IGI PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

ITJ4136

This paper appears in the publication, **Journal of Organizational and End User Computing**, Volume 20, Issue 2
edited by **M. Adam Mahmood**

Diffusing Management Information for Legal Compliance:
The Role of the IS Organization Within the Sarbanes-Oxley Act

Ashley Braganza, Cranfield University, UK
Ray Hackney, Brunel University, UK

ABSTRACT

Information systems are vital to successful compliance with Section 404 of the Sarbanes Oxley Act. However, there is little published academic literature which reports systematic studies that explain how IS organizations implement 404. Institutional theory was adopted as the lens through which to examine the experiences of 404 implementation in three global organizations. The methodology for the research involved in-depth case study analysis. We conclude that key implementation drivers for 404 are directives from senior authorities, financial and resource subsidies, standards being set and adhered to, and knowledge being deployed. The findings are believed to present significant insights into the complexities and role of IS in providing valid and appropriate approaches to 404 compliance.

Keywords: implementation; information systems; institutional theory; Sarbanes Oxley

INTRODUCTION

The Sarbanes Oxley Act (SOX) creates the deepest changes to the Securities Exchange Commission (SEC) rules since 1934 (107th Congress, 2002; Banham, 2003; Aberdeen Group, 2005). The act was passed in response to financial misstatements and high-profile corporate frauds such as Enron, WorldCom, Tyco, and Global Crossing. The act aims to reduce the level and scale of financial fraud due to an organization's man-

agement being able to misrepresent its financial condition (Ferrell, 2004; Rone & Berman, 2004). Organization-wide strong governance—that is the formal and informal rules that guide organizational action and behavior—and robust controls are therefore seen as essential to avoiding future accountancy deficiencies.

Section 404 of the act requires organizations to provide external auditors with documentary evidence of the existence and effective functioning of processes, systems, and controls used to generate all financial and management information made available to the public. Since in most organizations, processes, systems, and controls are embedded in a wide range of information systems, the IS organization assumes a significant role in 404 compliance (Chan, 2004; Hackney, Burn, & Salazar, 2004;Coe, 2005).

This article analyzes the implementation of Section 404 within organizations through the lens of institutional theory. Unlike previous regulatory frameworks which are based on self-regulation, the act makes the management of effective internal controls mandatory. Furthermore, the act backs up the requirements for controls with severe penalties including fines and prison sentences for those in breach of its provisions. SOX is binding on all companies listed on any American Stock Exchange, and hence non-U.S. companies are subject to its provisions (Dalton & Dalton, 2005; Coffee, 2005). Therefore, companies incorporated in other legal jurisdictions, such as the UK, for example, can be prosecuted, for the first time, in U.S. courts for being in breach of SOX (Dewing & Russell, 2003). In the past, company officials, such as the chief executive officer (CEO) and chief financial officer (CFO), could only be prosecuted in the country of the company's incorporation.

TAXONOMY OF 404 INTERVENTION DRIVERS

There is a significant amount of practitioner literature available that provides managers with methods and procedures they need to consider when implementing Section 404 (Duffy, 2004; Ivancevich, Duening, Gilbert, & Konopaske, 2003; Mayer, 2003; Quall, 2004). However, as normal, the practitioner literature lacks a theoretical basis for the approaches being recommended and is akin to the plethora of prescriptions for successful implementation of information systems. As in the wider IS academic field, our aim is to examine the role of the IS organization when implementing Section 404 through a sound theoretical lens, based on valid methods, in order to provide conceptual insights for 404 implementation.

Section 404 adds to the body of corporate governance literature. The most common approach used to study corporate governance is agency theory (Dalton, Daily, Ellstrand, & Johnson, 1998; Dalton & Dalton, 2005), which stems from the seminal work of Berle and Means (1932). They argued that the separation of ownership (sharehold-

ers) and control (management) gave managers—agents—an opportunity to act in their own self-interest by making decisions or acting in ways to increase their financial prosperity rather than that of the shareholders (Fama, 1980; Jensen, 1993). A variety of methods are deployed to minimize the opportunities for promoting management's self-interest over that of shareholders. These are exemplified by managing the board's composition, strengthening the role of non-executive directors (Barnhart, Marr, & Rosenstein, 1994), and linking the board's compensation to shareholder returns (Cadbury, 1992; Dalton, Daily, Certo, & Roengpitya, 2003). These methods are essentially self-regulatory.

Prior to the SOX Act, the roles of executive and non-executive directors, as well as internal and external auditors, were considered to provide sufficient 'checks and balances' to avoid financial disasters on the scale of Enron. However, the SOX Act, and in particular Section 404, has swept away traditional forms of self-regulation by mandating organizations have transparent systems of internal controls. The act also places significant responsibilities and potential penalties upon audit firms, and through them, on organizations' management (Duffy, 2004; Ooms-Piepers & Degens, 2004). Agency theory appears to be of limited use because it neglects the effects that external institutions can have on organizations and their behavior. Agency theory takes a narrower perspective by focusing on internal actors (managers) and one external stakeholder (shareholders) (Daily, Dalton, & Canella, 2003). The theory is geared towards finding ways to minimize agency costs incurred by organizations to stockholders (Aguilera & Jackson, 2003) and barely addresses the power that external institutions can have on board behavior (Pfeffer, 1981; DiMaggio & Powell, 1983).

These limitations of agency theory are likely to yield superficial insights into the role of IS organizations in the implementation of 404. We argue that institutional theory enables deeper insights into 404 implementation as it takes into account multiple stakeholders within and outside organizations and the use of power and influence to bring about changes in practices (King et al., 1994). Institutional theory suggests that organizations conform with rules and regulations about appropriate conduct and behaviors to ensure legitimacy within their environment (Suchman, 1995). Institutional properties have been developed by numerous researchers (Covaleski & Dirsmith, 1988; Jepperson, 1991; Meyer & Rowan, 1977; Scott, 1987; Zucker, 1987; Avgerou, 2000; Crowston & Myers, 2004; DiMaggio & Powell, 1991; Goodstein, 1994; Greenwood & Hinings, 1996; Oliver, 1991; Teo, Wei, & Benbasat, 2003).

