Sarbanes Oxley, Corporate Governance and Operational Risk

Alan D. Morrison
Saïd Business School, University of Oxford
and 2020 Governance AB, Stockholm

Sarbanes-Oxford Seminar,
22nd July 2004

1. Introduction

I have been asked to open this seminar with a general discussion of the Sarbanes-Oxley Act and its wider implications, with particular reference to operational risk management. I shall be approaching the subject from the perspective of an academic financial economist: naturally there is a danger that I will stray into territory which is better covered by the functional experts who will speak after me. I apologise in advance for any such transgressions, and I am sure that they will be corrected later in the day.

Ultimately I want today to deliver a clear outline of some of the salient points in the Sarbanes-Oxley Act, and to discuss their implications for the firms which have to comply with the Act. To do this properly I will have to take a step back from the precise content of the legislation, and start by discussing the economic and legal environment into which the Act was introduced. I will discuss the purpose of corporate governance, and will outline international variations in approaches to corporate governance. This will provide the basis for an analysis of the regulation of corporate governance. In both the discussion of governance and of its regulation, I will stress the importance of contracting and the problems which a failure to contract can cause.

There is a general consensus that the accounting scandals which arose in the early years of this century in the United States were evidence of failures of US corporate governance. Whether or not this is true, they certainly provided the catalyst for changes to governance law. The Sarbanes-Oxley Act, which was passed in the summer of 2002, is probably the most sweeping reform to US corporate governance law since the adoption of the initial federal securities laws of 1933/34. The law represents a shift from disclosure-based legislation to substantive regulation of procedures and practices. I shall discuss some of the most important points in the legislation with reference to my general statements about governance and its regulation, and I shall highlight some important consequences for non-US firms with US listings.

Finally, I shall spend some time asking whether Sarbanes-Oxley could represent an opportunity as well as a cost. It seems that the area in which this is most likely to be the case is operational risk management. Several experts will speak later in the seminar about the problems of creating operational risk management systems and the associated technical issues. Rather than attempting

to pre-empt their contributions, I will concentrate in this discussion upon conceptual issues: how we should define operational risk, how it can be measured, and some standard statements about operational risks which strike me as ill-conceived. This type of analysis can help us to understand where and how operational risk reporting systems can add value. My arguments will relate to the problems of definition, and how correct definitions can serve as the basis for contracts between investors and the firm. In this area, the Sarbanes-Oxley requirement for accurate monitoring and prompt reporting of operational problems may actually increase the values of corporations.

2. Corporate Governance

Suddenly policy-makers and the media are concerned with the phrase "corporate governance". The phrase is seldom defined and it is used in a variety of contexts. It is of clear relevance in the context of this seminar so I will start by discussing its meaning. It is difficult to do so, because the structures to which it refers differ so much from one country to another. I will start by discussing the Anglo-American corporation, which is of course the focus of the Sarbanes-Oxley legislation, before highlighting some alternative approaches.

In the US and in the UK, an important characterisation of the corporation is the separation of ownership from control. Financial capitalists provide investment in the form of equity or debt, while human capitalists provide their labour and work as managers in order to maximise the return which the firm makes on its assets. Insofar as financial capitalists need not be endowed with the managerial skills required to run a business, this system is an efficient one. It allows for efficient financial risk-sharing as well as for efficient asset allocation. But division of responsibilities does not come without a price. The corporation's managers may be more concerned with their personal returns than with those of the corporation. The financial capitalist cannot necessarily observe the manager's behaviour and so some economic inefficiency is likely to arise: while the manager is capable of allocating assets efficiently, in practice he may elect not to do so (for classic discussions of this problem see for example Jensen and Meckling, 1976, Fama and Jensen, 1983, and Jensen, 1993).

This problem is not a new one: Adam Smith (1776) recognised the problems stemming from the separation of ownership and control when he said

> "directors ... being the managers rather of other people's money than of their own, it cannot well be expected that they should watch over it with the same anxious vigilance with which the partners in a private copartnery frequently watch over their own."

Another early and classic analysis of the principal-agent problem in corporations is due to Berle and Means (1932). Quite apart from the inequity of managerial theft, it is the source of economic inefficiencies. When investors anticipate that their funds will not be well deployed, or that they will not receive the income which their investments generate, they will reflect any returns shortfall in the prices which they are prepared to pay for their shares. So firms lose up-front from the anticipated behaviour of their managers. In other words, managers pay in terms of lower salaries and reduced access to the capital markets for their misdemeanours. The increased cost of capital

market access will serve to raise the returns hurdle for investments and some perfectly satisfactory investments will not be made.

In the long run, managers will therefore not gain from perquisit consumption if it is anticipated by investors. If they could, managers would prefer to give a binding promise not to engage in this type of behaviour. In practice, such commitments are hard to police and to enforce in the courts and so after the fact they are likely to be broken. But it is important to emphasise that *both the manager and the investor would prefer a world in which such a commitment could be made.* Furthermore, such a world would see more productive activity: everyone would be better off.

Corporate governance in the UK and the US refers to the mechanisms by which managers attempt to bind themselves *ex ante* to rules governing their behaviour when they are raising funds.[1] In practice, this occurs at the time their companies are floated. Some of these rules are company-specific and are written into the corporate charter. Bilateral contracts do not in general seem to suffice, though. They are hard to police, they are extremely complex, and they are hard to enforce in the courts. Certainly, small investors would be less willing to invest in shares if for each investment they had to familiarise themselves with the contents of a fresh corporate charter, and if they then had to concern themselves with enforcing the charter. In cases like this (bankruptcy law is another) it is widely accepted that the financial system will function more effectively if there is a standard set of laws, and every firm abides by them. This reduces the floatation-specific costs of drafting laws, lowers investors' learning costs, and allows for some centralised enforcement. These gains will for good laws outweigh in general the specific costs which a firm might experience in forcing itself into the local legal straightjacket rather than designing its own governance arrangements.

