FAA had often inspected PanAm's Frankfurt systems before and after Lockerbie
- PanAm was never cited by regulators for using x-ray

Consider the contrasting example of litigation following the 1993 World Trade Center bombing. The Port Authority of New York and New Jersey, owner of the World Trade Center, sued the companies which made the fertilizer products the terrorists used in their bombs.201 The theories were negligence and products liability. The lower court and an appellate court dismissed the case without a jury trial, the company having no duty to the Port Authority and the attack having not been proximately caused by their manufacturing activities not having met requisite foreseeability tests.

A concurring judge sounded a more capacious liability note. While he agreed with the application of traditional tort principles to cut off liability, he offered what he called "an observation which may bear the fruit of protection from further similar disasters." The legal grounds of the case were thin. But with experience he predicted that our society will develop new legal duties that shift or create responsibilities on manufacturers of products attractive to terrorists.

The concurring judge's prediction becomes more likely in 9/11's wake and other catalysts of the controls culture. Controls can be seized upon as forging a broader set of duties owed to a broader class of potential plaintiffs. It remains misguided. Encouraging companies to take reasonable steps to reduce the prospects of terrorists mis-using their products may be desirable. But pushing fiduciary duty law and negligence arising from internal controls as a way to do so risks a backfire. In the *PanAm* case, ensuing liability for internal controls failure did more for the terrorists' cause than the actual bombing of the airplane.

2. TWA and Athens: Informal Controls

The issue of redundant screening as an internal control also divided the majority and the dissent in the case of Ospina v. TWA.202 As TWA Flight 840 approached Athens airport on

---

- the Pentagon relied on x-ray screening
- the FAA shortly after Lockerbie approved x-ray screening at all airports
- the U.K., facing IRA threats, used x-ray screening
- PanAm's x-ray was the most effective and expensive available

In short, this evidence would have supported the common sense claim on which PanAm's practical defense rests: it was most unlikely for a terrorist to plant a bomb in a suitcase bound for flights criss-crossing a continent and performing multiple take-offs and landings.

201 *Port Authority of N.Y. & N.J. v. Arcadian Corp*., 189 F.3d 305 (3rd Cir. 1998).

202 975 F.2d 35 (2d Cir. 1992).

April 2, 1986, a bomb exploded, killing four passengers and injuring others. Although the bomb created a large hole in the fuselage, the airplane landed safely. Passengers or their next of kin sued and all but two settled. The hold-outs sought damages and after a bifurcated trial, both won. TWA appealed, and the court reversed, over a dissent.

Evidence and other information arising in the case were so critical to the security and safety of commercial airlines and passengers and anti-terrorism strategies that much of it was filed under seal. Moreover, much of the trial was closed to the public, the trial transcript released daily only after US attorneys were given a chance to redact sensitive portions, and some grounds of decision were not published. Assessing whether the majority or dissent had the better of it is difficult because of the protective procedures used throughout the case including in each opinion. But there's enough surface difference offering useful lessons from the case relating to internal control procedures.

The legal framework of the case was again the Warsaw Convention, calling for a determination of whether TWA and its employees engaged in willful misconduct. To win, passengers needed to show TWA wrongfully neglected to perform certain acts that could have prevented the bombing. TWA stressed its compliance with FAA and local laws, versus the passengers' argument that a known terrorist boarded the plane without adequate screening applied to her or her baggage or two procedures often but not routinely (at that time) used to examine a plane's cabin and cockpit.

The majority saw it as a simple case. It said the sole issue was the sufficiency of the facts the passengers brought forward. It concluded that no reasonable jury could have found willful misconduct. The majority emphasized both the non-routine character of the procedures the passengers complained that TWA did not take as well as TWA's compliance with all applicable laws (in contrast to both the majority and dissenting opinions in the *PanAm* case). The majority conceded that if "TWA had searched the place where the bomb was hidden, the bomb would have been discovered. That would be true in any case involving a hidden bomb. However, the test for willful misconduct is not 20-20 hindsight."

Dissenting Judge Eugene Nickerson saw the case as posing a major policy issue for safety on commercial air carriers, specifically whether a carrier should receive shelter from liability under the Warsaw Convention if it willfully abandons passenger screening procedures it had for many years agreed to follow. The trial court had recorded his view that TWA allowed a known terrorist aboard in flagrant violation of many basic security measures. While most of these were kept under seal, the dissent singled out one for public reference.

