Communications of the Association for Information Systems

Volume 18 2006 *Article* 22

Implementing Section 404 of the Sarbanes Oxley Act: Recommendations for Information Systems Organizations

Ashley Braganza* Kevin C. Desouza†

*Cranfield University, a.braganza@cranfield.ac.uk

†University of Washington, kdesouza@u.washington.edu

Implementing Section 404 of the Sarbanes Oxley Act: Recommendations for Information Systems Organizations

Ashley Braganza and Kevin C. Desouza

Abstract

Section 404 of the Sarbanes Oxley (SOX) Act addresses the effectiveness of internal controls, which in most organizations are either fully or partially automated due to the pervasiveness and ubiquity of information technologies. Significant or material control deficiencies have to be reported publicly. The adverse impact on organizations declaring deficiencies can be severe, for example, damage to reputation and/or market value. While there are many practitioner-led manuals and methods for dealing with 404, there has been little published in the academic research literature investigating the role of Information Systems organizations in implementing Section 404. The paper addresses this gap in knowledge. We used institutional theory as the lens through which to examine the experiences of Section 404 implementation in three global organizations. We used the case study method and an abductive strategy to gather and analyze data respectively. Our findings are summarized in six recommendations. We found that institutional pressures play a critical role in the implementation of Section 404. In particular, organizations face coercive pressure to achieve Section 404 compliance, without which punitive sanctions can be imposed by regulators. Organizations tend to imitate one another in the methods they use so that each is perceived to be in line with their competitive environment. Organizations face normative pressures to act in ways that are socially acceptable, which is to achieve compliance. Failure to do so would be a signal to the market that the organization does not take controls seriously. We expand these findings in terms of power and influence tactics that IS organizations can use when implementing Section 404. Our findings provide directions for practice and lines of enquiry for further research.

Communications of the Association for Information Systems

IMPLEMENTING SECTION 404 OF THE SARBANES OXLEY ACT: RECOMMENDATIONS FOR INFORMATION SYSTEMS ORGANIZATIONS

Ashley Braganza
Cranfield University
Cranfield, Bedfordshire UK
a.braganza@cranfield.ac.uk

Kevin C. Desouza
University of Washington
Seattle, WA

ABSTRACT

Section 404 of the Sarbanes Oxley (SOX) Act addresses the effectiveness of internal controls, which in most organizations are either fully or partially automated due to the pervasiveness and ubiquity of information technologies. Significant or material control deficiencies have to be reported publicly. The adverse impact on organizations declaring deficiencies can be severe, for example, damage to reputation and/or market value. While there are many practitioner-led manuals and methods for dealing with 404, there has been little published in the academic research literature investigating the role of Information Systems organizations in implementing Section 404. The paper addresses this gap in knowledge. We used institutional theory as the lens through which to examine the experiences of Section 404 implementation in three global organizations. We used the case study method and an abductive strategy to gather and analyze data respectively. Our findings are summarized in six recommendations. We found that institutional pressures play a critical role in the implementation of Section 404. In particular, organizations face coercive pressure to achieve Section 404 compliance, without which punitive sanctions can be imposed by regulators. Organizations tend to imitate one another in the methods they use so that each is perceived to be in line with their competitive environment. Organizations face normative pressures to act in ways that are socially acceptable, which is to achieve compliance. Failure to do so would be a signal to the market that the organization does not take controls seriously. We expand these findings in terms of power and influence tactics that IS organizations can use when implementing Section 404. Our findings provide directions for practice and lines of enquiry for further research.

Keywords: Implementation, IS Strategy, Sarbanes Oxley, Information Systems, Institutional theory

I. INTRODUCTION

The Sarbanes Oxley (SOX) Act is the most significant overhaul of SEC rules since the 1934 Securities Exchange Act (Banham, 2003). Its core purpose is to reduce the likelihood of financial fraud, white collar crime, and financial reporting misrepresentations (Ferrell, 2004). The SOX Act

encompasses all publicly registered organizations under the jurisdiction of the Securities and Exchange Commission (SEC) irrespective of their location (Dewing and Russell, 2003). Consequently, organizations and their auditors, despite being incorporated in other legal jurisdictions, now fall within direct control of US authorities. The Public Company Accounting Oversight Board (PCAOB) has been established under SOX to oversee the audit of public companies that are subject to securities laws to protect investors' interest in the preparation of informative, accurate, and independent audit reports. The SOX Act is binding on US-quoted organizations from the beginning of 2005. For non-US based organizations the original date for compliance was mid-2005. Following strong lobbying by business leaders and governments, the compliance deadline for non-US based organizations listed in the US has been extended to mid-2006. At the heart of this extension is the concern that most organizations would be unable to meet the stringent requirements of SOX within the original timescales. The SOX Act was passed in response to financial misstatements and high profile corporate frauds such as Enron, WorldCom, Tyco, and Global Crossing. But financial misstatements are not restricted to US corporations. Royal Ahold, the Dutch-based third-largest global supermarket operator, reduced operating profits by US $500 million due to a misstatement of its 2001 and 2002 earnings, a consequence of irregularities in the accounts of its US subsidiary. Ahold's American Depository Receipts traded on the New York Stock Exchange, fell by 61% following the news (Anon, 2003a).

Section 404 of the SOX Act covers internal controls with which organizations must comply. Internal controls are vital to the accuracy of the numbers reported to the investing public. A key aim of Section 404 is to ensure financial transparency such that statutory reports and internal management reports are consistent and reflect the true financial position of the organization. Section 404 affects information systems (IS) organizations and their leaders, IT Directors, and Chief Information Officers (CIOs). With the widespread use of technology, many internal controls are either fully automated within information systems or are a combination of manual and automated controls (Duffy, 2004). The processes and their underpinning technology that capture, control, and transform data to information begin with the recording of business transactions. Section 404 covers a wide range of applications such as product accounting, general ledger, asset and inventory management, billing and accounts, receivables and payables, payroll, budgeting and other operational, tracking and reporting systems. These include not only the organization's main systems, e.g. their ERP systems, but also local databases and personal spreadsheets developed and used by employees an ad hoc basis.

Since corporate information systems (e.g. accounting information systems, financial analysis tools, production, and inventory systems) need to be tested for integrity of internal controls, it is only natural that we ask what role should the IS organization (e.g. the IS Department) play in SOX implementations. To date, the academic literature has little in the way of exploratory and descriptive studies that analyze the role of the IS organization in SOX implementations. However, one is sure to find some guidance from practitioner-oriented articles (Duffy, 2004; Ivancevich et al., 2003; Mayer, 2003; Quall, 2004). This paper will report on three exploratory and descriptive case studies that examined the role of IS organizations in SOX implementations. Two organizations are in the financial services sector, one is a subsidiary of a quoted US organization operating in the UK, and the other is a UK quoted company that is listed on the NYSE. The third is a professional services organization that attests financial statements and supports client organizations to achieve compliance with section 404 of SOX. To preserve confidentiality, we refer to them with pseudonyms. We use institutional theory as a lens to analyze the case findings. Specifically, we examine, (1) what are the implementation actions for Section 404, (2) how can these actions be deployed tactically during the implementation process, and (3) what lessons can be learnt from their deployment.

The paper proceeds as follows: We begin by providing a brief overview of Section 404 requirements, and our theoretical base, institutional theory. Next, we outline our research methodology. Following this, we present empirical findings from the three cases. Next, we conduct a discussion of the findings and the development of recommendations for the implementation of Section 404. Concluding the paper is a discussion of implications for practitioners and researchers.

II. SECTION 404 OF SOX

Section 404 deals with management's assessment of internal controls. It requires each organization's annual report to contain an 'internal control report' which: (1) States responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) Contains an assessment, as at the end of the organization's fiscal year, of the effectiveness of internal control structures and procedures for financial reporting. External auditors are required to attest and report on the assessment of internal controls made by the management. This attestation is required to be in accordance with standards for attestation engagements issued by the PCAOB.

All financial reports issued by an organization on a quarterly, six-monthly and annual basis must contain a statement that management is responsible for maintaining adequate internal controls, an assessment of their effectiveness, and a statement identifying the framework used to assess effectiveness. Organizations must report any material changes to internal controls on a quarterly basis. In effect, Section 404 requires the management team to ensure a seamless and scalable internal control system. They face fines or jail sentences if there is even a remote likelihood of any material misstatements and/or misrepresentations in financial reports arising out of a lax internal control system. The Act increases penalties for Officers and organizations convicted of accounting and reporting violations from $1,000,000 or imprisonment of not more than 10 years to $5,000,000 or imprisonment of not more than 20 years (Kulzick, 2004).