Standard legal requirements in the UK and the US have in the past focussed upon disclosure: firms have to publish audited accounts and they have to report market-sensitive information to their outside investors in a timely fashion. Disclosure is valuable in shareholder economies because it ensures that the share price reflects as much of the available information as possible. Indeed, there is a strong body of evidence to suggest that share prices do respond rapidly to new information.[2] An accurate share price has two roles: firstly, it facilitates asset allocation in the sense that investors can tell which technologies and ideas have in the past been successful; secondly, it facilitates the market for corporate control. Poorly performing managers may face a hostile takeover; at the least, they are likely to be fired. The associated incentive effects are obvious.

Non-disclosure governance arrangements might relate to institutional features which, even if not legally mandated, serve to convince investors that managerial slacking or incompetence will be hard to hide. For example, instituting an appropriately constituted risk management committee may serve as a commitment not to gamble with investors' funds. In the same way, you might find a commitment to abstain from coffee more convincing if it came from someone who had signed a legally-binding contract to pay £10,000 to a friend if she caught him drinking it.

I am concentrating here upon the rationale for corporate governance: in the UK and the US it is a means of binding managers to act in the best interests of their financial investors. It is hard to write and to enforce binding contracts governing every aspect of the firm's business and

[1] Shleifer and Vishny (1997) provide a useful recent survey of the thinking on this topic.

[2] See Fama (1970) and Fama (1991) for reviews of the evidence.

so there is a body of standard rules for publicly quoted companies relating to their reporting and to a lesser extent to questions like Board composition. While managers might prefer after signing the contract to renege upon it, they will always wish to find the contract which *ex ante* most convinces their investors that they will not do so. Some press comment associates governance with wider issues like the relationship of the company to its employees, to its community, or to the environment. For the purposes of today's discussion I do not think that these are relevant. For example, standard arguments from economics state that when they are free to take their labour elsewhere, employees will extract a fair return on their skills in bilateral bargaining with a firm whose objective is to maximise its return on financial capital. At the same time, if managers really are working to maximise returns on investments, then financial resources will be most efficiently allocated. It is true that neither the community nor the environment is in a position to bargain for an adequate share of the company's returns, but this is a matter for law-makers and not for the writers of corporate constitutions.

The territorial nature of standard governance arrangements such as the Sarbanes-Oxley Act is important. It ensures some commonality of approach within jurisdictions. When every corporation is faced as it is in the US with a set of institutions which are designed to protect the property rights of shareholders then corporate structures are likely to evolve in similar ways. So it is important to emphasise that, because legal arrangements vary, corporate structures also vary. For example, while under US law the firm works for its investors and bargains with other factors of production such as employees, under German law the firm's responsibilities are more widely defined. Labour and management, as well as shareholders, are in Germany regarded as stakeholders in the firm. They therefore have rights in determining the direction which the firm takes, an approach which is known as *codetermination*. German corporations have two tier boards: the higher supervisory board, or *Vorstand*, is composed half of shareholders and half of employee representatives (of whom a third are trades union representatives).

Systems like the German one (those of France and Japan, while different, are closer to the German model than to the Anglo-US one) are also contractual. While the US system is concerned mainly with the incentives of investors, codetermination systems are concerned also with the incentives of employees. One consequence of codetermination is a more secure employment contract. It was suggested in the late 1980s that security of job tenure was responsible for Japanese corporate successes because it provided the right incentives for employees to learn about their corporation and perhaps to improve it. The cost of providing incentives like this to the employees is attenuation of financial investor rights. The effects of the tradeoff between employee and investor rights have been studied by several authors, most notably by La Porta, Lopez-de-Silanes, Schleifer and Vishny (1998, 2000). When managers and employees are given decision rights *ex post* (as opposed to bargaining rights *ex ante*), minority shareholder rights appear in general to be weakened. In the absence of strong legally-assigned shareholder property rights, a far greater degree of active participation is required of financial investors. As a result small shareholdings are far less common: weak minority shareholder rights tend to go along with highly concentrated ownership and a very significant role for banks.

So the economies of scale which national governance arrangements bring have lead to a num-

ber of competing systems of governance. The Anglo-US system assigns strong property rights to financial investors and requires other stakeholders to negotiate clear contracts with the firm. It is characterised by large and dispersed shareholdings, and a strong emphasis upon capital market discipline and the takeover market. The continental European and Japanese systems assign some control rights to employees and in so doing weaken shareholder property rights. The consequence is more concentrated ownership, more bank involvement, and a weaker capital market.

Whether one of these approaches is superior to the others is not germane to today's discussion. It is interesting to note, however, that firms can to some extent expose themselves to alternate systems of governance by *cross-listing* on a foreign stock exchange. In so doing, they expose themselves to the discipline of a foreign capital market and they are forced to abide by the laws of their host country. Continental European firms which list in the United States for example are subject far more detailed disclosure requirements than they would be in their home countries. They might elect to cross list simply in order to tap the enormous US capital markets, but the above discussion of commitment value suggests another reason: they may cross-list in order to send a credible signal to their home investors of good future behaviour. In so doing, they will reduce their cost of capital in both home and overseas markets and so will raise the value of the firm. Quite a lot of hard evidence supports this thesis.[3] Any effect which Sarbanes-Oxley has upon cross-listing incentives is therefore likely to have an impact upon welfare in non-US countries. This is naturally a concern for Europeans, although there is little if any evidence that it was considered while the leglislation was being drafted. I will return to this point later.