Under Egyptian law, only Egyptian authorities were permitted to conduct physical searches of passengers at Cairo Airport. But the US government and US commercial airlines, including TWA, had determined that Egyptian security was inadequate at Cairo. As a result, prior to 1986, US carriers were required to conduct redundant screening in Cairo of all passengers, meaning screening done by TWA, in addition to that applied by Egyptian airport personnel. Though this requirement was not formalized as a regulation, TWA recognized it as essential and in fact continued it over the years. The practice was in effect at the time of this bombing, and had assumed added significance in the light of increased terrorist activities in the Middle East and elsewhere during the period.

But TWA and its workers employed laxer standards in this case. A female passenger was ticketed for boarding the flight. She was known as a "profile selectee," a would-be passenger posing a sufficient security threat to require careful screening. TWA escorted the profile selectee to the gate where it was equipped to do its own redundant screening.

The gate was closed and TWA did not ask the Egyptians to reopen it. Nor did TWA deny the profile selectee boarding, although it could not screen her. Instead, it handed her over to Egyptian security personnel at that gate, who took her into a private room, in which only she and the Egyptians know what happened, and allowed her to board. While exactly what happened in the private screening is unknown, it was clear that TWA never electronically screened her carry-on luggage and never checked her or her luggage with metal detecting hand wands. This redundant screening could presumably have detected bomb components. These procedures would have been done had TWA followed its standard practice, one it had agreed with the US government to adhere.

The dissent viewed this noncompliance as equivalent to willful misconduct, sufficient to support the jury's liability verdict against TWA. As to the formality underlying the promulgation and articulation of the procedure, the dissent viewed as irrelevant that the requirement was not in writing. *De facto* requirements are no less requirements for not being written down, it said. Although the dissent could not discuss the details in this sealed opinion, the record shows that once TWA abandoned the requirement for redundant screening, the airline had no adequate procedures to repair the breach.

The danger in Nickerson's position dissenting in the *TWA* case is it creates disincentives for compliance officers to develop voluntary protocols geared toward protecting corporate interests and the public from terrorist infiltration. To the extent best practices become legal mandates, compliance officers may be reluctant to serve as leaders in their development or even to follow control trends. The ideal environment to dispatch private corporations as soldiers in a war on terrorism is not threat of legal recrimination for failing to do so but rewarding leadership in the effort. Willfully ignoring regulations or controls may warrant liability, but good faith should be enough to defeat it. This means building a merit system rather than a liability system with respect to internal controls—at least for terrorism.

C. Control Horizons

PATRIOT's internal control provisions are more directive than those in *PanAm* and mandatory compared to those adopted voluntarily in *TWA*. The statute's regime nevertheless shows that directive specificity alone does not render internal controls any more reliable and that their appeal remains greater than what law should justifiably expect.

PATRIOT's specific internal control directives apply to the financial services industry, defined very broadly. They are principally intended to interdict money laundering. In brief, money laundering is the conversion of the monetary proceeds of an unlawful activity–ranging from drug dealing to income tax evasion–into funds with seemingly lawful origin. Businesses and charities can transfer their cash into terrorist channels this way, and also use those operations as fronts to channel funds generated from criminal activities such as smuggling of jewels and tobacco or kidnapping.203

---

203 Money laundering entails three separate steps. The first is called "placement," the physical positioning of tainted funds into the above-ground financial system. This could occur at any point in the financial pipeline–a casino, a securities brokerage, a bank, or car dealer. The launderer could pay dirty cash for a new car, for example, and turn around and sell that car to a second dealer in exchange for a cashier's check. The second is "layering," the successive movement of funds through a series of banks and other financial institutions, often in different countries, to blend the dirty cash into the clean stream. With sufficient cycles, the dirty origin is obscured and the resulting cash looks clean. The car dealer's check is deposited into an account. Funds in that account are

Many countries tolerate or condone money laundering, with some officials and bankers even partaking as beneficiaries.204 In the US, the practices are abhorrent, evidenced by the 1970 Currency and Foreign Transaction Reporting Act (Banking Secrecy Act or BSA), which requires financial institutions (banks, money transfer services, wire services, car dealers, travel agents and insurance companies) to report currency transactions greater than $10,000. 205

Money laundering appears to be critical to financing global terrorism and providing funds for terrorist attacks. It is relatively easy to practice money laundering due to the transparency, fluidity, and freedom-based characteristics of US financial markets and structures.206 Noting the leaky structure of U.S. financial markets, Congress announced that U.S. anti-money laundering efforts were outdated and complex and used parts of PATRIOT to seal the leaks.