These penalties have focused the minds of senior managers of all US listed organizations. There has been grudging acceptance that they have little choice but to commit significant resources to comply with the Act. A number of European organizations are considering delisting from US stock exchanges as a direct consequence of these requirements (Maitland, 2004). They want to avoid the cost and complexity of compliance with legislation that is beyond their own country's jurisdictional boundaries. However, access to the largest capital market in the world and the difficulty of unraveling current shareholding arrangements makes such action unlikely.

The costs and resources required for Section 404 implementation are significant. Recent reports suggest that fulfilling SOX requirements will cost the average large US company US $5.1 million in the first year and then a further US $3.7 million in on-going compliance (Maitland, 2004). Other studies suggest that audit fees for large organizations increase by about 35% (Foley and Lardner and KRC Research, as quoted in Swartz, 2003) and the overall cost to organizations may be as much as US $2.5 billion (AMR Research, as quoted in Swartz, 2003). A recent report showed that Sarbanes-Oxley compliance would cost UK organizations more than US $216 million (Knights and Reed, 2004) because they need to update IT systems to comply with Section 404. British Telecom estimates their costs will be in excess of US $18 million (Maitland, 2004).

SOX differs radically from previous regulations in terms of its scope, information disclosure requirements, penalties, jurisdiction boundaries, and sanctions (Schaub, 2004). In terms of scope, whereas other regulations apply within US borders, the scope of Section 404 is global, i.e. subsidiaries and head offices located in countries outside US fall within the remit of Section 404. Whereas previous information disclosure regulations accept that some amount of information is based on the Board's and Auditor's judgment, Section 404 requires organizations to disclose information that can be 'tracked and traced' through a system of risks and controls at a very granular level. The level of detail and the information assurance requirements are very severe in the context of SOX. Poor implementation can lead to significant penalties (Anon, 2003b; Berg, 2003). For CEOs and CFOs penalties include fines, jail terms, and bans from serving as a board member. As for jurisdiction boundaries, a country's regulatory system typically applies only within its legal jurisdiction. SOX and Section 404 transcends US jurisdictional boundaries. Thus, potentially a District Attorney in Hicksville can claim an UK organization is in breach of SOX in a US court and the UK company would have to answer to the US court.

The confluence of business processes, IT processes, and systems are central to compliance with 404 requirements. At the very least reporting processes have to be mapped and tested. This

has to be done to a level that ensures that consistent and accurate financial reports are provided to shareholders and potential investors. This requires some of the business analysis skills that many IS organizations already have. However, it also requires audit and control skills found in other departments. It requires the full involvement of people in the business as the knowledge about the processes and controls reside in practices and behaviors of people (Ray, Barney, and Muhanna, 2004; Tsoukas, 1996).

Much of the current literature on Section 404 implementation is practitioner led (Duffy, 2004; Ivancevich et al., 2003; Mayer, 2003; Quall, 2004). Typically these set out specific stages and steps that organizations need to undertake in order to address the requirements of 404. We need a richer picture, one that is derived from theory, than is available in the current practitioner literature.

III. THEORETICAL LENS: THE INSTITUTIONAL PERSPECTIVE

The SOX Act falls broadly within the domain of corporate governance. The most prevalent theoretical lens through which governance is studied is agency theory (Dalton et al., 1998). It stems from the seminal work of Berle and Mean (1932) who argued that the separation of ownership (shareholders) and control (management) gave managers – agents – an opportunity to act in their own self-interest. Agents would increase their personal wealth rather than that of the shareholders (Fama, 1980; Jensen, 1993). Agency theory suggests that boards of directors are appointed to scrutinize managers on behalf of the owners (Eisenhardt, 1989a). An 'agency cost' is incurred where managers promote their interests over those of shareowners (Fama and Jensen, 1983). Various mechanisms are used to control managers and minimize the potential loss to shareholders including the composition of the board, in particular, the appointment of independent directors (Barnhart, Marr, and Rosenstein, 1994) and CEO compensation (Cadbury Commission, 1992; Dalton et al., 2003). By and large these mechanisms are self-regulatory. A combination of executive, non-executive, and independent directors and external auditors have been thought sufficient to avoid serious fraud and misrepresentation within individual organizations. However, SOX has introduced external regulation of board and auditor responsibility taking it to a more granular level by ensuring that directors become individually and jointly accountable for all forms of public financial disclosures. Under these conditions, using agency theory as the basis for this study poses a number of limitations.

Agency theory reduces organizations to two participants: managers and shareholders (Daily, Dalton, and Canella Jr., 2003). It views organizations as a system of contracts between shareholders and managers that are aimed at minimizing agency problems (Aguilera and Jackson, 2003). What agency theory appears to overlook is the role of external institutions in shaping the actions of boards and employees actions within firms (DiMaggio and Powell, 1983). Although agency theory focuses on controlling the self-interest of directors, it does not address the relative power which boards, employees and external institutions can exercise (Pfeffer, 1981).

We argue that these drawbacks of agency theory limit insights to be gained into Section 404 implementation. Instead, we suggest that institutional theory provides a better lens through which to study Section 404 implementation. An institutional approach to the study of organizations has yielded insights into organizational actions due to institutional environments (Covaleski and Dirsmith, 1988; Jepperson, 1991; Meyer and Rowan, 1977; Scott, 1987; Zucker, 1987); (Avgerou, 2000; Crowston and Myers, 2004; DiMaggio and Powell, 1991; Goodstein, 1994; Greenwood and Hinings, 1996; Oliver, 1991; Teo, Wei, and Benbasat, 2003). However, our review of the extant literature shows that no previous research has been undertaken into Section 404 implementation based on institutional variables. Institutional theory suggests that organizations conform to rules and regulations about appropriate conduct and behaviors to ensure legitimacy within their environment (Suchman, 1995). The institutional approach takes into account multiple stakeholders within and outside organizations and the use of power and influence to bring about changes in practices (DiMaggio and Powell, 1991; King et al., 1994). DiMaggio and Powell (1983) identify three types of pressures that organizations face: coercive, mimetic, and

normative. Mimetic pressures cause organizations to take actions that make them more like others in their competitive space. An organization will imitate others to ensure it is perceived as being legitimate by customers, suppliers, regulators, and other key stakeholders. For example, the wave of Total Quality led to many organizations publicizing their commitment to quality to remain aligned with others in their industry. Coercive pressures are those brought about by organizations upon other organizations on which they are dependent. The pressure exerted can be formal or informal. Sources of coercive pressure include parent companies upon subsidiaries and regulators. Organizations that have a formal dependency are likely to converge upon similar policies. The adoption of policies and procedures to achieve and maintain compliance with section 404 is an example of coercive power. Normative pressures stem from perceptions of social acceptability. Senior mangers, such as the CEO and CFO, will tend to follow standards and behaviors that are adopted by their peers. In the area of Health and Safety, for example, standards set by one organization will pervade across an industry as CEOs would not want to be seen as having a lower standard of safety for their employees when compared with others in their sector.

In the context of SOX, these pressures arise as institutions such as the SEC can impose sanctions to modify the behaviors of other institutions, in particular audit firms. Audit firms can affect behaviors in client organizations if they are unable to affirm an organization's regime of internal controls. In organizations, parent companies can exert considerable influence and power over semi- and wholly-autonomous subsidiaries to change their practices, controls, systems, processes, and behaviors. These changes can be brought about by the use of power- and influence-based implementation tactics. Power-based tactics affect behaviors through the use of sanctions and direct use. Influence based tactics change behavior through education and social processes. This suggests that a range of interventions can be used for Section 404 implementation.

The pressures organizations face can be separated into 'supply-push' and 'demand-pull' institutional interventions (King et al., 1994). They describe supply-push as a force emanating from the producers of a standard or directive and its attendant intervention processes. Demand-pull intervention emanate from users' willingness to use or adopt the standard or directive. Supply-push in Section 404 implementations refer to the Act and its constituent sections, the COBIT framework (COBIT® 1994)[1], the COSO framework (COSO 1994)[2], guidelines provided by independent auditors and top management directives related to 404 compliance activities. Demand-pull attracts users to meet Section 404 requirements so that they adapt their practices and behaviors where there is a gap between required controls and their actual work they perform.

INSTITUTIONAL PERSPECTIVE TAXONOMY

King et al.'s (1994) taxonomy categorizes IT-innovation interventions into six generic types that contain strategic and conceptual differences in deployment, and are not necessarily mutually exclusive. We follow King et al.'s definitions and categorization but reinterpret their generic interventions, in the context of Sarbanes Oxley, as Section 404 implementation 'actions'. In effect, these actions are mechanisms that can enable IS organizations to take an effective role in supporting the implementation of 404 in their organization. Our study examines specific tactics that IT Organizations can take, using King et al.'s framework which is displayed in Figure 1.

---

[1] "Control Objectives for Information and related Technology (COBIT®)"– 1994 is published by the IT Governance Institute. COBIT is an internationally accepted set of guidance materials for IT governance. Further information is available from http://www.isaca.org/cobit.