3. Regulating Corporate Governance

I have argued that corporate governance concerns the contracts which managers write with their financiers in order to commit themselves to behave well. *Ex ante* (at the financing stage) managers wish to sign strong contracts, but *ex post* (when they have raised financial capital) they would probably prefer to renege upon their contracts. Because bilateral contracts are hard to draft, interpret, and to enforce, the State provides a common framework which investors and the courts understand. This framework reflects and reinforces the local institutional features. So the State clearly has a role in simple matters like enforcing property rights. But it is important to appreciate that the State's role is merely to *help investors and firms to write contracts to which ex ante they both wish to sign up.*

This is an easy thing to say: it is rather hard to characterise a governance code which is consistent with it. For example, it is natural to compare the Sarbanes-Oxley implications for operational risk management to those of the new Basel Accord. But the Basel Accord applies to banks which are regulated because the costs of their failure are borne by many more parties than just their investors: because it provides deposit insurance, the State bears much of the the financial costs of bank failure, and bank failure has wider systemic ramifications. Neither of these observations applies to corporations. The failure of Pepsi would be unlikely to trigger the failure of other soft drink manufacturers, and hence there is no particular reason why the State should

[3] See for example Reese and Weisbach (2002), Doidge, Karolyi and Stulz (2004) and Bris and Cabolis (2002).

concern itself with Pepsi's affairs. As corporate failure has neither systemic nor deposit insurance fund consequences, the only reason to regulate is to ensure that the firm abides by rules which *ex ante* it would have selected for itself. Good governance legislation works because it expands the range of contracting devices by which the firm can demonstrate its commitment and quality to its investors.

It is easy to misinterpret this argument. For example, if a rule has not yet made it onto the statute books it need not follow that this is because firms and their investors have not needed it in the past and hence do not require it now. Firms tend to access the capital markets infrequently, and I have already argued that the costs to an individual firm of drafting a new set of rules are very high. Quite apart from the significant problems of enforcement, it is hardly surprising that single firms are in general unwilling to go to the expense and trouble of writing a completely new clause into their constitution, even if the clause could be used by and could benefit future firms. New legislation could therefore simply fulfil a common need at a cost which was too high for a single institution to meet. Furthermore, the contracting story does not imply that every new rule to which existing corporations object is a bad one. If a rule tightens up a loop-hole after funds have been raised then at worst it transfers money from the managers of the firm to its shareholders, and for some firms it lowers the cost of accessing the capital markets and hence raises welfare.

Notwithstanding these arguments, it is clearly easy to enact bad legislation. Laws which undermine free contracting rather than facilitate it are socially destructive. Laws which provide new frameworks may impose costs which far outweigh any benfits which they generate for investors. Laws which assist local firms (about whom the legislators are most concerned) may at the same time damage others.

As yet it is unclear whether Sarbanes-Oxley is a good law which tightens up loopholes and facilitates better contracting; or a bad one which imposes burdens which either generate no benefits for the firm and for its investors, or whose benefits are achieved at an excessively high cost. In the remainder of my discussion I shall use the framework which I have presented as a basis for discussing the legislation and in particular for analysing its implications for operational risk management. I am afraid that I will not give a firm opinion regarding the net impact of Sarbanes-Oxley. I shall however argue that, conditional upon meeting the costs of satisfying the legislation, the law provides a genuine opportunity to strengthen investor/firm contracting by commiting to specific risk management techniques.

4. US Corporate Governance and the Sarbanes-Oxley Act

My contractual justification for corporate governance legislation falls between two distinct positions. Some authors (e.g. Bearle and Means, 1932) have argued that the dispersed investors in the corporation are virtually powerless to prevent managers enriching themselves at their expense. Others (e.g. Coase, 1937, and Easterbrook and Fischel, 1996) see the firm as a set of freely-made contracts. The former school favours State intervention to protect the investors, while the latter argues that contracts lead to efficiency and that the only role of the State should be to protect property rights and to provide courts.

The 1933 Federal Securities Act was intended simply to require truthful disclosure about securities, and to penalise falsehoods. Selection of specific governance arrangements could be left to the market. In its strong presumption in favour of regulation of disclosure and not of substantive behaviour, the Act favoured the free contracting approach. Although some changes to the legislation in favour of Federal regulation of behaviour rather than reporting occurred in the ensuing 70 years (see Ribstein (2002) for examples), the Sarbanes-Oxley Act is the first significant change in favour of substantive regulation.

I have argued that good regulation recognises the importance of free contracting, but have acknowledged that in some circumstances the State can resolve coordination problems in generating the right contracts. This certainly does not reflect the basis upon which the Sarbanes-Oxley Act was passed. A series of crashes and frauds involving Enron, WorldCom, Waste Management, Global Crossing and others generated a climate in which corporations and their managers were seen as uncontrollable and which strongly favoured the inteventionist approaches of the first school to which I referred earlier. At the same time, auditing firms were widely perceived as using their auditing operations as "loss-leaders" to sell non-auditing services. Enron's collapse from the seventh largest firm by market capitalisation to an empty and fraudulent shell and the evidence that WorldCom created billions of false earnings by capitalising expenses provided the basis for arguments that strong medicine was needed to restore public confidence in the financial markets. The Sarbanes-Oxley Act, which entered the statute books 29 days after the disclosure of accounting irregularities at WorldCom (Perino, 2003), was the response.

Figure 1 summarises the main sections of the Sarbanes-Oxley Act. I discuss below their content and their implications for corporate form.

Section Numbers	Subject Matter
100s	Creation and Operation of the Public Company Accounting Oversight Board
200s	Auditor independence
300s	Behaviour and compensation of CEO, CFO and professional advisors
400s	Disclosure rules
500s	Conflicts of analyst interest
600s	Funding and power of the SEC
800,900,1100s	Penalties for transgression

Figure 1: Main sections of the Sarbanes-Oxley Act.

Public Company Accounting Oversight Board

Section 101 of the Act creates the Public Company Accounting Oversight Board, a District of Columbia not-for-profit organization. The Board will consist of five members who will serve for five year staggered terms and only firms which have registered with the Board will be able to audit publicly-quoted companies. This gives the Board new and significant monopoly powers. It will also be responsible for creating, promulgating and monitoring standards of auditing and of ethical behaviour. Some of the standards by which audit firms will in the future have to abide, such as

seven year retention of work papers and peer review of audits, are laid down by the Act (section 103), and the Act also lays down inspection requirements for large audit firms (section 104). The Board will be overseen by the SEC and will be funded from audit fees.