PATRIOT gives the Treasury Secretary control over developing and implementing regulations requiring financial institutions to share with regulatory and law enforcement authorities information regarding individuals and organizations suspected of terrorist acts or money laundering.207 PATRIOT expands the responsibilities of the Financial Crimes Enforcement

---

transferred to another account and so on. The final step, "integration," culminates with the cash moving in legitimate uses or, sometimes, back into the dirty rivers of illegality where the money came from (terrorism, drugs, kidnapping). Funds from the car dealer shifted through a series of accounts are withdrawn when needed to fund ordinary operations. The process obviously gets easier with each successive step, with placement the most risky and integration the culmination. Law enforcement thus concentrates most of its efforts proportionally earlier in the process.

204 Among the most indulgent countries are those listed by the US as sponsors or practitioners of terrorism, including Iran, Iraq, North Korea, Syria, Libya, Sudan, and Cuba. Global safe havens are countries where it is easiest to engage in these activities while retaining a modicum of respect. These countries tolerate money laundering at the political level, and share such characteristics as: no information sharing agreements with other countries, instant corporations are available, offer state-of- the-art electronic communication systems, have rigorous bank secrecy laws and/or use the US dollar or other major currency as the local currency. Leading examples are Bermuda, the Cayman Islands, Channel Islands, Jersey, and Liechtenstein.

205 Under the BSA, annual filings of currency transaction reports exceed 12 million and suspicious activity reports exceed 150,000. 2002 National Money Laundering Strategy, at 43-44: (Bank CTRs totaled 13,040,064 (2000) and 12,594,533 (2001); Casino CTRs 342,320 (2001) and 380,858 (2000); Bank SARs totaled 153,502 (2000) and 182,253 (2001) and Casino SARs totaled 436 (2000) and 1,149 (2001)).

206 Offshore banking and related facilities designed to provide anonymity are used to disguise ownership and movement of criminal funds, thus making it difficult for law enforcement officials and regulators to track the money generated and used by terrorists. Private and correspondent banks are susceptible to manipulation by foreign banks and money launderers by hiding the identity of parties involved or allowing offshore accounts to be created.

207 Areas of concentration are (1) how terrorists transfer funds (for example through charitable organizations and non-profit organizations); (2) the relationship between international narcotics traffickers and foreign terrorist organizations; and (3) identifying accounts and transactions

Network (the "FinCEN"), founded in 1990 and part of the Department of the Treasury.208 Both direct that the private sector use internal controls to feed information into FinCEN.

Regulations require financial institutions—not just banks—to designate one or more persons to receive information and monitor accounts involved in potential terrorist activities and establish procedures to protect shared information.209 Financial institutions are encouraged and sometimes required to establish anti-money laundering programs rooted in internal controls. Mandates include designating a compliance officer, creating an on-going employee training program and creating an independent audit function to test anti-money laundering programs.

Enhanced due diligence requirements are required to establish, maintain, administer, or manage private banking accounts.210 Controls must be designed to detect and report instances of money laundering through these accounts. At a minimum, institutions must take reasonable steps to ascertain the identity of the nominal and beneficial account owners, identify the source of the funds in accounts, report any suspicious transactions, and conduct enhanced scrutiny to detect and report transactions that may involve the proceeds of foreign corruption. Due diligence programs are to be tailored to the financial institution's: line of business; financial products and services; size; clientele; and location. The institution's program must evaluate and consider risks associated with different foreign financial institutions, private banking customers and other relevant factors. These due diligence programs are to be melded into existing programs mandated under BSA.