King et al. (1994) use institutional theory to develop a taxonomy to categorize IT interventions at institutional and organizational levels (Robey & Boudreau, 1999). We argue that Section 404 requires organizations to intervene

to change controls and processes embedded in information systems and have accordingly adapted King et al.'s taxonomy for the study of 404 implementation for the following reasons. First, they recognize an institution to be a social entity that can bring to bear both influence and power over other social entities. In the context of Section 404, the SEC has sanctions that it can use to modify actions of institutions such as within audit companies. These companies can sway client organizations' behaviors to ensure the system of internal controls is approved (Kurien et al., 2004).

King et al. (1994) suggest the need for power-based and influence-based implementation tactics. Power-based tactics change behaviors through the use of penalties. Influence-based tactics affect behavior through social processes such as negotiation and politics (Jasperson et al., 2002). Second, King et al.'s taxonomy acknowledges the social aspects of interventions, which involve recipients and implementers of the intervention. The interactions between the groups are dynamic and complex. In 404 interventions, there are several levels of implementers and recipients. At the highest level are institutions such as the U.S. Congress and the Public Company Accounting Oversight Board in the role of implementers and audit firms, and organizations as recipients. Within organizations, SOX program teams act as implementers and IS departments can act as implementers and/or recipients. Line managers are recipients because they need to change their working practices in response to the intervention. Third, King et al.'s framework distinguishes between 'supply-push' and 'demand-pull' interventions. Supply-push is characterized as a force arising from the production of a change. Demand-pull interventions emanate from users' willingness to use the product of the intervention. The taxonomy for 404 interventions is illustrated in Figure 1 based on King et al.'s original classification.

King et al.'s (1994) taxonomy describes IT intervention drivers that we have reinterpreted, in this study as Section 404 intervention 'drivers'. The six drivers are described briefly in Table 1.

RESEARCH METHODOLOGY AND CASE STUDY DATA

This study is based on an multi-case study approach (Yin, 1989) where the design allows researchers to take a more holistic view of phenomena (Eisenhardt, 1989b) and especially where the aim is to explore an area that has received little previous research attention (Benbasat, Goldstein, & Mead, 1987).

Organizations affected by 404 can be split into two broad categories: (1) listed companies—that is, those whose shares are traded on a U.S. stock exchange, that have to achieve clean 404 certification; and (2) audit firms that have to attest to internal controls. This study is based on two listed companies and one global audit firm. The three specific case study settings for this research

Figure 1. A taxonomy of intervention drivers

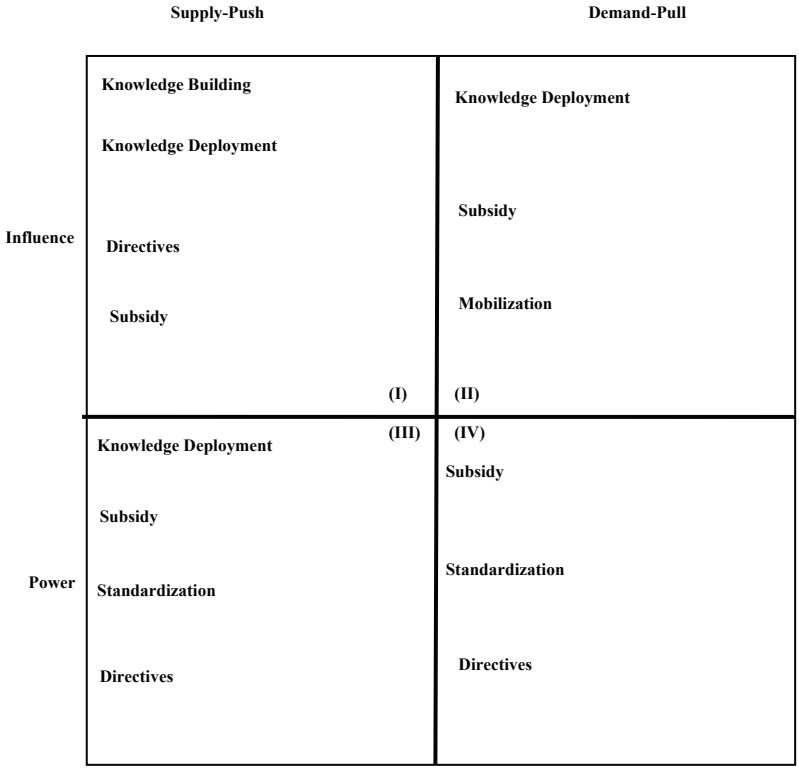

Table 1. A description of 404 intervention drivers (adapted from King et al., 1994)

Intervention Driver	Section 404 Context
Knowledge Building	Finding out about Section 404 and its requirements, e.g., research into internal controls
Knowledge Deployment	Making information about 404 available to people, e.g., through training courses
Subsidy	Covering the costs of 404 implementation through the provision of budgets and human resources
Mobilization	Promoting and publicizing 404 and its implications, e.g., through internal communications that endorse the benefits and making people aware of 404
Directives	Putting in place rules and procedures that people have to follow
Standardization	Setting standards that lead people to follow prescribed courses of action

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 404 requirements. The organizations had to have implemented 404 in a UK division in order to analyze the initial effects of their implementation tactics.

The primary sources of data were the Sarbanes Oxley program team and the IT division. The aim was to gather mostly qualitative and non-quantitative data (Blaikie, 2000). A variety of data-gathering techniques were used, including semi-structured interviews with key roles in 404 implementation (including the program director, IT director, IT manager, and finance manager) and internal documents such as written reports. Additional data was collected through informal discussions that were held both face-to-face and over the phone. The data gathering strategy was flexible as this study sought to find a representative and unbiased set of data (Orlikowski & 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 article. The research process involved interviews lasting about two to three hours each.

The Case of Alpha

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 the 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 404 covered its processes, significant business processes, and controls for documentation. Alpha's overall SOX program started in November 2004.

The Case of Beta

Beta is the UK consulting division of Omega Group, a large U.S.-based global professional services group with operations in over 25 countries. Omega started a formal SOX program in the U.S. first because American organizations had to be 404 compliant by the end of 2004, whereas overseas subsidiaries had to be compliant by 2005. Omega adopted a program management approach to SOX implementation.