[2] COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission. Like COBIT they published a set of guidelines that are widely accepted as the benchmark for compliance purposes. Their main publications are "Internal Control — Integrated Framework" 1992 and 1994.

Following King et al., each cell in Figure 1 will be referred to using its Roman numeral, e.g. III refers to power-based actions aimed at stimulating supply side activity.

KNOWLEDGE BUILDING

King et al. (1994) suggest knowledge building is about creating a knowledge-base necessary to develop an innovation and its use. This includes knowledge related to the technical aspects of an innovation and its application in the organization. The implementation of 404 requires implementers and users to acquire knowledge about the Act in general and 404 specifically. This includes finding out the requirements in terms of defining internal controls, identifying significant accounts, understanding business cycles, and agreeing control objectives. This also includes tailoring 404 requirements to the organization's context. Mechanisms for building knowledge include research undertaken, access to external sources of expertise, internal and external training and collaborations with other organizations.

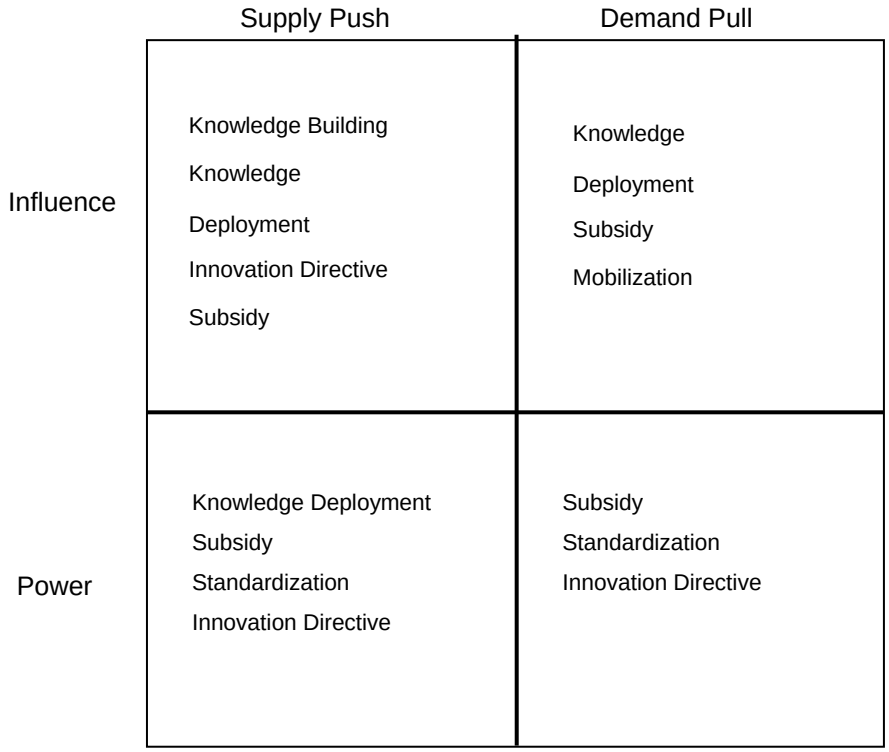

Figure 1: Diffusion Actions

KNOWLEDGE DEPLOYMENT

According to King et al., knowledge deployment refers to disseminating knowledge and developing an understanding of that knowledge among people. A typical method of knowledge deployment is the creation and launch of training programs. Where the organization does not have the necessary knowledge it can bring in knowledgeable individuals or organizations, or move employees who are knowledgeable to its less knowledgeable parts. Knowledge repositories, such as manuals, leaflets, and intranets or portals, are methods of knowledge deployment. In the Section 404 context, knowledge deployment is necessary as implementers and users need to understand specific requirements to avoid having the auditor's report qualified. This information is prescribed by regulatory bodies such as the PCAOB. Knowledge deployment can be achieved by moving knowledgeable people from one part of the organization to another or creating steering teams with knowledgeable representatives from the various parts of the

organization and by making relevant Section 404 information available in one central place on the intranet.

SUBSIDY

A subsidy is the use of resources to cover implementers' costs during innovation development and users' costs during deployment and use. Subsidies are often used to reach specific goals or produce definite outcomes. Subsidies take the form of resources, such as, funding, peoples' time, or allocating teams to the innovation. Subsidies can create the supply of an innovation and stimulate its demand. Subsidies can be coercive or influential in nature. Subsidies can mitigate users' early adopter risks associated with an innovation. Subsidies are likely to be essential to Section 404 implementation. Already, cost estimates appear to be significant. Moreover, the cost of failure (i.e. qualified auditors reports) is too high a price to pay when compared with spending even several million dollars. Subsidies can be used to buy in expertise, sell the importance of Section 404 compliance, make templates and knowledge available, and monitor actual deployment by giving implementers time and authority to check up on subsidiaries and their progress towards compliance.

MOBILIZATION

Mobilization refers to actions taken to persuade decentralized individuals and subsidiary companies to use an innovation. King et al. (1994) argue that fostering a positive view of an innovation increases the likelihood of its adoption across the organization. Some mobilization methods available are promotional and awareness campaigns. A key aspect of mobilization is addressing influential organizational members' self-interests so that they consider the innovation crucial to its future. In the context of Section 404 implementation, mobilization can include presentations, workshops, and other forms of communication and promotional campaigns that accentuate positive aspects of Section 404 compliance with peoples' work. This can be achieved by ensuring visible senior management commitment and support.

STANDARD SETTINGS

Standard settings are agreements between organizational members that favor certain courses of action. Standards act on users by constraining the scope of options they have and by formalizing their actions. Once a standard is agreed upon, all interested parties are expected to adhere to it. In this way, standards are power-based rather than influential in nature. While standards aid diffusion of an innovation, they can also restrain innovation by restricting changes and improvements to practices. Standards can be hard to implement where they conflict with users' current practices and behaviors. Section 404 prescribes a generic set of standards with which organizations must comply. These standards are interpreted by organizations and formulated into a set of procedures and central mechanisms. Furthermore, users, such as subsidiaries and individuals, have to comply with prescribed controls. Many Section 404 controls are mandatory with the intention of giving users little room to deviate. These impositions on users must be set against the broader degrees of currently held freedom.

INNOVATION DIRECTIVE

Innovation directives are formal rules that govern development and use of an innovation. Innovation directives, according to King et al. (1994), are actions that command an organization to produce innovations and set out orders to use the innovation. A directive may require the organization to change its structure or processes to stimulate diffusion. Innovation directives in a Section 404 context are power-based. These are the extent to which users are 'told' to comply with the internal controls. Implementers can demonstrate their use of the procedures and internal controls being laid down. Innovation directives impact on the development of the 404 compliance regime to be adopted by the organization.

IV. RESEARCH METHODOLOGY

This research study is based on an exploratory multi-case study approach (Yin, 1989). A case study design allows researchers to take a more holistic view of phenomenon (Eisenhardt, 1989b) especially where the aim is to explore an area that has received little previous research attention (Benbasat, Goldstein, and Mead, 1987). Case study designs generate rich contextual data that provide insights into a phenomenon, rather than developing axiomatic laws that measure and predict and that can be generalized from a random sample to a predefined population (Blaikie, 1995). This study intends to explore Section 404 implementation and produce insights useful to a variety of stakeholders including CIOs and IS directors and academic researchers.

Organizations affected by Section 404 can be split into two broad categories: companies that have to achieve 404 certification and audit firms that have to attest internal controls. This study is based on two companies seeking 404 certification and one global audit firm. The three specific case study settings for this research were chosen based on theoretical, rather than statistically representative, criteria (Eisenhardt, 1989b). All three had to be large organizations with a global presence and therefore subject to meeting Section 404 requirements. The organizations had to have implemented Section 404 in a UK division in order to analyze the initial effects of their implementation tactics.

The case study design led to the use of qualitative methods to explore Section 404 implementation in these organizations. The primary sources of data were the Sarbanes Oxley Program Team and the IT Organization. The aim was to gather mostly qualitative and non-quantitative data. A variety of data gathering techniques were used, including semi-structured interviews with key personnel responsible for Section 404 implementation. We also examined internal documents such as written reports. Additional data was collected through informal discussions that were held both face-to-face and over the telephone. The data gathering strategy was flexible as this study sought to find a representative and unbiased set of data (Orlikowski and Baroudi, 1991). Open-ended questions to conduct the interviews were developed into an interview schedule using theoretical constructs based on the taxonomy described earlier in this paper.