Another layer of control PATRIOT imposes requires financial institutions to provide suspicious activities reports ("SARs"). Long a requirement imposed on banks, PATRIOT extends the SAR requirement to include all financial institutions designated by the Treasury, which extends as far as the rest of PATRIOT. SARs are intended to furnish federal authorities and intelligence agencies information regarding the types of financial activities taking place in US financial

---

involving terrorist groups. PATRIOT mandates increased scrutiny of foreign financial institutions and domestic ones operating outside the U.S. It targets classes of international transactions or types of accounts that pose particular, identifiable opportunities for criminal abuse.

208 FinCEN is a highly secure, government-wide data access service and financial communications center. It provides global alerts regarding suspicious activities. FinCEN's Director is appointed by the Treasury Secretary and advises and makes recommendations concerning financial intelligence, financial criminal activities and other financial activities to the Under Secretary of the Treasury for Enforcement. The Director is also responsible for maintaining the government-wide data access service, including maintaining, analyzing and disseminating information collected throughout the financial infrastructure.

209 The information gathered from these sources will be incorporated, by the Secretary, in a semi-annual report, which will be published and disseminated to financial institutions to provide consistent information about patterns of suspicious activities and other insights. The Act encourages the President to push for like reforms in negotiations with foreign financial officials and institutions doing business with U.S. financial institutions, particularly to maintain adequate records of transactions and account information and provide these to U.S. law enforcement officials and domestic financial institution officials.

210 Private banking accounts are those requiring a minimum deposit of $1,000,000, owned directly by the person establishing the account and managed by the financial institution.

institutions. PATRIOT encourages financial institutions to make voluntary disclosures about suspicious customers, though they are not permitted to inform people that they have been reported and face no liability to them for doing so. The provisions also sweep into PATRIOT all money transmitters, large and small, whether through formal or informal networks and whether domestically or internationally. All must develop requisite internal controls and all must file SARs.

Financial institutions need to know exactly who their customers are to file accurate SARs. To that end, PATRIOT authorizes the Secretary to impose regulations regarding customer information gathering. At a minimum, these regulations may require financial institutions to (1) verify the identity of customers opening an account; (2) maintain records of identity (name, address, other vital information); and (3) consult a terrorist list to determine if a customer is on it. Foreign governments are encouraged to require the name of wire transfer senders be included on transfer forms from its point of origination through the point funds are disbursed.

PATRIOT's controls drill directly on combating money laundering intended to fund terrorist activity. Banks may have skills in detecting strange activity indicating money laundering. In fact, credit is claimed that the banks have played a role in changing criminal behavior by their reporting.211 The working hypothesis, which all agree is untested, holds that banks can identify terrorist financiers specifically and that other organizations can effectively join banks in doing both.

It is far from certain that non-banks have such skill or capability and even more uncertain whether banks or any other financial institution–or organization of any kind–can distinguish money laundering conducted by drug traffickers or tax cheats, say, versus terrorists.212 To give a sense of scale, the money service business (MSB) industry alone consists of 160,000 independent or local outfits throughout the US, in addition to 8 multi-national corporations.213 These have never before been subject to such regulations and adjusting to them will be costly, confusing, and, one fears, unlikely to pay off.

Securities brokers and dealers are far more integrated and organized, represented as a trade group by the Securities Industry Association (SIA). The SIA promptly responded to the Act by publishing a pamphlet entitled "Preliminary Guidance for Deterring Money Laundering Activity," through its Anti-Money Laundering Committee. This catalogued the requirements of the Act in plain English. It also illustrated hypothetical situations with concrete examples. These focus on what constitutes "suspicious activity," when an account is opened and subsequently.214

Drawing on literature used by banks in their experience with the BSA's SAR requirements,

---

211 *E.g.*, 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 40.

212 The Secretary of the Treasury and the Attorney General announce in their 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 20 (one assumes they meant Anti-Money Laundering Strategy): "Law enforcement, in coordination with the financial sector and international bodies, is attempting to determine if there are any specific indicators of terrorist-related."

213 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 43, n. 51. As of that report's date, July 2002, fewer than 10% of MSBs had registered with FinCEN as required. *Id.* at n.52.