The Case of Gamma

Gamma is a wholly owned subsidiary of Zeta. Zeta is a UK-based professional services firm registered with the PCAOB. Zeta is a global firm, and about 40 countries in which it operates, including the U.S. and UK, are influenced by SOX. Gamma offers a range of audit and non-audit services. 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 404 within IS services in Gamma.

ANALYSIS, SYNTHESIS, AND RESULTS

For each intervention driver, the findings are condensed into a theoretical proposition for 404 implementation.

Table 2. The case of alpha

Intervention Driver	Alpha
Knowledge Building	• Established a Central SOX program team with a program director and people from group accounts and internal audit • Conducted a pilot in the lending process with external auditors • Pilot study produced 404 documentation • Applied documents to test existing controls in the lending process • Central team and auditors used pilot findings to develop practical approaches to implement 404 • Did little knowledge building with external consultants • Relied on external auditors and PCAOB (Public Company Accounting Oversight Board) Web site • Program director and central team IT representative studied competitors' approaches to 404 implementation for information systems to remain consistent with competitors
Knowledge Deployment	• Created a central committee that included the group chief accountant, group internal audit, project managers, and the SOX program director • Created a standard Group Technology Division governance structure • Created a Project Control Committee (PCC) with representatives from relevant Group Technology Division departments and the committee rep • Central program team created a Web site on the intranet to store documents and templates • Appointed a representative to interface to each business division, with one rep dedicated to Group Technology Division • GROUP Technology Division appointed a program manager to take 404 implementation forward within the division
Subsidy	• Alpha covered the costs of supporting 12 significant committees including a central committee, which reported to the group finance director • Spending estimated to be several million dollars • Budgets created as implementation progressed • No budgets were refused or expenditure turned down
Mobilization	• Created a one-day seminar for heads of finance at divisional level and their staff • Seminar co-facilitated by SOX program director and an external audit partner • Seminars outcomes: create awareness of SOX and 404, alert senior managers to resources required for 404 implementation, and facilitate creation of implementation plan • Seminar attendees were individuals directly involved with SOX implementation • Organized forums by the larger global accountancy and audit firms to reconfirm their approach
Directives	• Central committee mandated each division to use agreed documentation • Central committee allowed divisions some flexibility to manage their teams according to that division's environment, but with certain minimum requirements to be achieved
Standardization	• Selected the COSO[1] framework as the overall entity level controls framework • Adopted a centralized approach towards both entity and activity level controls, including application and general IT controls • Group Technology Division and the central committee rep developed 404 compliance approach using GTD's existing Process Framework, documentation, and controls testing standards • Used COBIT[2] framework to model the approach • Undertook research to ensure COBIT met COSO framework requirements

continued on following page

Table 2. continued

Outcomes	• Discussed proposed methodology with external auditors • Auditors ratified Alpha's 404 compliance methodology as acceptable • PCC applied Group Technology Division's process framework on significant business cycles and controls to achieve 404 compliance within the division • Established templates to document processes and controls and attest documentation • Assessments showed that existing controls were adequate and already in place • Existing IT controls assessed as 404 compliant, including controls for the following GTD processes: change management; performance and capacity management; data back-up and recovery; security and continuity services; services operation and monitoring; incident management; user requirements; design, development, and testing of solutions • Developed an overarching process to manage GTD processes • One of the central team's overarching concerns was to ensure that Alpha was compliant in all respects, but was not going beyond 404's basic requirements

Table 3. The case of beta

Intervention Driver	**Beta**
Knowledge Building	• Omega appointed the U.S.-based Global Finance function as overall sponsor for SOX implementation • Omega monitored SOX legislation development through the various Congress and Senate approval stages and therefore accumulated knowledge of SOX and 404 • The Global Finance function developed documentation, e.g., templates to capture, on paper and in spreadsheets, 404 control procedures • Gathered information through the use of questionnaires covering, among other things, control objectives, control activities, and overall status • The questionnaires covered five business cycles, i.e., revenue, expenditure, company-level controls called 'Tone from the Top', treasury and payroll, and financial reporting • Beta and its IT department relied on the Global Finance function for information about SOX • Beta's IT and finance departments were responsible for completing the questionnaires
Knowledge Deployment	• U.S. global chief financial officer given responsibility for liaising between Global Finance and overseas subsidiaries • Beta's SOX program board comprises the UK CFO and CEO and included members of Omega's program board • Beta sent people from the U.S. to the UK; people from the UK were sent to Australia • Beta's IT department's supported Global Finance in ensuring the accuracy and validity of information contained in the documentation • Beta's IT department corrected controls so that they did not appear to be that inadequate or broken in the 404 documentation • Beta's IT department liaised with global IT for implementing 404 documentation within Beta • Beta IT had almost no direct contact with people in the UK business
Subsidy	• No precise value can be placed on costs, but they are estimated in terms of millions of dollars • Beta used internal resources, with 41 people from the IS department alone dedicated to 404 documentation • Twelve individuals were at the center of completing the SOX documentation • Costs were calculated as the implementation progressed, and IS and finance budgets increased accordingly

continued on following page

Table 3. continued

Mobilization	• Managers from Omega's finance department delivered presentations to explain SOX and 404 to Beta's management team and individuals working on SOX documentation • Managers from Beta's internal finance department made presentations to operational managers to explain the documentation they needed to complete • Operational managers had to complete prescribed templates, which were often the wrong version • Beta's finance department implemented procedures to ensure latest versions of templates were communicated
Directives	• Beta already had controls in place to cover levels of internal oversight, operations of the board, and delegation of power from board to subsidiary committees • Beta documented control narratives, internal control systems, and control objectives in prescribed templates • SOX implementers tested conclusions, monitored project completion, and assessed Beta's compliance based on the documentation produced • Beta's IT department played a key role in proving system compliance based on the control narratives in the documentation • IT expanded control narratives and led the definition of how Beta operated its internal controls
Standardization	• Omega's global IT function, based in the U.S., developed an assessment method for IT controls based on the COBIT framework • Global IT sent assessment method to Beta's IT department in the UK • Beta's IT department created templates (based on the assessment method) for documenting processes and controls, and shared these with other firms within Omega Group
Outcomes	• Beta conducted internal assessments of its documented controls • Beta's board concluded the organization had documented a robust system of internal controls and no new controls needed to be introduced in the SOX documentation • Individuals working on specific business cycles identified areas where Beta could enhance its documented controls • Aimed to achieve best practice and consistency across Beta's documented business cycles