This is clearly a move towards more prescriptive regulation. There will in the future be far more oversight of auditing firms and the costs of this will of course be bourne by the audited firms: ultimately, therefore, by the shareholders.

Auditor Independence

Section 201 of the Act may cause major changes to the industrial organisation of professional services firms in the United States. It prohibits audit firms from also providing non-audit services to audit clients. These include bookkeeping, financial information systems design, actuarial services, investment advice or dealing, legal and expert services. In general therefore, cross-selling of consultancy services will be outlawed.

The Act also discusses the relationship of the auditing firm to the client. In particular (section 203), there is a requirement that audit and reviewing partners be circulated after five years. Finally, a firm cannot be audited by an institution which in the previous year employed either the CEO or senior accounting officers upon an audit of the firm.

These rules are of course intended to avoid possible conflicts of interest. They will certainly reassure investors that disclosed figures are unbiased. Some industry participants have however expressed concern that the rules may close important information transmission channels. For example, changing audit partners may cause a loss of valuable expertise which could serve to *improve* oversight, rather than to weaken it. Similarly, if the audit firm has the best information about a corporation's requirements for financial information then it may be inefficient to prevent it from selling its expertise in the form of IT consultancy.

Behaviour and Compensation of CEO, CFO and professional advisors

The sections of the Sarbanes-Oxley Act numbered 300 represent possibly the most substantial shifts in US Federal corporate governance law away from disclosure and towards detailed conduct of business regulation. The sections which I will discuss have a significant impact upon the organisation of the company (301), the job descriptions of its senior officers (302) and their compensation (304). Moreover, section 307 seems likely substantially to change the relationship of the firm to its legal advisors.

Section 301 requires US securities exchanges to prevent an issuer from listing if it does not have an independent audit committee which is directly responsible for selecting, hiring and managing the relationship with, any public accounting firms employed by the firm. In addition, the audit committee must establish procedures for dealing with complaints, and must have wide authority to engage its own professional advisors. Thus, this part of the Act stipulates the way in which the firm must be organised.

Some concern has been expressed amongst legal scholars that it may be impossible for some non-US firms both to meet the requirement for an independent audit committee and to satisfy local

requirements. For example, in German firms the audit committee's role is generally performed by the supervisory board, the Vorstand, which does not meet the requirements of section 301. Foreign issuers are not required to comply with this part of the legislation until July 31, 2005, and its ultimate implications appear still to be somewhat unclear.

Section 302 of the Act has received possibly more press attention than any other part of the Act. It requires the CEO and CFO to certify financial and other information contained in each annual and quarterly report. They have responsibility for establishing and maintaining internal controls and they are required to ensure that they receive reports of all material information. Furthermore, they are under an obligation to disclose to the audit committee any deficiencies which they uncover in the design or operation of internal controls, along with details of intended corrective action.

In prescribing the reports which the CEO and CFO will produce and in defining precisely some of their job responsibilities, section 302 again moves significantly from the former emphasis in US law upon disclosure requirements. It has been criticised on the grounds that the CEO and CFO are already responsible for internal controls and for the accuracy of financial information. It may have some bite though on the grounds that it resolves a commitment problem of the type which I discussed when motivating corporate governance. It may be difficult for a CEO to commit to examine internal controls in the absence of a clear auditing requirement or of legal machinery for dealing with transgressions. Equally, this legislation makes it easier for the CFO to commit never to use ignorance as an excuse: while *ex post* this excuse may be acceptable to both the company officers and to the investors, it is never *ex ante* efficient.

Section 304 is a rare example in the US of State interference with compensation policies. It requires the corporation's CEO and CFO to reimburse any equity-based compensation or profits from stock sales following a required restatement of a financial document as a result of material non-compliance of the issuer due to misconduct with any financial reporting requirement under securities laws. While some authors (see for example Homström and Kaplan, 2003) have argued that this law will reduce the proclivity of corporate officers to attempt to manipulate short-term stock price movements I find it very hard to justify: if such a law is truly value-increasing it is difficult to understand why it should not simply be written into the corporate charter on a case-by-case basis. In practice section 304 seems likely simply to raise the costs of employing senior corporate officers, both directly because of the danger of confiscation of compensation, and indirectly, because the replacing stock options with cash payments will undermine managerial incentives.

Section 307 undermines the confidentiality of the firm-lawyer relationship. It requires the firm's lawyers to report evidence of material breaches of securities laws or of fiduciary duty to the firm's chief legal officer and to its CEO. If they do not respond with sufficient speed, the breach must be reported to the audit committee or to the full board of directors. There has been quite a bit of criticism of this law, some of it from lawyers. It has been suggested that corporate officers may be unwilling to ask for advice if they think that in doing so they may reveal a problem which will then become public knowledge with potentially harmful effects for the officers involved. This may of course be a problem. At the same time, this is a classic example of a rule which in the absence of legal strictures neither the law firm nor the firm would be able to commit *ex ante*. So introducing this law may serve to increase the value of the corporations which are subject to it. I think that

it is almost impossible to tell *a priori* whether this is the case and, as it was introduced with an extremely wide-ranging raft of other laws, it is regrettably probably impossible for us to disentangle its effects from the rest of the legislation.

Disclosure Rules

Some straightforward changes have been made to disclosure requirements with respect to off-balance sheet transactions, and to insider transactions. The Act also requires firms to disclose whether their audit committee contains a financial expert. This part of the Act also imposes some conduct of business obligations. For example, section 402 prohibits listed companies from making loans to executive officers or directors. This is likely to have a significant impact upon compenstion policies.