214 The suspicion in the case of financial services relates to account data that deviates from norms. The baseline deviation includes the account's history as well as accounts of similar type. In securities trading, Medicare billing, defense contracting, and other foci of internal control administration, similar concerns of suspicion arise, requiring and producing similar standards.

various triggers at the outset are highlighted, starting with customer concern about regulatory compliance and reporting, particularly as to the customer's identify and business. Second, customers who seek accounts or transactions lacking business sense or that are inconsistent with stated objectives. Third, a suspect background or affiliation, including press reports of "possible criminal, civil or regulatory violations." Fourth, those appearing to be acting as agents for another party but who are not forthcoming about the other entity. And finally, customers who can't readily describe the nature of their business or who lack knowledge of basic industry facts.

A longer list of triggers is offered concerning activity after accounts are opened. Hordes of cash is the first tip off, whether in single large ($10,000+) doses or lots of smaller ones. Likewise are multiple fund transfers lacking apparent business purpose to or from laundry-friendly countries, including those with favorable bank secrecy laws or with reputations as tax havens. Other tell-tale signs, if lacking an apparent business purpose: sudden substantial wire transfers, quick round trips (deposits and transfers), purchases of long-term assets promptly followed by liquidation/distribution orders, multiple accounts under a single name, transactions involving legitimate but launder-enabling securities (such as penny stocks, Regulation S stocks, and bearer bonds) and–the best–a "customer exhibits a total lack of concern regarding risks, commissions, or other transaction costs."

The SIA is at one extreme, seemingly well-prepared to take up the demands of PATRIOT, while the MSB is at the other, with most hardly even aware of PATRIOT's new requirements. The costs in both cases, however, are high or uncertain at best. The costs and uncertainties are reflected in the individual public filings of affected businesses. They fall into three categories. At one extreme companies exhibit confidence that PATRIOT will have no material effect,215 while at the other companies say they are unable to predict what the effect will be,216 and a third group lying somewhere in between, indicating that they don't foresee any material effect but can't really be sure.217 All this disclosure reflects the common sense and obvious point that there will be costs. The agencies recognize compliance costs as well. They advertise their inclination to balance law enforcement needs against those costs (as well as privacy risks).218

The education and training required are substantial, particularly considering that most of the targeted sectors have no experience with anti-money laundering regulations.219 Likewise, the regulators have no relevant experience with those industries. Each is called to educate the other and

---

215 *E.g.*, LNB BANCORP, SEC FORM 10-Q (filed May 15, 2002) ("Management does not believe that PATRIOT will have a material impact on the financial position, results of operation or liquidity of the Corporation").

216 *E.g.*, MAINSTREET TRUST INC., SEC FORM 10-Q (filed May 15, 2002) ("To date, it has not been possible to predict the impact PATRIOT and its implementing regulations may have on the Company or its subsidiary banks in the future.").

217 *E.g.*, MOUNTAIN BANK HOLDING CO., SEC FORM SB1 (filed March 22, 2002) ("While we believe PATRIOT may, to some degree, affect our record keeping and reporting expenses, we do not believe that it will have a material adverse effect on our business and operations.") Disclosure in this area is becoming more uniform.

218 *E.g.*, 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 40.

219 *Id.*, at 41.

this sort of learning is neither cheap nor a high-probability pay off. On top of this, of course, are federal rules limiting the ability of private sector groups from participating in executive branch policy making.220

Costs tend to linger. For example, the volume of currency transaction reports, required at the $10,000 level, has skyrocketed to a dozen million annually. In 1994, Congress passed legislation creating exemptions from the CTR reporting requirements for certain low-risk transactions, such as those conducted by governmental agencies, fellow banks, and stock exchanges.221 Yet the CTR level did not drop off and banks continued filing reports in exempted areas. PATRIOT directed the Treasury to look into why this is so, but it is a good bet that it is more expensive to alter controls to filter for and omit the exempted transactions than to file extra reports.