Knowledge Building

All three cases created a central team to take responsibility for developing knowledge about SOX and its implementation in their organization. These teams focused on producing templates that could be used to assess and prove that controls were in place. Beta and Gamma's parent companies have their head offices based in the U.S., and these parent companies were involved with developing and monitoring this legislation while it was going through its various stages of approval. These cases had the opportunity to build up significant amounts of knowledge as a result. Alpha, on the other hand, being UK-based, had no involvement with SOX in its formative stages. Alpha had to rely on briefings from audit firms and the PCAOB Web site for information. It had to build its knowledge base about the documentation to be used for 404 certification from first principles. As the Alpha program director stated:

At the start of the program I got called into the group finance director's office and asked to lead the Sarbanes Oxley program. I had never heard of this before and thought 'what is this thing?'

Table 4. The case of gamma

Intervention Driver	Gamma
Knowledge Building	• Zeta's U.S.-based audit and legal partners accessed information directly from the PCAOB • A specific division within Zeta U.S.—The Professional Risk and Technical Quality Group—developed training material for subsidiary firms to use • Gamma appointed a UK steering and project team • Gamma's steering and project teams used much of Zeta's 404 compliance work
Knowledge Deployment	• Gamma established a steering group for SOX • Steering group chaired by senior partner and included people at regional compliance level, regional audit partners, internal legal council, and IT people • Steering group assumed overall responsibility for independent compliance and regulation, and defined the brief for 404 compliance • Zeta's Professional Risk and Technical Quality Group answered internal queries from member firms • Same group addressed public and client events, and wrote articles and instruction documents on SOX • Zeta coordinated internationally with member firms to develop one set of information • Developed repositories of SOX knowledge on the intranet which are accessible globally by those involved with 404 • Steering and project team meetings were held in London
Subsidy	• Moving people with 404 knowledge around the globe meant that there were significant amounts of travel and related costs • About 100 individuals with 404 knowledge and experience traveled from the U.S. to the UK for between 6 and 12 months as well as to other countries that lacked 404 knowledge • No overall 404 implementation budget, therefore no clarity of overall spending to achieve 404 compliance • Costs estimated to be in the region of $10 million; one system alone cost about $1 million • No expenditure was refused
Mobilization	• Use of written formal communication, regionalization, training, knowledge bases, links, changing methodologies, etc. aided 404 implementation • Regional representatives on steering groups communicated with each other to maintain regional level coordination
Directives	• U.S. created audit systems which were rolled out in the UK and other countries affected by SOX • Audit systems allowed for deviation from mandated practices in different countries due to variations in local audit practices and client relationships
Standardization	• Zeta developed standards for IT general controls which all subsidiaries had to follow strictly • Zeta produced standards for end user computing applications such as the use of spreadsheets which has to be followed • The firm used COBIT as the basis for setting IT control objectives
Outcomes	• Zeta, globally, and Gamma, in the UK, developed the capability to conduct SOX/404 audits • The organization developed consistent audit methods that could be applied globally

In addition to the central team, each organization created SOX implementation teams at subsidiary or local levels. These teams had to develop their own knowledge base, and this was done through a variety of tactics such as seminars and briefings. Knowledge building focused on the documentation to be produced for the central team. Alpha developed its documentation in the context of its lending process. The pilot was run by the central team and involved a small number of people from the group technology and the external auditors. It chose this process because it was complex:

We wanted to tackle the lending because we felt if we could do it for lending all the others would be easier. (Program Manager, Alpha)

Beta, on the other hand, had to complete lengthy questionnaires that were then sent back to the U.S. to be compiled. These questionnaires were filled in by the IT and finance functions on behalf of the business. In Gamma, a central department based in the U.S. developed documents and templates for the subsidiaries to use internally and with external clients. Local subsidiaries were not expected to develop their own knowledge base about 404 documentation.

What becomes apparent in all three cases is that this intervention driver was about finding out about the requirements of the PCAOB, and creating documents and templates that could be used to prove adequate controls were in place. Once the documentation—whether in the form of templates or questionnaires—was in place, these were completed by people in the finance function with support from IT managers. People managing the day-to-day business in these organizations had little or no involvement in building knowledge about 404, and the introduction of controls needed to ensure compliance. End users were not involved with documenting the controls that were being proposed by the central teams.

The above discussion leads to the first theoretical proposition.

Theoretical Proposition #1

Proposition 1a: *Knowledge building in the context of Section 404 is focused on documenting controls on paper rather than affecting practice.*

Proposition 1b: *Lack of end user involvement can limit the extent to which controls are actually used in practice*

Knowledge Deployment

The three case study organizations established committees and teams to oversee 404 implementation. This is exemplified by Alpha's Project Control Committee, Beta's Program Board, and Gamma's Steering Group (I) (the roman numerals refer to the four quadrants of Figure 1). Information about SOX was disseminated from the center to the subsidiaries through the committees and teams. The central teams pushed

knowledge about 404 from the center to subsidiaries using technology. They developed repositories on their intranets to store documents and templates created centrally (I). The repositories contained information about 404 and its requirements, presentation material, guidelines, templates, and roll-out plans. Only those directly involved with developing and completing 404 templates accessed the 404 intranet sites. The repositories were not promoted to people beyond the teams and committees involved with 404 implementation.

The SOX Web site was a powerful way of getting information to the finance people…We didn't tell the head of operations and his direct reports (about the central SOX repository) because they weren't completing the questionnaires. (Finance Manager, Beta)

The organization used face-to-face briefings and more personal communications media such as transferring people from one country to another for extended periods of time. However, these communications were to people directly involved with the implementation of 404 documentation. The aim of these communications was to create demand for 404 compliance within the finance and IT communities that were directly involved with completing 404 documentation (II). The extent to which the case study organizations stimulated demand for 404 controls from the end users was very limited (II).