Table 1: Case Study Interviews

Site	Date	Duration	Respondent's job title
Alpha	6th January 2005	2 hours	Program Manager (IT)
	20th December 2004	2 ¾ hours	Program Director
Beta	23rd December 2004	2 ½ hours	Finance Manager
	23rd December 2004	2 ¼ hours	IT Manager
Gamma	16th December 2004	2 ¼ hours	Global IT Director
	4th February 2005	2 ½ hours	IT Partner
	13th December 2004	2 ¼ hours	Compliance Partner

The case study interviews were conducted between 16th December 2004 and 4th February 2005, however discussions to gain permission commenced several months before hand. The research process involved seven interviews amounting to sixteen and a half hours of interviews in total. A full breakdown of dates, duration, and interviewees is provided in Table 1. This allowed for a comprehensive examination of each organization's Section 404 implementation, tactics used, and their effects. Interviews were semi-structured in nature, allowing for departures from the subject where a relevant or interesting issue emerged during an interview. All bar one interviews were

recorded (the tape machine and the back up machine would not operate) and notes were taken during the interview. Interview data was combined with other data collected including notes and internal reports. The data were analyzed based on an Abductive Strategy, moving from first-order constructs (raw data collected) to second-order constructs (researcher categories, themes, codes) (Blaikie, 1995; Schutz, 1967). The results were written up and sent to interviewees to remove factual errors. All errors and omissions were corrected so that the case studies reflected interviewees' perceptions.

V. FINDINGS

We now present the findings within each case study. In the next section, we integrate the findings across the three cases.

ALPHA GROUP

Alpha Group is one of Europe's largest UK-based global financial services organizations. It offers a full range of banking services under a number of well known brands. The Group comprises eight customer-facing divisions, in addition to six group and central divisions. Each Divisional head reports into the Group Chief Executive. This case study focuses on Group Technology Division (GTD). GTD defines the Group's overall technical architecture and develops and operates the majority (over 80%) of its systems and technical platforms. GTD's scope for Section 404 covered its processes, significant business processes, and controls for documentation.

Alpha's overall SOX program started in November 2003. A small central SOX Program team was formed with a Program Director and people from group accounts and internal audit. A central committee, reporting to the Group Finance Director, was formed and included the group chief accountant, group internal audit, project managers, and the SOX Program Director. This committee appointed a representative to face-off to each business division, with one representative dedicated to GTD. SOX was treated like a project and the organization used a project management method which set out the steps to follow, timescales, format and timings of progress reports to be submitted, and so on. Each division had to use this project management method but with some flexibility. The committee gave divisions flexibility to manage their teams according to their environment, but with certain minimum requirements to be achieved.

Alpha's central SOX program team, with some guidance from its external auditors, conducted a pilot to produce Section 404 documentation and to test existing controls in the lending process. This process was chosen because people across the organization could easily identify with it. The team and auditors used the pilot's findings to develop practical approaches to implement Section 404. A one-day seminar was created for divisional finance heads and their staff for whom the implications of Section 404 were relevant. The seminar was co-facilitated by the SOX Program Director and a partner from their external auditors. The seminars were intended to create awareness of SOX and Section 404, to alert senior managers about resources needed for implementation, and to facilitate next steps for implementing Section 404.

The central SOX team established the overall approach by developing entity level controls using the COSO framework. They wanted to take a centralized approach towards both entity and activity level controls including application and general IT controls. GTD and the committee representative worked together to agree an approach to 404 compliance utilizing GTD's existing Process Framework, documentation and controls testing standards. This approach was offered to non-GTD IT functions for adoption. According to the Programme Director, the organization received little guidance from consultants, PCAOB, external auditors, and SEC committee.

> "We developed our own understanding about 404s requirements. We spoke to our internal audit department and legal department to get their interpretation of SOX. We didn't want to rely on external consultants as we felt they didn't know much more than we did." (Programme Director)

The Programme Director, along with the IT representative in the central team, conducted a study of competitors to understand their approach to Section 404 compliance for information systems. They used the COBIT framework to model their approach. COBIT sets out standard controls organizations are expected to achieve, exemplified by IT security. The SOX Programme team also undertook research to explain how COBIT met requirements of the COSO framework. They used their documentation to show controls were in place and were being tested. They discussed the proposed methodology with external auditors. The auditors ratified the methodology as acceptable. Staff directly involved with SOX attended seminars and forums organized by the big four audit houses to reconfirm their approach and to understand how others were implementing 404 to remain consistent with competitors. Much of this guidance was freely available. One of the central team's overarching concerns was to ensure that Alpha was compliant in all respects but was not going beyond Section 404's basic requirements.

> "Compliance is a huge cost to us and provides the organization with no real competitive advantage. Yet we were conscious that failure to comply would mean harsh penalties potentially so we didn't mind spending money on getting it right but equally if we spent too much we wouldn't get a return on that investment." (Programme Manager)

GTD identified a Program Manager to take Section 404 implementation forward within the division. The GTD Program Manager created a standard GTD governance structure, including a Project Control Committee (PCC) with representatives from relevant GTD departments and the committee representative. The PCC used GTD's process framework to focus on significant processes and controls to ensure Section 404 compliance within GTD. After the PCC identified the scope of Section 404 within GTD, they modified an existing template to document processes and controls and attest documentation. The PCC discovered that existing controls were adequate and already in place, and consequently existing IT controls were judged to be quite sound. These included controls for the following processes: change management, performance and capacity management, data back-up and recovery, security and continuity services, operate and monitor services, incident management, user requirements, design, develop and test solutions and an overarching process to manage GTD processes.

Knowledge building is evident from the activities of the SOX Program Director, SOX Project Leader, and various committees. The lending process pilot exemplifies an in-house experiment to understand first-hand the implementation of the new regulations. The central team gathered relevant SOX knowledge to develop necessary Section 404 documentation of GTD's internal controls.

Knowledge deployment includes the appointment of a knowledgeable SOX program director and a central team coordinating across divisions and bringing in knowledgeable individuals (consultants and auditors) to increase content. Adoption was spurred by setting up seminars and presentations in appropriate form. The SOX program director and project leader dispersed knowledge about Section 404 throughout the organization through the intranet and aided adoption by interacting with users.

In terms of *mobilization* the organization made a moderate amount of effort. Top management and Board sponsorship are evident given that they are responsible for overall compliance. However, little emphasis has been placed on efforts to get employee buy-in to Section 404 implementation.

Subsidization is where top management provided resources for Section 404 implementation and also provided 'shared organizational resources' in the form of the SOX program director and IT rep for GTD to draw upon. Complementary products and services for speeding implementation such as creating a central knowledgebase and purchase of a process management tool, ensuring there were no caps on expenditure to access expertise from external sources, and vertical divisions being able to allocate and control funds to implement internal control show that subsidization is widely used by the organization.

Standardization (also referred to as standard setting) is used as a power-based action in the specification of minimum standards for documentation and design of controls. The Group has mandatory standards and expects people in GTD to comply. The standards are intended to ensure consistency of compliance across the divisions. The central team made clear that action will be taken against divisional heads that deviate from the standards; however, specific methods of implementation could differ to suit the specific circumstances of the business unit. It is interesting to note that IT standards were driven by GTD. These standards were agreed between GTD and the IT representative from the central team. These standards were only applicable to IT, and only proposed for other smaller IT functions (either geographically remote, not yet integrated businesses or specialist support teams). GTD standards were not mandated across any other area outside of GTD unless the central team wanted to do this. The central team adopted GTD's standards which were also approved by Alpha's auditors.

The manifestation of *innovation directives* mandates that existing and newly developed processes and systems conform to 404 requirements. The approach was top down for overall direction but the implementation was bottom up. Other innovation directives are top management's content creation (project plans, etc.) and the project leader's efforts such as putting all communication from senior management on the intranet. The stance that top management adopted in Section 404 implementation was that the organization always had controls and SOX required it to provide the necessary supporting evidence.

BETA GROUP

Beta is a part of the consulting division of a large US based global professional services group with operations in over 25 countries including the UK. Beta initiated a formal SOX program in the US soon after the Act was passed in 2002. Although SOX legislation was monitored before it was passed, little in terms of action was taken until it became law. In early 2004, practical implementation started for Beta in the UK. There are four senior individuals on its SOX program including the Regulatory Accountant, Finance Director, SOX coordinator, and US liaison. The US Global Chief Financial Officer, who is also a member of the global finance team, is responsible for global SOX-US liaison. The Beta UK SOX team comprises the UK CFO and CEO and the four individuals mentioned above. Beta has used internal resources and has two people dedicated to each major business cycle. There were twelve individuals involved in SOX for Beta UK, including the top team.