Section 406 requires companies to disclose a written code of ethics, or to explain why they do not have one. This reflects an increasing tendency towards notions of corporate social responsibility. In the wake of scandals like the Enron affair, it has received little real critical attention, but it is nevertheless an interesting step. Many commentators have argued that attempting to endow corporations with moral responsibilities risks subverting their real purpose of wealth creation. In practice, the ethical requirements of the Sarbanes-Oxley Act relate mostly to compliance with the law and to the management of conflicts of interest so this part of the Act appears unlikely to be an immediate cause of disputes.

Sections 404 and 409 will constitute much of the remainder of today's discussion so I will outline them in some detail now before returning later to their implications.

Section 404 has been well publicised. It requires an annual internal control report containing a statement of the responsibility of management for establishing and maintaining adequate control of financial reporting. More materially, it requires a statement identifying the framework used by management to evaluate the effectiveness of the internal control and an assessment of the effectiveness of the internal control. The auditor is required to attest to the accuracy of these statements.

The requirements of section 404 are clearly tilted more towards disclosure than towards procedural requirements. As such they are in line with the broad thrust of securities laws since the 1930s. Nevertheless, they place new and possibly costly demands upon regulated companies. In particular, they imply the existence of a *formal and verifiable* system of checking internal controls. In many firms controls are essentially built into formal and informal communication channels and it will be difficult to codify them. This process of formalisation is complicated by the need to provide audit trails. So it will not only be necessary to write down the corporation's control mechanisms: it will be necessary to prove that they have been employed. It is possible that in some firms compliance will be achieved only by changing significantly the corporation's reporting lines: in other words, this apparently innocuous reporting requirement may have non-trivial knock-on effects upon organisational structure. It is not clear to me whether this will have still wider ramifications. A number of management theorists have explained corporate success in terms of unique characteristics such as structure and culture which are nebulous and hard to preserve. Complying with this law without upsetting the delicate cultural balance of the corporation may be hard. Foreign issuers will have

until April 15, 2005 to resolve these problems and to comply with the requirements of the Act.

Section 409 has received perhaps less attention than 404, but its impact may in the longer term be even greater. It requires quoted companies to disclose to the public in plain English and on a "rapid and current basis" any information concerning material changes in the financial condition of the company's operations. Compliance is required by 23 August, 2004. It appears that the initial requirement for a 48 hour reporting horizon has been supplanted by a four business day requirement.[4]

Like section 404, section 409 is simply a disclosure requirement: compliance methods and their structural implications are left to the regulated firm. Nevertheless, and notwithstanding the extension of the reporting deadline, section 409 is likely to have major repercussions for regulated companies, particularly if detailed reporting standards are introduced. Like section 409, it requires quantative and verifiable information on company procedures, and it forces firms to make a rapid decision about the likely impact of changes to standard conditions. Although financial markets appear on average to be pretty good at aggregating information, one obvious concern is that frequent company announcements of potentially deliterious events will destabilise the stock price.

More immediately, section 409 requires the implementation of real-time monitoring systems. I shall return to this problem later. In brief, though, corporations will have to capture important operational information and establish procedures for responding to it. As with section 404, this introduces organisational complications. The obligation to maintain near real-time information on decision-making within the firm and systemic shocks outside it will require both a clear understanding of the firm's organisational structure and the consequences of exogenous shocks such as supplier failure or severe weather; and also sufficient technical skill to build systems capable of generating timely and useful information. Furthermore, as per the discussion of section 404, many of a firm's most important channels of communication are tacit and informal. It will be hard to identify, let alone to monitor, some of these. At the very least careful mapping of organisational form will be required; conceivably, that this requirement can most efficiently be met if the corporation is somewhat restructured.

Conflicts of Analyst Interest

During the last stock market boom there were some instances where it appeared that stock market analysts had overstated the value of some corporations in order to secure valuable corporate finance adivsory business for their enmployers. This type of cross-selling is potentially more damaging to the efficient operation of the capital markets than that by auditors to their consultancy divisions. It is not the main focus of today's discussion, but it is worth noting that Sarbanes-Oxley's section 501 contains provisions which force securities exchanges to adopt rules dealing with the problem. For example, analysts will no longer be allowed to submit their reports to the subject companies for clearance; retaliation for bad reports is prohibited; and better information partitions ("Chinese walls") are mandated.

[4] Current events are reported to the SEC using a form 8-K. As a consequence of section 409 of the Sarbanes-Oxley Act, eight new items have been added to the form and a further two items have been transferred from periodic reports to 8-K. Specific details of the changes are available from `www.sec.gov/rules/final/33-8400.htm`.

Some commentators have expressed muted opposition to the changes on the grounds that they will undermine information gathering incentives in financial markets. Their longer term effect has yet to be determined, but they strike me on the whole as positive.

Funding; Disciplining Transgressors

The remainder of the Act provides for the enhanced funding which the SEC will require (section 601) and gives the legislation teeth: for example, section 802 stipulates a 20 year penalty for destruction, alteration of falsification of records in Federal investigations and bankruptcy; section 807 raises the criminal penalty for securities law to 25 years imprisonment, and section 906 institutes a $1,000,000 fine or 10 years' imprisonment for CEOs and CFOs who knowingly give false certification of compliance with the Act.

5. Cross-Listings Incentives

I discussed earlier the importance of corporate law and corporate governance arrangements as precommitment devices. I argued that a firm's managers may wish when raising money to constrain themselves to abide by conduct rules which, after investment has occurred, they would prefer to disregard. This is an easier thing for a manager to accomplish in a country with well-developed institutions than in one with weak or corrupt legal systems. Managers in weaker regimes would probably be prepared to pay something to improve the quality of law enforcement because in so doing, they would lower their total cost of funding. This is one of the reasons that companies choose to cross-list on foreign exchanges: in doing so, they effectively "rent" the host countries' corporate laws. Sarbanes-Oxley both alters the nature of US securities laws, and also raises the rent on them. It clearly has ramifications for foreign companies which list in the US.