On the benefit side of PATRIOT's equation, payoff odds are low. These reports have sometimes worked to catch launderers, famously the Bank of New York customers Peter Berlin and Ludmila Edwards, Russian operators of an illegal money transmittal business.222 But no evidence indicates the catching or interdiction of terrorists. Conversely, bragging rights are taken for catching terrorists running a cigarette smuggling ring in the US to raise funds, but these were caught because of ordinary law enforcement on the street rather than via SARs or other tips.223

While aggregate organizational budgets of many terrorists groups are large, discrete cells can sometimes get by on the cheap and appear to have great patience.224 Moving sums lower than sensible SAR and CTR thresholds is easy, and an obvious strategy. It defeats the regulatory structure, rendering the expense wasted. Launders will always conduct regulatory arbitrage, looking for the next loophole to outsmart the regulators. And regulators must be equipped and eager to stay one step ahead. Designing prophylactic strategies to preempt the launderer's next move is sensible, as from moving from Citibank to E-Trade, for example. But this does not mean every avenue must be pursued or any should be pursued without assessing the costs.

To take a concrete example, what are the odds that these new controls will work to prevent financing of terrorism, to catch terrorists before they act? In the case of the 9/11 hijackers, amounts used ranged from $2,860 to $69,985. Records show funding to the hijackers in the early part of the period and returns of balances by them just before or on September 11. Up-front funding for most of the group, from June through September 2000, consisted of bank transfers from UAE to New York or Florida banks in amounts of $4,790, $9,985, and $9,485 followed by $19,985 and $69,985. Advance funding for the alleged hijacker who missed his flight began upon his entry into the US with $35,000 cash in February 2001.

---

220 *Id*.

221 31 U.S.C. § 5313(d)-(g).

222 *E.g.*, 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 30.

223 *E.g.*, 2002 National Money Laundering Strategy, at 20 (boasting of the jury conviction in a side bar accompanying narrative discussing terrorist financing methods and role of banking and financial industry in law enforcement). *United States v. Hammoud* (Grand Jury Indictment, Docket No. 3:00CR147-MU) (24 defendants). The case is discussed in detail in LAWRENCE A. CUNNINGHAM, CRACKS AND SEALS (manuscript 2003).

224 *See* CUNNINGHAM, CRACKS AND SEALS, *supra*.

Meanwhile two conspirators opened bank accounts in UAE using cash in June 2001 that was eventually used to fund credit card charges and ATM withdrawals of the others in amounts less than $5,000. One suspect received wire transfers of $15,000 from the UAE to Germany in July 2001 and turned around and made wire transfers of $14,000 from Germany to the US. During the five days before September 11, a half dozen or so wire transfers were made from various hijacker accounts in the US to an account in the UAE–$8,055; $2,860; $5,000; $5,000; $5,400; along with a deposit in the UAE to the same account of $16,348 and the account at that bank of the hijackers was drained to zero.

Are these sufficiently suspicious activities to have warranted reporting? Apparently not, because the banks didn't despite being subject to the BSA and its SAR reporting system before September 11. Any currency transaction reports filed to address the handful of transfers exceeding $10,000 would have been lost among the other dozen million filed in 2001. The only relevant difference PATRIOT creates is that now all other financial institutions must do the same. The effect is likely to produce the same result: nothing. As with so many goals that internal controls have been designed to meet, this one more likely will produce false complacency rather than effectively achieving the ultimate goal.225

225 Yet there's no need to despair. Just because corporate internal controls may be unreliable and costly allies in a war on terrorism, many other allies exist. First, and most obviously, is voluntary reporting. FinCEN, belatedly in the scheme of things, but promptly after September 11, 2001, established a hotline for financial institutions to report transactions raising suspicions of terrorist financial activity. *See* 2002 NATIONAL MONEY LAUNDERING STRATEGY, at 20. Second, and equally obvious, is ordinary law enforcement. As much as the Department of Justice emphasizes the importance of the private sector in conducting its work, its member agencies along with state and local forces perform an extraordinarily able job in the ordinary course of identifying and catching crooks, money launderers and terrorists included. The relative effectiveness of combating a long-running terrorist financing operation using corporate internal controls versus state troopers on the highways, is shown by the case of the Hezbollah Cigarette Smugglers. *United States v. Hammoud* (Grand Jury Indictment, Docket No. 3:00CR147-MU) (24 defendants). *Cf.* V. S. Khanna, Corporate Crime Legislation: A Political Economy Analysis, SSRN (theorizing rise of corporate crime legislation as product of desire of corporate managers to avert civil liability, an explanatory thesis that this Article suggests should be prescriptive).