The organization took a program management approach to SOX implementation. An audit program was initiated to develop questionnaires covering control objectives, control activities, test status, source, assessor's name, sample size, and overall status. This was done for five major business processes, i.e. revenue, expenditure, company level controls called 'Tone from the Top', treasury and payroll, and financial reporting. The company level controls applied are pervasive controls which included the level of internal oversight, operations of board, CEO remit from board, and delegation of power from board to subsidiary committees. The tasks in 404 implementation involved developing control narratives, defining systems of internal control and control objectives, testing conclusion, monitoring the project in terms of percentage of completion, and assessing whether or not Beta UK were in compliance; essentially covering 404 from start to finish. IT was crucial for demonstrating system compliance. It expanded on control narratives developed by the SOX team and played a fundamental role in defining how the firm operated its internal controls. Beta UK created templates for documenting processes and controls and circulated these to member firms within the Group.

The UK IT organization was informed that, although they reported to Global IT organization, the overall sponsor for SOX implementation is the Global Finance function based in the US. The UK IT organization's role was to support Global Finance in ensuring the accuracy and validity of information and to test and remediate controls. In terms of Section 404, the Global IT function, also based in the US, developed an assessment method for IT controls based on the COBIT framework. Global IT sent this assessment to Beta's IT organization in the UK. Concurrently, the UK IT organization was in the process of changing all its back office systems, processes,

architecture, and infrastructure to a new data center. The UK IT organization's challenge was to meet both SOX and transfer deadlines. They liaised with Global IT for implementing Section 404 within the UK firm although there was little direct contact with the UK business. Beta UK and its IT organization did not undertake any research as they were driven mainly by time pressures. The UK SOX team concluded, based on internal assessments, that the Beta UK has a robust system of internal controls. They identified no significant areas where there is a need to introduce new controls. From discussions with the business, the UK SOX team became aware that the communication of Section 404 standards and policies needed to be improved. Beta UK has put in place policies to ensure the latest standards and policies are communicated. In a small number of instances, the UK SOX team identified areas where Beta could enhance its controls. The changes the UK SOX team made evolved through testing are a direct result of Section 404. They are aiming to achieve best practice and consistency across their business processes.

Knowledge building is evident in the staggered implementation of Section 404. Most of the knowledge building occurred in the US and was then adapted to suit non-US subsidiaries. Given their time pressures, UK managers realized that the information and experience of the US could be applied to support their own divisional SOX strategy. Their solution was a hierarchical design that linked SOX focus areas to project content.

Knowledge was deployed in this case by means of the intranet and the use of a web based tool that aided dissemination of information. The organization created a Sarbanes Oxley space on their intranet to act as a repository for the 404 information. This contained the latest guidance from the PCAOB, procedures that were to be adopted across the organization, general information about SOX and s404, and its impact on the organization. In the UK, the intranet was accessed mainly by people who had some direct interest in SOX and Section 404 compliance; hence, it was used by a small number of people. According to the Finance Manager:

> "The information on the intranet was useful because it was up to date and we could direct other people who wanted information about SOX to it. It was a good way of creating awareness".

Another knowledge deployment tactic was the deployment of knowledgeable individuals across divisions to assist with the implementation. About four or five individuals were sent to the US and Australia from Beta UK and Beta UK had the same number of people transferred from there.

Beta used *subsidization* in allocating funding to implement 404 as evident in procuring a web based system for documentation and monitoring. Funding was made available in the form of peoples' time that was used for implementation. Beta UK made the services of the intranet coordinator available for the organization as a whole and employed existing resources. As Beta UK perceived compliance to SOX as 'necessary', they applied subsidization as a power-based action to ensure implementation progress.

Mobilization took the form of an awareness drive aimed at key individuals, rather than general organization-wide awareness creation. This implementation can be seen as formal, and actions of an influential nature were barely considered. The implementation of Section 404 was mandated and linked strategically to UK IT Organization's divisional project activity. Traditional oral means of communication in the project domain were replaced in favor of documentation. The focus of the UK SOX team was on getting consistency in approach across the organization.

Innovation directives are deployed extensively. Managers implementing 404 took the view that people affected by the new standards would have little option but to change as Section 404 compliance was mandatory. Information about 404 projects, such as stage of completion, templates used, and key individuals involved, etc. had to be published on the intranet and staff under the jurisdiction of divisional and functional managers were involved in documentation and testing. The view of the organization was that as information on Section 404 compliance was important they would have to demonstrate it.

GAMMA GROUP

Zeta is a global professional services firm registered with the PCAOB. Over forty countries in which Zeta operates, including the US and UK, are influenced by SOX. As mandated by law all firms that audit SEC registered companies are required to register with the PCAOB. This requirement influences Section 404 implementation from three dimensions: a) the registration process with PCAOB required building processes and systems; b) incorporating a system for authorization for services, rules on what Zeta can and cannot sell to its clients; and, c) helping clients with compliance. Zeta identified a Director to lead each of these aspects. A specific division within Zeta, The Professional Risk and Technical Quality Group, was involved in activities such as developing training, answering specific internal queries, public speaking, and articles on SOX. Zeta coordinated internationally with member firms to develop one set of information. They developed knowledge repositories which are accessible globally through their intranets.

Gamma is Zeta's UK practice. Gamma offers a range of audit and non-audit services across industries. Gamma is structured in various client facing and internal divisions. Section 404 has direct and indirect implications on all of Gamma's divisions. This case focuses on the implementation of Section 404 within IS services in Gamma.

According to Gamma, the requirement for organizations to have internal controls is well established as is the onus on auditors to consider internal control environment in designing and carrying out audit procedures. However, Gamma accepts that the reporting requirements stipulated by SOX and the PCAOB for both issuer and audit firms are new. It is these reporting requirement that lead to the development to the evidentiary requirements.

Gamma established a steering group for SOX. The steering group comprised senior partner as chair with overall responsibility for independent compliance and regulation, people at regional compliance level, regional partners, internal legal council, and IT people. The steering group had responsibility to define the brief for Section 404 compliance. The project was guided by top management through the heads of the steering committees, as they reported to the Group CEO/COO. Regional representatives on steering groups communicated with each other to maintain regional level coordination.

Gamma reused much of Zeta's 404 compliance work. Systems developed for the US were rolled out in the UK as they were in other countries affected by SOX. It was the responsibility of the steering group to define the brief. Use of written formal communication, regionalization, training, knowledge bases, links, changing methodologies, etc. aided Section 404 implementation. There were significant amounts of travel for individuals involved with Section 404 implementation. A number of meetings were held in London both at steering committee and 404 project levels.

Knowledge building initially occurred in a formal manner, as SOX developments were monitored in the US. Sarbanes Oxley Data Centre - a central hub of knowledge and the way of knowledge sharing - was created. There were weekly news roundups on policies and standards, tips, e-learning, and research.

Knowledge deployment included sending Gamma people to the US for training and experience, as well as making the Central SOX Database accessible via the intranet (to disseminate best practice) to employees. The concept of a corporate intranet functioning like the contents of a book is in itself knowledge deployment, allowing employees to know as much as they would be interested in knowing about the subject. All IT personnel involved in 404 had access to the IT business cycle on the web-based tool. In addition, they communicated on a face to face basis.

Subsidization took place in the form of the central resources Risk and Quality, Systems Performance Analysis, technical specialists that provided free know how, company-wide SOX training courses and helpdesk support. Again in this case, funding did not appear to be an issue as Section 404 implementation is necessitated by law. Gamma's view is that preparing clients for a robust audit of their controls is vital to Section 404 implementation and invested in people to ensure they had the skills for rigorous application of 404.

Standardization is used as an action in this case through a uniform compliance architecture, information model, and categorization of processes and technology. The firm has formalized the levels of discretion with regards to adherence to standardized controls.

Innovation directives are defined by business needs and originate from the needs of users. Top management sponsorship is critical to completing Section 404 implementation in the short timescales defined by the financial year end of the firm. However, the prevailing view is that 404 requirements are not really new, as frameworks such as COSO and COBIT have been around for some time and are already incorporated in their internal controls. Gamma has had the necessary Section 404 requirements in place for use with clients, but now they are required to prove to the authorities that these requirements are being used in practice. Gamma's IT organization views 404 as a business problem not an IT problem. So the role of the IT Organization was seen as helping to meet business needs which meant that 404 had to be driven by business.

VI. DISCUSSION

Our discussion first highlights the actions the case study organizations took to address the institutional pressures they faced. Second, we elaborate each implementation action and condense our findings in recommendations for how IS organizations can be more effective in the implementation of section 404.

Mimetic pressures cause organizations to copy each other and become more alike others in its environment. Mimetic pressures are exerted on organizations when faced with practices that others have adopted; and adoption leads to perceived success, which in the context of 404, is to gain certification that appropriate controls are in place. Organizations imitate others that experience similar external pressures in order to acquire legitimacy or social fitness. Organizations succumb to mimetic pressures to minimize the costs of acquiring knowledge, reduce learning costs, and manage the risks of being the first to address a new challenge.