Legal and economic scholars have addressed this point. It is perhaps a little early to draw blanket conclusions, but the general consensus appears to be that the rent on US Law may have been raised further than its value to non-US corporations. Ribstein (2003) identifies this effect. He notes that the effects upon cross-listing companies are disproportionately high because these firms tend to list in the US in order to commit to better disclosure, rather than to adopt new substantive forms of governance. Moreover, US lawmakers are of course not concerned primarily with the concerns or interests of non-US firms. Nevertheless, foreign firms constitute nearly 17% of NYSE listings and in an attempt to forestall their flight from US markets, the SEC has responded to pressure from cross-listing firms by granting them some exemptions from the Act's provisions.

Notwithstanding the SEC's concessions, concerns remain that foreign firms will cease to list, and will possibly de-list, in the US. There is as yet little evidence on this effect. Some recent related work by Engle, Hayes and Wang (2004) examines the going-private incentives for US companies and demonstrates that they have been affected by the Act. They find a modest increase in going-private decisions after the Act. These decisions were mostly concentrated amongst smaller firms, which also experienced the largest positive market response to their going-private announcement. This work is at least weakly supportive of the hypothesis that Sarbanes-Oxley has reduced the value of a cross-listing.

6. Operational Risk Management

Identifying Operational Risks

I now turn to the main focus of the seminar: namely, the consequences of sections 404 and 409 of the Act. Both are concerned with the corporation's internal controls. Section 409 in particular implies a requirement that firms have in place accurate control systems which allow for almost real-time capture of important data and identification of problems. The measurement, reporting, and use of this type of data is typically referred to as "operational risk management."

Operational risk management has in recent years become an important focus of financial institutions. A failure of controls led ultimately to the collapse of Barings Brothers, to the Orange County pension fund disaster and to the foreign exchange trading losses at AIB. The consequences of operational risk need not be quite so spectacular, though: a failure to honour a sales commitment or to settle a transaction need not trigger an organisation's failure, although it could have serious ramifications for its reputation and for its share value.

Operational risk was defined in an industry study conducted jointly by the BBA, ISDA, RMA and PwC (1999) as "the risk of direct of indirect loss resulting from inadequate or failed internal processes, people and systems or from external events," and this definition was adopted by the Basel Committee for its new Capital Accord. But this definition is (perhaps constructively) ambiguous. Culp (2001) notes that the distinction between operational and regular business risk is a function of the firm's strategies. For example, bankruptcy of a major creditor might under some circumstances constitute a failure of control systems, but for a debt recovery company it is an inevitable part of doing business.

As a result of section 409 of the Sarbanes-Oxley Act corporations listed in the US will have to start actively measuring and managing their operational risks. This is both a cost and potentially an opportunity. Measuring operational risk allows corporations to develop objective criteria for analysing the adequacy of internal controls (see Netter and Poulsen, 2003, for a discussion and a review of some literature). Moreover, an audit committee cannot function effectively without a clear assessment of risks, accurate identification of problems, and some methods for tracking and resolving those problems.

Section 409 of the Sarbanes-Oxley Act forces companies to address these issues. Once a corporation has made the the decision to continue to list in the US its response to this requirement will have a significant impact upon its value. Firstly, the Act creates a *new* operational risk: failure adequately to fulfil its requirements may lead to litigation resulting in a potentially disastrous loss of reputation. So, although a relatively *ad hoc* approach to internal controls and their management may be a feasible one it is potentially very costly, and it generates few benefits for the shareholders. In contrast, firms which generate properly designed enterprise wide management systems for operational risk are able actively to manage risks of reputation and customer loss and so to generate shareholder value. Moreover, these firms will be making the most out of corporate building blocks like the audit committee which they are in any case forced by the Act to adopt.

Corporations which respond to Sabanes-Oxley by implementing or improving their operational risk management systems face problems of measurement and quantification to which I now turn.

Risk Measurement

In practice, operational risk is estimated either using top-down approaches based upon macro data, or bottom-up approaches based upon the observation of individual events. A simple top-down approach would look at total turnover and use historical experiences in similar companies to extrapolate information about likely operational losses; a more sophisticated approach might use the volatility of earnings as an explanatory variable.

The bottom-up approach applies standard statistical techniques to extrapolate possible loss distributions from observed operational variables. So for example a corporation might attempt to determine using past experiences the interrelationship between a number of explanatory risk factors and hence to determine a statistical distribution for losses. This could then be simulated using Monte Carlo methods and used to determine a Value at Risk figure for reporting purposes.

The use of Value at Risk (VaR) figures is commonplace in banking, where they have been used for over a decade to analyse the riskiness of traded portfolios of equities, bonds, and derivatives. A VaR figure is simply a percentile on the loss distribution over a particular time horizon. So if for example I quote a 3 day 95% VaR of £5 million I anticipate that with 5% probability I will in the next three days lose over £5 million; the VaR figure tells us nothing about the potential losses in the 5% of outcomes which are bad.

Value at Risk calculations are very attractive to risk managers; they represent simple summaries which are comparable across lines of business. They are certainly very useful in the context of asset portfolios. But in the case of operational risk it is important that we do not ascribe to this method of reporting powers which it does not have. The problem with operational risk as opposed to market risk is that it is fundamentally *endogenous*. By this I mean that operational risk arises as a consequence of the day-to-day choices which the firm's employees make, and that these choices are a consequence of the environment in which they work and the ways in which they are monitored and compensated. The very act of installing an operational risk management system is likely to change behaviour patterns and with them the level of operational risk to which the firm is exposed. We should therefore be sceptical of claims about operational risk levels which are based upon experiences which pre-date the measurement and management of operational risk.

So notwithstanding the statistical sophistication of the VaR methodology we should be wary of false precision in the figures which it generates. It goes without saying that we should be profoundly suspicious of a VaR figure based upon top-down approaches which ignore entirely the micro economic effects of new control systems, reporting structures, or even simply of the presence of a new and independent audit committee. In short, we need to understand why operational risk management adds value, and then to concentrate our efforts in this direction.