The documentation and templates created by the central teams were mandatory. In other words, each division or subsidiary had to complete the documentation within strict timescales. The importance of the documentation was stressed in communications, yet subsidiaries did not necessarily provide the resources required to complete the documentation. The SOX program teams in each organization were working to the deadlines set in legislation and hence had to ensure timescales were adhered to.

We put together a list of divisions that were late. At first there was a great deal of resistance to publishing the list but then we sent the list to the CFO…none of the teams wanted to be seen as late…I'd get calls from directors asking if they were in the red zone ahead of the list going out. (Program Director, Alpha)

People didn't see the importance of sticking to deadlines. It (404 implementation) was not core business for people in finance and IT so 'why bother?' was an attitude we had to overcome. (IT Manager, Beta)

The organizations used the tactic of 'name and shame' to ensure knowledge was deployed and timescales adhered to (III).

The above discussion leads to the second theoretical proposition.

Theoretical Proposition #2

Proposition 2a: *Knowledge deployment tactics are used to create demand in implementer communities rather than end user communities.*

Proposition 2b: *Power-based tactics are used by implementers to 'push' Section 404 document completion to other implementers and stopped short of involving end user communities.*

Subsidy

Each case study organization subsidized the implementation of 404 documentation. The costs in all three cases ran into several million dollars. Subsidies were used to create demand by meeting the costs of maintaining committee and team members' time (II). The costs of people moving for extended periods of time between countries and associated living and other costs were all absorbed by the organization (II). From a supply-push perspective (III), subsidies were used to allow program and project team members to ensure 404 documentation was completed properly.

The message was 'pay what it takes to do the documentation'…I cannot recall a discussion about withholding funding related to 404 activities. (Global IT Director, Gamma)

No pressure was brought to bear to cap expenditure…we had to meet the quality standards to meet the requirements of (404). (Program Director, Alpha)

Subsidies were used to provide sufficient resources to push through the implementation of 404 documentation. Access to funding gave project teams the ability to influence decision makers who said they did not have sufficient resources to implement 404.

We got the message out—that if you hear 'we need it for next Tuesday' it has to be done by next Tuesday. So people get around to doing it when they can because they are stretched for resources. I was able to say—'you need resources then here's the budget to get some'. It changed their perception. (IT Manager, Beta)

The consistent message across all three organizations is that funding was not a problem. However, two of the organizations, Beta and Gamma, could not quantify the overall spending on 404 implementation. In these organizations, budgets were diffused across different finance and IT departments in different subsidiaries. As the finance manager at Beta put it: "We made up the costs as we went along…what we spent was funded." Alpha held budgets centrally which was controlled by the program director; however, many of the costs at divisional level were masked from the central view.

The above discussion leads to the third theoretical proposition.

Theoretical Proposition #3

Proposition 3a: *Creating high-quality Section 404 documentation is more important than the overall spending to achieve Section 404 implementation.*

Proposition 3b: *Budgets for Section 404 documentation are fragmented across finance and IT departments, but not end user operational departments.*

Directive

Each organization created a set of documentation that had to be completed. This documentation was created by the central teams, and subsidiary companies and divisions had no choice but to ensure the documentation was completed.

The 404 processes are mandatory…its top-down coming from the U.S. down to the subsidiaries. (Compliance Partner,[3] Gamma)

Our business in now becoming rules based…the extent to which judgment can be exercised is being removed. (Global IT Director, Gamma)

IT controls were also mandatory. IT operations such as password controls, managing access to systems for starters and leavers, and access violations are mandated by the central teams; further, documentation supporting these controls had to be completed.

Organizations used controls and processes that were already in place (I). For example, Beta had controls for issues such as the delegation of power from the board to subsidiary committees and the operations of the board. These were adopted in their current form. Alpha followed a similar approach:

We repackaged existing processes and controls as 404 processes and controls. (Program Manager, Alpha)

The top-down mandatory approaches adopted by these organizations suggest that implementers drove the completion of 404 documentation (I, III).

The extent to which demand pull was used was limited to the flexibility that project teams were allowed to meet local conditions (IV). For example, Gamma's audit systems allowed for some variations due to local country audit practices, and Alpha allowed divisions to manage teams to fit with that division's culture. In both cases, however, there were still a set of directives that had to be followed.

The above discussion leads to the fourth theoretical proposition.

Theoretical Proposition #4

Proposition 4a: *The completion of Section 404 documentation is made mandatory to be accomplished.*

Proposition 4b: *Organizations allow for local customization of Section 404 documentation to match local conditions*

Mobilization

Communications to raise awareness of SOX were carried out to a very narrow group of people: those directly involved in the Sarbanes Oxley program. According to one program 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. (Program Director, Alpha).

In another case, the direction of communications was top-down with little time for questions from users. The pressure was on getting 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)

These views suggest 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, especially as many of these are embedded in information systems, to be documented. The assumption underpinning this view is that, provided this documentation is in place for the external auditors to test, the board can claim a sound set of internal controls in the financial statements are in place and that the 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. (Program Director, Alpha)

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

When I raised the question, 'How should we do this process?', the reaction I got was 'Don't ask. That will only delay the implementation and delay getting a tick in the box…Get the documentation out of the way and then get back to business'. (IT Manager, Beta)

This finding is 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. Mobilization requires the use of influence over people who have to adopt procedures and change processes that are 404 compliant. Current

theory suggests that this requires the development of mutually shared assumptions and alignment with the prevailing rational arguments being made for 404 compliance in the organization (Robey & Markus, 1984). Yet there appears to be little effort being made to involve wider participation across the business. A common occurrence is the use of spreadsheets to handle figures to prepare reports. This can happen at many different organizational levels: a local office, country head office, and the global headquarters. 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 departments ought to be aware of 404, its implementation and implications.

The above discussion leads to the fifth theoretical proposition.