When looked at from an institutional perspective, we see that case study organizations imitated each other in Knowledge Building. They set up central teams to create a single approach for their organization, learnt from auditors etc. We observe that the organizations used many of the same techniques, e.g. intranets and repositories for Knowledge Deployment. All the organizations used Subsidies to ensure Section 404 compliance was achieved. Innovation Directives were used to drive implementation using power. However, this had little effect on creating demand users. Mobilization was used to create a positive impression about 404 and the case for ensuring timescales and deadlines were achieved. Standards were set so that subsidiaries could imitate each other.

Coercive pressures are formal and informal pressures on a focal organization by other organizations on which it is dependent. In the context of 404 implementation, at institutional levels, audit firms and their client organizations are dependent on the PCAOB. Coercive pressure arises from the severe sanctions the PCAOB can impose upon audit firms, like removing an auditors' license, and the power audit firms have over their clients by withholding certification of the organization's accounts. From the case studies we observe that they used power-based actions of standard setting, innovation directives, and subsidies to ensure subsidiaries complied with deadlines and adhered to documentation requirements. The relatively softer influencing actions of knowledge building, knowledge deployment, and mobilization played a lesser role.

Normative pressures focus on social pressures to conform to a set of norms or standards that are widely accepted in the industry. The norms become standards of behavior that organizations' leaders coalesce around. These standards are shared across organizations, for example, between audit firms, as no one audit firm would want to be singled out as being different in terms of their standards of 404 compliance.

An apparently different standard could leave the audit firm open to attack by others. Normative behavioral pressures exist between the audit firm and its client organizations. These pressures were addressed through Knowledge Building and Knowledge Deployment, exemplified by running seminars and training events for clients. Organizations too learnt from one another using the same actions of Knowledge Building and Knowledge Deployment. Power-based actions such as standard setting, innovation directives, and subsidies were used to bring subsidiary behavior in to alignment with head office requirements. This included the use of tactics such as 'name and shame' where the heads of subsidiaries that were non-compliant were reported to the CEO and CFO.

Having examined the institutional pressures, we turn our attention to each action and develop a recommendation for IS organizations from an institutional perspective. In terms of *knowledge building* all cases relied on Sarbanes Oxley Central program teams to develop a core base of knowledge about 404. The program team used a number of tactics such as attending seminars, searching guidance from their auditors about the COBIT and COSO frameworks, ways of adapting these to the organization operations, and commissioning specific pieces of research on the relationship between COBIT and COSO. In the case of Beta and Gamma whose head office and Central Program Team are based in the US, knowledge building was carried out in the US and handed down to the UK subsidiary. The UK IT Manager stated:

> "We had an assessment passed to us by Global (US-based) on COBIT. We didn't do any research in the UK". (IT Manager, Beta).

Alpha undertook its knowledge building in the UK relying very little on its US subsidiary. Instead, it drew heavily on the knowledge of its auditors and seminars provided by the bigger audit firms. Gamma's knowledge building activities were internally focused. According to one respondent:

> "We worked with internal experts for understanding needs and defining standard IT requirements. We worked on identifying what are the things we need to make sure for the systems to work right." (Compliance Partner, Gamma).

It is noteworthy that the IT organizations in Beta and Alpha had a small role to play in knowledge building. Even within the Central Program Teams knowledge building was done by people with financial audit or compliance skills. IT organizations appear to be recipients of 404 knowledge building activities. However, one IT manager claimed in retrospect:

> "Going forward we would take up Sarbanes Oxley training to build knowledge". (IT Manager, Beta).

Although knowledge building appears to be an obvious diffusion action in theory, it is also highly necessary in practice.

> Recommendation #1:
> Knowledge building is a necessary action for Section 404 implementation. Section 404 knowledge building is best undertaken by a central team. IT organizations need to take on greater responsibility for developing their knowledge of Section 404 implementation.

All three organizations used intranets and web-based tools to spread Section 404 knowledge, *knowledge deployment*. They developed knowledge repositories to cascade information from central program teams to IT organizations. The repositories contained information about 404 and its requirements, slide packs, guidelines, templates, and roll-out plans. In addition, the organizations used more standard forms of communication. For example, Beta used existing face-to-face communication mechanisms such as team briefings and corporate presentations: "We did tend to deploy the top team". (Finance Managers, Beta). Two organizations, Beta and Gamma, transferred employees as a means of moving knowledge from those departments that had it to those that didn't.

> "About 100 people were sent to the US from the UK for a period of 6 months to a year. They were manager and senior associate level people with 7-8 years of experience". (Global IT Directors, Gamma).

> "The best way to pass information immediately was to send employees to other entities. We sent people to the US, Australia and had people from there". (IT Manager, Beta).

These individuals were expected to build up their experience and help deploy 404 in their home country, develop case studies and examples which could be shared. Other tactics for knowledge deployment included video-conference meetings, regular phone calls between key players in different subsidiaries and the central program team, progress monitoring reports which tracked the extent to which each subsidiary had achieved the overall plan, and consultations between subsidiaries that were more advanced with those less advanced with their 404 implementation.

Each organization's central program team accessed external knowledge and expertise. Central program teams went directly to the PCAOB web site to keep up to date with most recent developments. All organizations took legal council from in-house and external lawyers. The two quoted companies discussed 404 requirements with external auditors that attend to their boards' statement on internal controls. These discussions enabled central teams to plan overall 404 implication program, break this down into constituent projects, and develop reporting mechanisms. We argue that knowledge deployment is essential to Section 404 implementation.

Recommendation # 2: Knowledge deployment is a necessary action for creating and deploying 404 implementation plans. Technology, in the form of knowledge repositories and portals, are vital to ensuring one version of 404 is implemented throughout the organization. A variety of communication mechanisms can be used to spread Section 404 knowledge.

We expected *subsidy* to form a key action for Section 404 diffusion. Nonetheless, we were surprised by the position adopted by these organizations. All said 404 implementation funding was a non-issue; none of the respondents were able to place a single financial figure simply because 404 expenditures did not fit into any single cost code. One manager estimated that the cost incurred by his subsidiary alone was 'six figures'. The prevailing view was that as the organization had little choice but to comply, costs were barely considered. One respondent said that costs were managed by having "requirements-based budget" (Sarbanes Oxley Programme Director, Alpha). This point is made by another respondent:

> "Requirements have been changing every three months and we made it (costs) up as we went along. We didn't know how any number of factors could play out…costs needed to evolve". (IT Partner, Gamma).

The data suggests there were few, if any, resource constraints placed upon the central program teams or the subsidiaries. The central team was able to draw on resources as needed and numbers in specialist departments such as internal control grew. Expenditure on Section 404, specific information technology has been minimal. All time invested in an application that could store 404 related documentation e.g. process maps and control narratives.

Recommendation #3: Subsidies are important to the initial development phase of Section 404 and its subsequent implementation and use in the organization and the IT Organization

Innovation directives were widely used in the case organizations. The consensus across the organizations is summarized by one respondent:

> "We (The Central Programme Team) are telling. Tell not sell. We have a brief from the Board and Finance Director…The organization is populated with senior staff who would

> prefer autonomy but they have no room to maneuver. There might be some push-back but nothing very serious". (Finance Manager, Beta).

According to another respondent implementation has been top-down with consistent methodologies rolled out across subsidiaries. Although not the primary aim of Section 404, this legislation has led to IT organizations standardizing their internal processes:

> "We have change control processes for which there are many different versions depending on the application. The need to and cost of documenting each variation has led to these being rationalized to one change control process". (Global IT Director, Gamma).

In spite of this 'tell' approach and the rationalization of processes, use of innovation directives is less clear about changing actual practices to bring them into line with the documented controls. In all three cases, respondents saw little need for change in behaviors or 'what people do in their work' due to Section 404 implementation:

> "There have been no changes in internal structure, operations, processes and systems". (Program Directors, Alpha).

We argue that without even small changes to these aspects of the organization, the edicts and directives issued from the centre are unlikely to be fully implemented. One reason for this according to one respondent is:

> "Changing behaviors will lead to a massive battle in most organizations. Organizations that are trying to put controls in place find that this is causing lots of problems". (IT Partner, Gamma).

Thus, the future that emerges is that although Section 404 implementation is being driven from the top of the organization, through the central program team, the actual input on users in the organization is minimal. The organizations appear to be doing the "minimum to comply rather than change what they are doing in the business and driving change" (IT Global Director, Gamma). We suggest that organizations are treating Section 404 implementation as a 'tick-box' routine.

Recommendation #4: Innovation directives are less effective for creating demand – pull from users. They may be more effective to support implementers 'push' the need to achieve Section 404 certification, throughout the organization, before and during implementation.

Mobilization in the form of Communication about awareness of SOX was carried out to a very narrow group of people: Those directly involved in the Sarbanes Oxley program. According to one Programme Director:

> "We didn't take the view that we needed to create awareness. Communications were sent only to people actually doing (404) work e.g. process improvement teams. Awareness was not really necessary as many staff are in operational roles and they don't need to understand (404) requirements. Communication was facilitated through the central program team on a need to know basis". (Programme Director, Alpha).