The Value of Operational Risk Management

I have argued throughout my discussion that corporate governance is all mitigating the contracting problems which exist between the firm and its investors. Contracting is necessary because after investment occurs the incentives of investors and of managers are not perfectly aligned. Contracting is difficult because investors either do not have the information required to identify a breach of

contract, or because they lack legal remedies for broken contracts. Some corporate structures and some laws enable managers to provide more plausible *ex ante* guarantees to investors and these increase both shareholder value and social welfare.

I think that there is a strong case to make for viewing operational risk management as another governance response to this fundamental contracting problem. *Ex ante* there is agreement between the manager and the investor that strong internal controls are desirable; *ex post* these controls may be personally costly to the manager, either because she finds their enforcement difficult or because they restrict her rent-seeking activities. If she can credibly contract up-front to manage operational risk then she may reduce her cost of capital.

To examine operational risk management systems through this lens, we can start by considering the nature of a good operational risk management contract between the manager and her investors. I have already touched upon the first significant problem: it is extremely hard precisely to distinguish operational risks from business risks. A good contract should identify the risks which are an inevitable consequence of its business, and equally should identify those risks which it will attempt to stamp out. This will provide investors with confidence that they understand the company's business, and will provide them with redress against managers who deviate from the straight and narrow.

This suggests an alternative definition of operational risk: *operational risks are those risks which the company does not regard as essential to doing business and which it should therefore monitor and attempt to reduce.* This definition clearly includes the risks identified in the Basel Committee's publications, but it makes their identification somewhat simpler. It also has the advantage of making explicit the central importance of delineating these risks. Although the State cannot perform this delineation on a firm-by-firm basis, it can recognise that delineation is itself a valuable contracting device and it can provide a legislative framework which helps companies to commit to a particular delineation. In the case of Sarbanes-Oxley, this is achieved through the simple expedient of making it compulsory to do so[5] and ensuring that the law is able to penalise those who do not. Of course, risks may over time move into or out of the ambit of the operational risk manager; the company should respond by explicitly recognising these changes in its section 404 and 409 reports.

The identification of operational risks therefore forms an important part of the investor/manager contract. In theory such a contract could leave the risks explicitly undefined, in which case investors would at least know that they were taking whichever risks the manager deemed appropriate, or it could be very specific. The contract should further include a definition of the scope of the operational risk management activities: to what extent the risks identified in the contract will be measured and tracked. In other words, it should discuss the corporation's control systems. Once again, Sarbanes-Oxley provides a framework both for doing this, and for punishing transgressors. The final part of the contract, covered by section 409 of the Act, should stipulate the types of corrective actions which will be performed in response to material operational events.

[5] Two of the new form 8-K items which are discussed in footnote 4 concern the signing and termination of material definitive agreements *that are entered into in a manner that is not in the ordinary course of business.* It is therefore incumbent upon firms explicitly to define the "ordinary course of business."

Viewing operational risk management as part of the governance contract between managers and investors therefore gives us a clear picture both of why operational risk management adds value, and it tells us how we should perform risk management. Its emphasis upon clear risk definitions mitigates strongly in favour of a bottom-up approach to risk management. Moreover, and perhaps less obviously, it is concerned with the appropriate management of *procedures*, and not with reporting possibly spurious Value at Risk numbers. A VaR number can be wildly inaccurate because the statistics upon which it is based are flawed. This does not necessarily mean however that the manager is abnegating her responsibilities, which are to track operational risk and to attempt to introduce organisational procedures which can diminish it. Good employment contracts are enforceable and tie rewards and punishments closely to the consequences of the manager's actions. It therefore seems more natural to contract upon measureable attributes such as procedures and controls, and not to rather hard-to-quantify attributes such as VaR figures based upon questionable Monte Carlo simulations.

In this light of this discussion we can start to understand how an appropriate response to sections 404 and 409 of the Sarbanes-Oxley Act could increase shareholder value. I will address this question in the final part of my discussion.

Implementing Section 409 Reporting

I have made a case for management of operational risk through identifying and tracking key organisational *processes*. This is a difficult task in a large and complex organisation. I argued above that it consists of three stages: *defining* operational risks; defining the scope of *measurement and tracking* systems; and defining organisational *responses* to operational risk. I consider each of these below.

Defining Operational Risks – Operational risks depend upon the business policy and the objectives of the organisation. Operational risk management should therefore start with an examination of the corporation's high level strategies and mission statements. It will also require a careful analysis of the business processes used to support the company's core activities. For example, if a core activity is collecting payments from customers, operational risks will attach to the mechanisms which perform this job. For example, an operational risk might be "failure to trigger late payment actions" in the appropriate system.

So operational risk definitions require a clear understanding of the organisation's business processes. A key output from the definitional phase should therefore be an inventory of the important business processes. This immediately defines the key risks and hence will help to guide strategic risk management thinking.

Measurement and Tracking of Processes – The operational risk definition needs to be supplemented by a means of measuring and tracking operational risk events. Typically, a number of operational risks which be associated with each business process. For each of these the company should stipulate the scope of its risk measurement systems. In practice this will require a statement of quantative indicators of performance, or *Key Performance Indicators (KPIs)*. For example, the "failure to trigger late payment actions" risk may be measured using elapsed time to payment, pay-

ments received over 30 days late, and so on. Publication of the KPIs is an important contractual device: it provides an accurate picture of the managerial response to operational risks.

Section 409 requires companies to monitor their operational risks in real time. So generating a list of KPIs is only a first step. The corporation also needs to institute computer systems and procedures which will facilitate the timely capture of KPI data, and also its aggregation into useful management reports. But this is of course an inevitable corollary of the contractual view of risk management. Once the manager has published the KPIs, she is responsible for monitoring them and hence should institute such systems.