Theoretical Proposition #5

Proposition 5a: *Communications are limited to those directly involved in Section 404 implementation with little communications with end user communities.*

Proposition 5b: *End users have little or no knowledge of Section 404 and its impact on the day-to-day operations in the business.*

Proposition 5c: *Section 404 documentation is perceived as a box-ticking exercise which can limit its ability to prevent future financial scandals.*

Standard Setting

All the case study organizations used COSO and COBIT as the standards for setting their controls. SOX requires organizations to select and adopt a control framework. Many organizations have adopted the COSO framework for entity-level controls. However, COSO does not cover specific IT-related controls, and consequently, the IT Governance Institute published COBIT (1994), which is a set of standards that address operational and compliance control objectives that organizations can adopt. Within these broad frameworks, all three organizations developed their own assessment methods, templates, and control objectives (III). As stated earlier, the documentation that supported these standards was compulsory and had to be completed (III).

People (in subsidiaries) were told to document their processes using specific templates. They had to capture the controls. (IT Manager, Beta)

The effect of standardization was to centralize controls and processes. In Gamma, Zeta produced the standards centrally and then rolled them out across subsidiary firms. These firms attempted to push back the extent to which the center was "interfering with local operations," according to the compliance

partner. However, local subsidiaries had very limited room to negotiate.

Our ultimate sanction against a subsidiary firm is to withdraw the use of the brand…If you don't comply (with the standards) we will remove the brand.(Global IT Director)

The above discussion leads to the sixth theoretical proposition:

Theoretical Proposition #6

Proposition 6: I*mplementers use standards to drive the completion of Section 404 documentation.*

DISCUSSION

The common theme that emerges from these cases is that the introduction of Sarbanes Oxley, in general, and the requirements of Section 404, in particular, were limited to finance and IT departments. The rest of the business, namely end user departments, has a very small role to play, if involved at all in some instances. Each case organization used implementation tactics that involved supply-push from implementers using influence (I). Knowledge-building tactics included developing the legislation during its passage from inception through to approval into statute; dealings with the PCAOB, auditors, and legal council; workshops and seminars; and pilots. Virtually all the knowledge building focused on the documentation that needed to be completed so that the organization's external auditors could certify compliance. Each organization's central SOX team created forms and templates that showed, on paper, that controls were in place. Knowledge deployment involved the rollout of these forms and templates. The organizations established Web sites on their intranets to store and share documents and templates. The implementers agreed which of the extant controls could continue to be used, retagging these as being 404-compliant controls. This had the effect of cutting down on the amount of effort and gaining the support of people in subsidiaries and departments that already had controls in place that they perceived to be adequate. Subsidiaries were used extensively to build within and share knowledge between those directly involved with 404 implementation, exemplified by steering group, committee, project, and program teams.

The case organizations used demand-pull and influence tactics (II), and these too focused on those directly involved with 404 implementation. Central teams were usually the first to learn about 404, and they shared their knowledge with subsidiaries and divisions affected by 404 through workshops and electronic means. The direction of communication was top-down with little effort being made to create real demand. Individuals directly involved with 404 implementation were not encouraged to change or improve extant processes and controls. This approach tended to reduce the implementation of 404 to 'box ticking': to demonstrate that controls have been documented

with little regard to what was going on in the actual business. The overarching concern was to complete the documentation within the timescales set by the legislation itself. Communications about 404 implementation to people in end user operational communities were negligible. Nonetheless, organizations had to subsidize the tactics used such as flying people with knowledge of 404 requirements to different countries.

The use of supply-push and power tactics (III) is highly prevalent when achieving 404 implementation. Although the case study organizations used influence-based tactics, they resorted to power-based tactics to push through 404 implementation. The publication of names of executives and program directors who were behind schedule or below quality levels exerted significant force on those people to adhere to the timescales and quality targets set by central teams. Organizations took a top-down approach, making completion of documents and templates mandatory. Individual finance and IT departments in subsidiaries or divisions were given little leeway, with sanctions being made available for use by senior executives. Lack of resources could not be used as an excuse for failing 404 implementation. Implementers had access to funding as and when they needed it. This lever could be used to bring in resources from other parts of the group or from external sources such as contractors to ensure subsidiaries achieved the outcomes necessary.

The demand-pull and power tactics (IV) softened some of the supply-push/mandatory forces at work. Subsidiaries outside the U.S. needed to comply with local laws and customs. For example, the ways in which relationships with customers are managed in, say the UK, could not be made to change overnight, and hence, documenting controls that reflected new ways of dealing with customers simply set up the organization to fail. Therefore, variations from the global standards and directives were allowed to ensure subsidiary organizations agreed to complete 404 documentation. The ways in which teams, in individual subsidiaries or divisions, were managed during the completion of the documentation varied to take into account cultural characteristics between different parts of the same organization in the same country and between different countries.

The overarching detraction from the implementation of Section 404 is that the legislation calls for controls to be documented. The audit firms and the organizations that have to be 404 compliant have interpreted this to mean the mapping of processes and controls. This has generated huge amounts of paper as organizations produce details of controls. On paper, therefore, organizations appear to be meeting the requirements of 404. However, the extent to which the organizations actually work in accordance with the documented controls is questionable. The concern is that we may see the emergence of another Enron in spite of Section 404.

OUTCOMES OF 404 IMPLEMENTATION

We discern two major outcomes from the implementation of Section 404 of the Sarbanes Oxley Act. The first is that each organization fulfilled 404 certification requirements in the timescales stipulated by the act. The documentation and templates completed were sufficient for external auditors to ratify that, on paper at least, all material risks had adequate controls associated with them. Many organizations used their existing control regimes to form the large part of 404 controls. The organizations rarely identified the need to introduce a new control, which given the breadth and scope of a 404 implementation is surprising. We would expect organizations to identify a small number of new controls that could be introduced. However, this was, by and large, not the case.