In another case, the direction of communications was top down with little time for questions from users. The pressure was on getting Section 404 compliance done and out of the way.

> "The focus was on 'are you on time and are you going to do it (complete the documentation)…don't ask questions just do it was the impression from the global team. Get it done and clear it out of the way so we can get back to business". (IT Manager, Beta).

The assumption underpinning these views would appear to be that Section 404 does not require the organization to 'do' anything differently in the business. The underlying view is that 404 requires financial processes and controls to be documented and, provided this documentation is in place for the external auditors to test so that the board can claim a sound set of internal controls in the financial statements, this organization has met the requirement of 404.

> "There are bigger more important things happening (than 404). General business managements' view is that the requirements of the Act are not asking us to do anything different from what we have been already doing. We were already doing it (processes and internal controls) but we needed to put in place the documentation so that the auditors are able to identify with it". (Programme Director, Alpha).

> "Most people don't know what Sarbanes Oxley is and need not be aware of it either". (Compliance Partner, Gamma).

We find this surprising as SOX requires processes and controls to be in place and documented wherever it is possible that these can have a material affect on figures reported in financial statements. A common occurrence is the use of spreadsheets to handle figures to prepare reports. This can happen at many different levels; for instance, in a bank, this could happen in a branch, area office, head office, and the global head quarters. The use of spreadsheets, databases, and project plans occurs in all business cycles and processes contained in COSO and COBIT frameworks. Examples include inventory controls, pricing, account analysis and reconciliations, and program changes. This suggests a much wider audience, than those in the finance and IT organizations, ought to be aware of 404, its implementation and implications.

Recommendation #5: Mobilization is a necessary action for those directly involved in Section 404 implementation; such as finance, compliance, internal audit, and IT organizations during the initial stages of implementation. Mobilization is an important action for positively influencing behaviors of people in the organization towards Section 404 implementation.

In terms of standard setting, all three organizations had IT standards and controls already in place. To this extent, the organizations were not brand new start-up sites. The central program teams, in two quoted organizations took existing standards and updated these based on advice from their auditors in the case of the UK-based organization and the US central team in the case of the US subsidiary. The general view across all respondents is that standards existed prior to Sarbanes Oxley.

> "We have a robust system of internal controls. These are no significant areas where we have identified the need for new controls". (Finance Manager, Beta).

> "We were largely capturing controls already in place but over time had not been documented". (IT Manager, Beta).

Nonetheless, 404 implementation did require changes to controls, for example, in Beta managers could orally delegate authority to approve certain financial transactions. As a result of 404, this delegation has to have written confirmation. Gamma introduced a compliance architecture that complies with the regulations and provides a coherent set of standards that are uniform throughout the globe. Progress towards adopting this compliance architecture has been slow because IT controls have tended to be voluntary. Users are expected to use the architecture to gain consistency. In Alpha, the standards set by the central team are mandatory:

> "Group (the central program team) has issued mandatory standards and expects compliance. It is made clear that action will be taken against instances of non-compliance". (Programme Manager, Alpha).

Historically, these organizations have not had many mandatory controls. These were typically aimed as guidelines to suggest courses of action. With 404, not only do organizations have to

increase the controls that are mandatory, they have to allow different subsidiaries a degree of freedom in the way in which the standards are implemented. Differences are caused by the nature of the application, e.g. payroll or the characteristics of the subsidiary.

> Recommendation #6:
> Standard setting is a necessary action for establishing 404 compliance requirements and achieving consistent implementation during the implementation stages of Section 404.

VII. IMPLICATIONS, LIMITATIONS, CONCLUSIONS

The empirical evidence suggests that even though each of the six actions was deployed to some extent, there is an emphasis on the power-based dimension in each case. Innovation directive, subsidy, standard setting, and knowledge deployment were largely driving Section 404 implementation for the IT organizations of these organizations and were mainly regulated by the central SOX team. This suggests that organizations were faced with the externally driven coercive pressure of 404 compliance, applied similar coercive pressures internally to ensure subsidiaries achieve compliance within the deadlines set by the legislation. They also experienced mimetic pressures as each of the case study organizations imitated competitors to ensure avoided sanctions. Normative pressures on the management of organizations are apparent as they had to ensure their organizations financial controls were certified. Failure to achieve this would suggest that individuals running non-compliant organizations take a lax approach to financial controls and that their behaviors are below those of their peers.

The use of institutional pressures may have been necessary given the size of 404 projects, their time-critical nature, and the implications of not getting the right controls in place. However, the influence based dimension was equally important in implementation (Anand, Ashforth, and Joshi, 2004). Our findings suggest that more effort could have been made towards specific knowledge building or mobilization activities. Many of the problems encountered by the cases study organizations can be traced to these two actions.

Our study suggests that IT Directors and CIOs need to educate people in their IT organizations with respect to 404 to ensure they understand its requirements and procedures. IT Directors and CIOs need to work more closely with their counterparts in the Finance function. Their efforts should be directed towards gaining stakeholder buy-in through mobilization to aid diffusion. They should plan to support the business through future strategic and operational innovations, especially where these require new or enhanced information systems changes. The implementation of these systems can be delayed where the changes affect key controls. Consequently, IT Directors and CIOs can find themselves in the unenviable position of holding back the business from achieving competitive gains.

This study opens up fresh lines of inquiry for further research. This study examined Section 404 implementation through the lens of institutional theory. There are significant potential insights to be gained from studying the implementation and diffusion of SOX and section 404 through other theoretical lenses. Specifically, we believe that resource-based and organization theories will yield interesting results. SOX, and 404 in particular, is fertile ground for trans-disciplinary research as the affects the social, political, identity, and governance fabric of an organization. A further area of work is to replicate this study by carrying out further cases, in different industries, to understand the implementation and diffusion of 404 in a variety of contexts, cultures, and countries. A new line of investigation could be started by researchers employing different methods. This research is based on the case study method. We suggest that the use of longitudinal studies in the interpretive tradition can show the effectiveness of specific tactics. There is a need for a more quantitative approach to understand aspects of 404 implementation such as the investment in IT costs and resources, the impact on other ‘strategic’ initiatives as scarce resources were diverted to 404 implementation and the extent to which IT organizations are prepared for SOX’s annual cycle.

This study has its limitations. In particular, it is based on a small number of cases and, hence, the generalizability of its findings can be questioned. The issue of generalizability is addressed by understanding that the fundamental aim of the case study design is to generate rich contextual data that provide insights into a phenomenon, which in this study is the implementation and diffusion of section 404 of the SOX Act.

In summary, we adapted King et al.'s taxonomy based on institutional theory to examine 404 implementation and diffusion. Six diffusion actions were developed and implementation tactics were categorized based upon these actions. In-depth case studies were conducted in three global organizations who had implemented 404 to understand their implementation tactics. Data from the three cases were analyzed to develop recommendations to describe the implementation of 404 in these organizations. The taxonomy and recommendations provide a common language and basis of understanding from which to maintain 404 and SOX compliance.

Acknowledgement: The authors are grateful for the support provided by Reena Malharkar during the data collection phase of this study.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.
2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. the author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Aguilera, R. V. & Jackson, G. 2003, "The cross-national diversity of corporate governance: Dimensions and determinants", Academy of Management Review, vol. 28, no. 3, pp. 447-465.

Anand, V., Ashforth, B. E., & Joshi, M. 2004, "Business as usual: The acceptance and perpetuation of corruption in organizations", Academy of Management Executive, vol. 18, no. 2, pp. 39-53.

Anon 2003a, "Sarbanes-Oxley claims first European success", International Financial Law Review p. 1(1).

Anon 2003b, "SEC enforces first Sarbanes-Oxley penalties", Information Management Journal, vol. 37, no. 6, p. 21(1).

Avgerou, C. 2000, "IT and organizational change: an institutionalist perspective", Information Technology and People, vol. 13, no. 4, pp. 234-262.

Banham, R. 2003, "Period of adjustment", Journal of Accountancy, vol. 195, no. 2, p. 43(6).

Barnhart, S., Marr, W., & Rosenstein, S. 1994, "Firm performance and board composition: Some new evidence", Managerial and Decision Economics, vol. 15, pp. 329-340.

Benbasat, I., Goldstein, D., & Mead, M. 1987, "The Case Research Strategy in Studies of Information Systems", MIS Quarterly, vol. 11, pp. 369-386.

Berg, P. F. S. 2003, "Unfit to serve: Permanently barring people from serving as officers and directors of publicly traded companies after the Sarbanes-Oxley Act", Vanderbilt Law Review, vol. 56, no. 6, p. 1871(36).

Blaikie, N. 1995, Approaches to Social Enquiry Polity Press, Cambridge, MA.