Responses to Operational Risks – Reporting systems are of use only if there is a mechanism in place for responding to them. Assigning organisational responsibility for assessing and responding to operational risk management systems is therefore an essential part of the risk management process. This ensures that the organisation is in a position to identify and to respond to events which have a material effect upon the operational risks which it has defined. It is a central part of section 409 of the Sarbanes-Oxley Act.

7. Conclusion

The Sarbanes-Oxley Act has shifted the emphasis of US corporate governance law away from disclosure and towards conduct regulation. To understand the importance of this shift, we have to consider the meaning and the purpose of corporate governance. I have argued that corporate governance concerns the contract which the corporation's managers write with its financiers. When a manager is better able to commit to certain ways of behaving the corporation's cost of capital will be reduced and its value will rise. This is desirable to every party *ex ante*, but *ex post* the manager may prefer to consume perquisits; a good corporate governance arrangement will help him commit not to do so. While these arrangements could in theory be designed on a company-by-company basis, in practice the incentives to do so are weak and the State generally assists by providing a common framework for companies operating in its jurisdiction. As a result we tend to see commonality of governance arrangements across the companies operating in a particular jurisdiction.

The Sarbanes-Oxley Act provides new commitment mechanisms for US-listed companies. These are based to come extent upon changes to the structure of the corporation, for example via the introduction of audit committees. The Act also provides in section 409 explicitly for regulation of operational risk management systems. I have argued that operational risk management is valuable insofar as it strengthens the contract between the manager and the investor. This has clear implications for the design of operational risk management systems. I have stressed firstly the importance of defining their scope through careful cataloguing of business processes; secondly the need precisely to define the key performance indicators which will be used to monitor operational risks; and finally, the importance of clearly defined managerial responsibilities for responding to the output of these systems.

References

Berle, A. A. and G. C. Means (1932), *The Modern Corporation and Private Property*, Macmillan, New York, N.Y.

Bris, A. and C. Cabolis (2002), 'Corporate Governance Convergence by Contract: Evidence from Cross-Border Mergers', Working Paper 02-32, International Center for Finance, Yale University.

British Bankers' Association, ISDA, PricewaterhouseCoopers and RMA (1999), *Operational Risk: The Next Frontier*, RMA, Philadelphia.

Coase, R. H. (1937), 'The Nature of the Firm', *Economica*, Vol. 4, No. 16 (November), pp. 386 – 405.

Culp, C. (2001), *The Risk Management Process: Business Strategy and Tactics*, John Wiley, New York, N.Y.

Doidge, C., G. A. Karolyi and R. M. Stulz (2004), 'Why are Foreign Firms Listed in the U.S. Worth More?', *Journal of Financial Economics*, Forthcoming.

Easterbrook, F. H. and D. R. Fischel (1996), *The Economic Structure of Corporate Law*, Harvard University Press, Cambridge, Mass.

Engle, E., R. M. Hayes and X. Wang (2004), 'The Sarbanes-Oxley Act and Firms' Going-Private Decisions', Mimeo, Graduate School of Business, University of Chicago.

Fama, E. F. (1970), 'Efficient Capital Markets: A Review of Theory and Empirical Work', *Journal of Finance*, Vol. 25, pp. 383–417.

——— (1991), 'Efficient Capital Markets: II', *Journal of Finance*, Vol. 46, No. 5 (December), pp. 1575–1617.

Fama, E. F. and M. C. Jensen (1983), 'Separation of Ownership and Control', *Journal of Law and Economics*, Vol. 26, No. 2 (June), pp. 301 – 325.

Holmström, B. and S. N. Kaplan (2003), 'The State of U.S. Corporate Governance: What's Right and What's Wrong?', Working Paper in Finance 23/2003, European Corporate Governance Institute.

Jensen, M. C. (1993), 'The Modern Industrial Revolution, Exit and the Failure of Internal Control Systems', *Journal of Finance*, Vol. 48, No. 3 (July), pp. 831–880.

Jensen, M. and W. Meckling (1976), 'Theory of the Firm: Managerial Behaviour, Agency Costs and Capital Structure', *Journal of Financial Economics*, Vol. 3, pp. 305–360.

La Porta, R., F. L. de Silanes, A. Shleifer and R. W. Vishny (1998), 'Law and Finance', *Journal of Political Economy*, Vol. 106, No. 6, pp. 1113 – 1155.

——— (2000), 'Agency Problems and Dividend Policies Around the World', *Journal of Finance*, Vol. 55, No. 1 (February), pp. 1 – 33.

Netter, J. M. and A. Poulsen (2003), 'Operational Risk in Financial Service Providers and the Proposed Basel Capital Accord: An Overview', *Advances in Financial Economics*, Vol. 8, pp. 147 – 171.

Perino, M. A. (2003), 'American Corporate Reform Abroad: Sarbanes-Oxley and the Foreign Orivate Issuer', *European Business Organization Law Review*, Vol. 3, No. 2 (October), pp. 213 – 244.

Reese, W. A., Jr, and M. S. Weisbach (2002), 'Protection of Minority Shareholder Interests, Cross-Listings in the United States, and Subsequent Equity Offerings', *Journal of Financial Economics*, Vol. 66, No. 1 (October), pp. 65 – 104.

Ribstein, L. E. (2002), 'Market Vs. Regulatory Responses to Corporate Fraud: A Critique of the Sarbanes-Oxley Act of 2002', *Journal of Corporation Law*, Vol. 28 (Fall), pp. 1 – 67.

——— (2003), 'International Implications of Sarbanes-Oxley: Raising the Rent on US Law', *Journal of Corporate Law Studies*, Vol. 3, No. 2 (October), pp. 299 – 327.

Shleifer, A. and R. W. Vishny (1997), 'A Survey of Corporate Governance', *Journal of Finance*, Vol. 52, No. 2, pp. 737–783.

Smith, A. (1776), *An Inquiry Into the Nature and Causes of the Wealth of Nations*.