The second outcome is that there is a very low expectation that behaviors of people will change with respect to risk and controls, at any level of the organization. The overwhelming feeling seems to be one of 'tick the boxes and get back to business as usual'. One interviewee, with experience of several large global organizations, said:

Executives are using 404 as a way of minimizing change rather than driving change through the organization. They don't want to tackle the really hard issue of changing behaviors towards how people manage risk. (Compliance Partner, Gamma)

This was reinforced by one program director:

We concluded that there was no need to change existing processes and controls…There was no need to change behaviors and attitudes. (Program Director, Alpha)

Arguably, without changes in behaviors and attitudes, it is quite difficult to see how 404 documentation can truly prevent another Enron. Organizations appear to be taking a rule-driven legalistic approach rather than dealing with deeper social relationships, inadequate operational processes, and poor 'real' IT governance (Weill & Ross, 2005). This is reflected in the recent academic literature which reinforces rule-driven approaches (Haworth & Pietron, 2006; Krishnan et al., 2005). Until organizations and academics seriously address these issues, the vast amount of time and resources spent on documenting 404 risks and controls may not result in effective compliance.

CONCLUSION

The research in this article presents a systematic analysis of three multinational organizations in relation to their compliance with Section 404 of the Sarbanes-Oxley Act. The importance of appropriate IS was determined in this respect where standards, procedures, and applications are critical for successful accountancy processes. A number of significant implementation drivers are reported that will reduce the potential for financial deficiencies. As a result,

it is believed the integration of institutional theory with observed practice provides valuable insights into meeting the challenges of SOX and subsequent IT governance.

REFERENCES

107th Congress of the United States of America. (2002). *The Sarbanes-Oxley Act of 2002.* HR3763, Washington, DC.

Aberdeen Group. (2005). *SOX compliance and automation.* Boston: Author.

Aguilera, R.V. & Jackson, G. (2003). The cross-national diversity of corporate governance: Dimensions and determinants. *Academy of Management Review, 28*(3), 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, 18*(2), 39–53.

Argyris, C. (1971). Management information systems: The challenge to rationality and emotionality. *Management Science, 17*(6), 275–292.

Avgerou, C. (2000). IT and organizational change: An institutionalist perspective. *Information Technology and People, 13*(4), 234–262.

Banham, R. (2003). Period of adjustment. *Journal of Accountancy, 195*(2), 43(6).

Barnhart, S., Marr, W., & Rosenstein, S. (1994). Firm performance and board composition: Some new evidence. *Managerial and Decision Economics, 15,* 329–340.

Beath, C.M. (1991). Supporting the information technology champion. *MIS Quarterly, 15*(3), 355–372.

Benbasat, I., Goldstein, D., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly, 11,* 369–386.

Berghel, H. (2005). The two sides of ROI: Return on investment vs. risk of incarceration. *Communications of the ACM, 48*(4), 15–20.

Berle, A., & Means, G. (1932). *The modern corporation and private property.* New York: Macmillan.

Cadbury, A. (1992). *The financial aspects of corporate governance.* Report of the Committee on the Financial Aspects of Corporate Governance, Gee and Co., London.

Coffee, J.C. Jr. (2005). Internal controls: The scarlet letter. *Corporate Governance Advisor, 13*(1), 1–6.

Chan, S. (2004). Sarbanes-Oxley: The IT dimension. *The Internal Auditor,* (February), 31–33.

Coe, M.J. (2005). Trust services: A better way to evaluate IT controls. *Journal of Accountancy,* (March), 69–75.

Blaikie, N. (2000). *Designing social research.* Oxford: Blackwell.

COBIT. (1994). *Control objectives for information and related technology.* Rolling Meadows, IL: 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. So-

cial transformation, and fall of a university budget category. *Administrative Science Quarterly, 33*(4), 562–587.

Crowston, K., & Myers, M.D. (2004). Information technology and the transformation of industries: Three research perspectives. *Journal of Strategic Information Systems, 13,* 5–28.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management,* (Winter), 77–85.

Daily, C.M., Dalton, D.R., & Canella, A.A. Jr. (2003). Corporate governance: Decades of dialogue and data. *Academy of Management Review, 28*(3), 371–382.

Dalton, D.R., & Dalton, C.M. (2005). Sarbanes-Oxley legislation and the private company: If not for marriage then certainly engagement. *Journal of Business Strategy, 26*(2), 7–8.

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, 46,* 13–26.

Dalton, D.R., Daily, C.M., Ellstrand, A.E., & Johnson, J.L. (1998). Meta-analytic reviews of board composition, leadership structure, and financial performance. *Strategic Management Journal, 19,* 269–290.

Dewing, I.P., & Russell. (2003). Post-Enron developments in UK audit and corporate governance regulation. *Journal of Financial Regulation and Compliance, 11*(4), 309–322.

DiMaggio, P.J., & Powell, W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160.

DiMaggio, P.J., & Powell, W.W. (1991). Introduction. In W.W. Powell & P.J. DiMaggio (Eds.), *The new institutionalism in organization analysis* (pp. 1–38). Chicago: University of Chicago Press.

Duffy, M.N. (2004). Section 404 opens a door. *Journal of Accountancy, 197,* 8.

Eisenhardt, K.M. (1989a). Agency theory: An assessment and review. *Academy of Management Review, 14,* 57–74.

Eisenhardt, K.M. (1989b). Building theories from case study research. *Academy of Management Review, 14*(4), 532–550.

Fama, E.F. (1980). Agency problems and the theory of the firm. *Journal of Political Economy, 88*(21), 288–307.

Fama, E.F., & Jensen, M.C. (1983). Separation of ownership and control. *Journal of Law and Economics, 26,* 301–325.

Ferrell, O.C. (2004). Business ethics and customer stakeholders. *Academy of Management Executive, 18*(2), 126–129.

Goodstein, J.D. (1994). Institutional pressures and strategic responsiveness: Employer involvement in work-family issues. *Academy of Management Journal, 37*(2), 350–382.

Greenwood, R., & Hinings, C.R. (1996). Understanding radical organizational change: Bringing together the old and new institutionalism. *Academy of Management Review, 21*(4), 1022–1054.

Hackney, R.A., Burn, J., & Salazar, A. (2004). Strategies for value creation in e-markets: Towards a framework for managing evolutionary change. *Journal*

of Strategic Information Systems, 13(3), 91–103.

Haworth, D., & Pietron, L.R. (2006). Sarbanes-Oxley: Achieving compliance by starting with ISO 17799. *Information Systems Management, 23*(1), 73–87.