Cadbury Commission 1992, The Financial Aspects of Corporate Governance, Gee and Co, London.

COBIT® 1994, Control Objectives for Information and related Technology, IT Governance Institute.

COSO 1994, Internal Control - Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission.

Covaleski, M. A. & Dirsmith, M. W. 1988, "An institutional perspective on the rise. Social transformation, and fall of a university budget category", Administrative Science Quarterly, vol. 33, no. 4, pp. 562-587.

Crowston, K. & Myers, M. D. 2004, "Information technology and the transformation of industries: Three research perspectives", Journal of Strategic Information Systems, vol. 13, pp. 5-28.

Daily, C. M., Dalton, D. R., & Canella Jr., A. A. 2003, "Corporate governance: Decades of Dialogue and Data", Academy of Management Review, vol. 28, no. 3, pp. 371-382.

Dalton, D. R., Daily, C. M., Certo, C., & Roengpitya, T. 2003, "Meta-analyses of financial performance and equity: Fusion or confusion?", Academy of Management Journal, vol. 46, pp. 13-26.

Dalton, D. R., Daily, C. M., Ellstrand, A. E., & Johnson, J. L. 1998, "Meta-analystic reviews of board composition, leadership structure, and financial performance", Strategic Management Journal, vol. 19, pp. 269-290.

Dewing, I. P. & Russell, P. O. 2003, "Post-Enron developments in UK audit and corporate governance regulation", Journal of Financial Regulation and Compliance, vol. 11, no. 4, p. 309.

DiMaggio, P. J. & Powell, W. W. 1983, "The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields", American Sociological Review, vol. 48, no. 2, pp. 147-160.

DiMaggio, P. J. & Powell, W. W. 1991, "Introduction," in The New Institutionalism in Organization Analysis, W. W. Powell & P. J. DiMaggio, eds., University of Chicago Press, Chicago, pp. 1-38.

Duffy, M. N. 2004, "Section 404 opens a door", Journal of Accountancy, vol. 197, p. 8.

Eisenhardt, K. M. 1989b, "Building theories from case study research", Academy of Management Review, vol. 14, no. 4, pp. 532-550.

Eisenhardt, K. M. 1989a, "Agency theory: An assessment and review", Academy of Management Review, vol. 14, pp. 57-74.

Fama, E. F. 1980, "Agency problems and the theory of the firm", Journal of Political Economy, vol. 88, no. 21, pp. 288-307.

Fama, E. F. & Jensen, M. C. 1983, "Separation of ownership and control", Journal of Law and Economics, vol. 26, pp. 301-325.

Ferrell, O. C. 2004, "Business ethics and customer stakeholders", Academy of Management Executive, vol. 18, no. 2, pp. 126-129.

Goodstein, J. D. 1994, "Institutional pressures and strategic responsiveness: Employer involvement in work - family issues", Academy of Management Journal, vol. 37, no. 2, pp. 350-382.

Greenwood, R. & Hinings, C. R. 1996, "Understanding radical organizational change: Bringing together the old and new institutionalism", Academy of Management Review, vol. 21, no. 4, pp. 1022-1054.

Ivancevich, J. M., Duening, T. N., Gilbert, J. A., & Konopaske, R. 2003, "Deterring white-collar crime", The Academy of Management Executive, vol. 17, no. 2, pp. 114-127.

Jensen, M. C. 1993, "The modern industrial revolution, exit, and the failure of internal control systems", Journal of Finance, vol. 48, pp. 831-880.

Jepperson, R. L. 1991, "Institutional effects, and institutionalism," in The New Institutionalism in Organizational Analysis, W. W. Powell & P. J. DiMaggio, eds., University of Chicago Press, Chicago, pp. 143-163.

King, J. L., Gurbaxani, V., Kraemer, K. L., McFarlan, F. W., Raman, K. S., & Yap, C. S. 1994, "Institutional factors in information technology innovation", Information Systems Research, vol. 5, no. 2, pp. 139-169.

Knights, M. & Reed, K. 2004, "UK plc dealt Sarbox deadline", Accountancy Age.

Kulzick, R. S. 2004, "Sarbanes-Oxley: Effects on Financial Transparency", S.A.M. Advanced Management Journal, vol. 69, no. 1, p. 43(7).

Maitland, A. BT chairman criticises US governance. Financial Times , 22(1). 2004. London.

Mayer, A. F. 2003, "Preparing for Basel II by Optimizing Sarbanes-Oxley", The Journal of Bank Cost & Management Accounting, vol. 16, no. 3, p. 27(7).

Meyer, J. W. & Rowan, B. 1977, "Institutional organizations: Formal structures as myth and ceremony", American Journal of Sociology, vol. 83, pp. 340-363.

Oliver, C. 1991, "Strategic responses to institutional processes", Academy of Management Review, vol. 16, no. 1, pp. 145-179.

Orlikowski, W. J. & Baroudi, J. J. 1991, "Studying information technology in organizations: Research approaches and assumptions", Information Systems Research, vol. 2, no. 1, pp. 1-28.

Pfeffer, J. 1981, Power in Organizations Pitman, Marshfield, MA.

Quall, J. C. 2004, "Implementing Section 404: A Practical Approach to the Sarbanes-Oxley Act", The CPA Journal, vol. 74, no. 8, p. 52.

Ray, G., Barney, J. B., & Muhanna, W. A. 2004, "Capabilities, business processes, and competitive advantage: Choosing the dependent variable in empirical tests of the resource-based view", Strategic Management Journal, vol. 25, pp. 23-37.

Robey, D. & Boudreau, M. C. 1999, "Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications", Information Systems Research, vol. 10, no. 2, pp. 167-185.

Schaub, A. 2004, "Europe and US must guard against regulatory clashes", International Financial Law Review p. 1(1).

Schutz, A. 1967, The Phenomenology of the Social World Northwestern University Press, Evanston.

Scott, W. R. 1987, "The adolescence of institutional theory", Administrative Science Quarterly, vol. 32, no. 4, pp. 493-511.

Suchman, M. C. 1995, "Managing legitimacy: Strategic and institutional approaches", Academy of Management Review, vol. 20, pp. 571-610.

Swartz, N. 2003, "The cost of Sarbanes-Oxley", Information Management Journal, vol. 37, no. 5, p. 8(1).

Teo, H. H., Wei, K. K., & Benbasat, I. 2003, "Predicting intention to adopt interorganizational linkages: An institutional perspective", MIS Quarterly, vol. 27, no. 1, pp. 19-49.

Tsoukas, H. 1996, "The firm as a distributed knowledge system: A constructionist approach", Strategic Management Journal, vol. 17, pp. 11-25.

Yin, R. K. 1989, Case study research: Design and methods, Revised edition edn, Sage Publications, Inc., Newbury Park.

Zucker, L. 1987, "Institutional theories of organization", Annual Review of Sociology, vol. 13, pp. 443-464.

ABOUT THE AUTHORS

Dr. Ashley Braganza is a member of faculty at the Cranfield School of Management at Cranfield University, Bedford, UK. He is the Director of the Centre for Organisational Transformation and Director of nexus, The Knowledge Exchange. He has authored three books and numerous conference and journal papers. His publications have appeared in prestigious practitioner and academic journals such as Information Systems Journal, Communications of the ACM, International Journal of Information Management, International Journal of Project Management, International Journal of Knowledge Management, Knowledge and Process Management, Integrated Manufacturing Systems, International Journal of Entrepreneurship and Innovation Management, Int.J. Services Technology and Management, and the Journal of Strategic Change.

Dr. Kevin C. Desouza is on the faculty of the Information School at the University of Washington. He is a founding faculty member of the Institute for Innovation Management (I^3M) and is an affiliate faculty member of the Center for American Politics and Public Policy, both housed at the University of Washington. He has authored *Managing Knowledge with Artificial Intelligence*, co-authored *The Outsourcing Handbook*, *Managing Information in Complex Organizations*, and *Engaged Knowledge Management*, and edited *New Frontiers of Knowledge Management*. His most recent book is *Agile Information Systems*. In addition, he has published articles in practitioner and academic journals such as the *Communications of the ACM, Information & Management, Technology Forecasting and Social Change, Journal of Engineering and Technology Management, Business Strategy Review, Across the Board, Journal of Contingencies and Crisis Management, Business Horizons, Communications of the AIS, European Journal of Information Systems, Government Information Quarterly, Journal of the American Society for Information Science and Technology, IEEE Software, IEE Engineering Management, Human Systems Management, Journal of Business Strategy, Information Systems Management, Journal of Knowledge Management, International Journal of Technology Policy and Management*, *Disaster Recovery Journal,* among others. Dr. Desouza is a fellow of the Royal Society of Arts.

.

Communications of the Association for Information Systems

ISSN: 1529-3181