Ivancevich, J.M., Duening, T.N., Gilbert, J.A., & Konopaske, R. (2003). Deterring white-collar crime. *Academy of Management Executive, 17*(2), 114–127.

Jasperson, J.S., Carte, T.A., Saunders, C.S., Butler, B.S., Croes, H.J.P., & Zheng, W. (2002). Review: Power and information technology research: A meta-triangulation review. *MIS Quarterly, 26*(4), 397–459.

Jensen, M.C. (1993). The modern industrial revolution, exit, and the failure of internal control systems. *Journal of Finance, 48,* 831–880.

Jepperson, R.L. (1991). Institutional effects, and institutionalism. In W.W. Powell & P.J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 143–163). Chicago: University of Chicago Press.

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, 5*(2), 139–169.

Kling, R., & Iacono, S. (1984). The control of information systems development after implementation. *Communications of the ACM, 27*(12), 1218–1226.

Knights, M., & Reed, K. (2004). UK PLC dealt Sarbox deadline. *Accountancy Age,* (3), 7–9.

Haworth, D., & Pietron, L.R. (2006). Sarbanes-Oxley: Achieving compliance by starting with ISO 17799. *Information Systems Management, 23*(1), 73–87.

Kurien, P., Rahman, W., & Purushottam. (2004). The case of re-examining IT effectiveness. *Journal of Business Strategy, 25*(2), 29–36.

Legare, T.L. (1995). Minimizing resistance to technological change. *Information Systems Management, 12*(4), 59.

Levine, H.G., & Rossmoore, D. (1994). Politics and the function of power in a case study of IT implementation. *Journal of Management Information Systems, 11*(3), 115–133.

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

Markus, M.L., & Benjamin, R.I. (1996). Change agentry—the next IS frontier. *MIS Quarterly, 20*(4), 385–407.

Mayer, A.F. (2003). Preparing for Basel II by optimizing Sarbanes-Oxley. *Journal of Bank Cost & Management Accounting, 16*(3), 27(7).

McFarlan, F.W., & McKenney, J.L. (1983). The information archipelago—governing the new world. *Harvard Business Review, 61*(4), 91–99.

McWhinney, W. (1992). *Paths of change: Strategic choices for organizations and society.* Newbury Park, CA: Sage.

Meyer, J.W., & Rowan, B. (1977). Institutional organizations: Formal structures as myth and ceremony. *American Journal of Sociology, 83,* 340–363.

Ooms-Piepers, M., & Degens, R.M.I. (2004). SOX 404 business en tool alignment. *Compact KPMG, 31*(4), 26–33.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review, 16*(1), 145–179.

Orlikowski, W.J., & Baroudi, J.J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1–28.

Pfeffer, J. (1981). *Power in organizations.* Marshfield, MA: Pitman.

Quall, J.C. (2004). Implementing Section 404: A practical approach to the Sarbanes-Oxley Act. *CPA Journal, 74*(8), 52.

Robey, D., & Markus, M.L. (1984). Rituals in information system design. *MIS Quarterly, 8*(1), 5–15.

Robey, D., & Boudreau, M.C. (1999). Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. *Information Systems Research, 10*(2), 167–185.

Rone, J., & Berman, A. (2004). Musing on post-Enron reforms. *Journal of Accounting, Auditing and Finance, 19*(3), 331–342.

Sabherwal, R., & King, W.R. (1992). Decision processes for developing strategic applications of information systems: A contingency approach. *Decision Sciences, 23*(4), 917–943.

Saunders, C.S. (1981). Management information systems, communications, and departmental power: An integrative model. *Academy of Management Review, 6*(3), 431–442.

Scott, W.R. (1987). The adolescence of institutional theory. *Administrative Science Quarterly, 32*(4), 493–511.

Suchman, M.C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20,* 571–610.

Swartz, N. (2003). The cost of Sarbanes-Oxley. *Information Management Journal, 37*(5), 8.

Teo, H.H., Wei, K.K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. *MIS Quarterly, 27*(1), 19–49.

Tractinsky, N., & Jarvenpaa, S.L. (1995). Information systems design decisions in a global versus domestic context. *MIS Quarterly, 19*(4), 507–534.

Weill, P., & Ross, J. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review, 46*(2), 26–34.

Yin, R.K. (1989). *Case study research: Design and methods* (revised ed.). Newbury Park, CA: Sage.

Zucker, L. (1987). Institutional theories of organization. *Annual Review of Sociology, 13,* 443–464.

ENDNOTES

1 COSO is the set of guidelines published by the Committee of Sponsoring Organizations of the Treadway Commission.

2 COBIT stands for Control Objectives for Information and related Technology. See *www.isaca.org* for further information.

3 A *compliance partner* is the partner responsible for the compliance line of business in Gamma.

Ashley Braganza is the Director of the Centre for Organisational Transformation and Director of nexus – The Knowledge Exchange at the Cranfield School of Management. He is the Chair of the British Academy of Management Special Interest Group in Transformation, Change and Development. He has authored three books and numerous papers. His publications appear in prestigious academic and practitioner journals such as Communications of the ACM, Communications of the AIS, Information Systems Journal, European Journal of Information Systems, Journal of Strategic Change, International Journal of Information Management, Integrated Manufacturing Systems, International Journal of Project Management, International Journal of Knowledge Management, *and* Knowledge and Process Management.

Ray Hackney is the chair in business systems within the Business School at Brunel University, UK. He has contributed extensively to research in the field with publications in numerous national and international conferences and journals. He has taught and examined on a number of Doctoral and MBA programmes including Manchester Business School and the Open University. He led the organising committee for the annual BIT and BITWorld Conference series and is a member of the Strategic Management Society and Association of Information Systems. Professor Hackney has served on the Board of the UK Academy for Information Systems since 1997 and was also the vice president research for IRMA (USA). He is currently an associate editor of the JGIM, JEUC, JLIM, ACITM, EJIS *and case editor for* IJIM. *His research interests are the strategic management of information systems within a variety of organisational context, with an increasing speciality in government sectors and has he has contributed to a number of EPSRC and European funded research projects. Professor Hackney was president of the Information Resource Management Association (IRMA) during 2001/2002 and is now an executive member of the Information Institute.*