SOX, compliance and power relationships: Tactics for the CIO

Ashley Braganza and Arnoud Franken
Cranfield School of Management
Bedford, UK

Chief Information Officers (CIOs) around the globe are being drawn into the implementation of Sarbanes Oxley (SOX) compliance. According to the Public Company Accounting Oversight Board (PCAOB) (www.pcaob-us.org) [1], 15,000 US companies, 1,200 non-US based companies and 1,423 accounting firms spread across 76 countries are affected by SOX. In particular, Section 404 (404), which deals with management's assessment of internal controls, affects CIOs and information technology (IT) departments (Berghel 2005). With the widespread use of technology, internal controls are either fully automated by being embedded within information systems, or combine automated and manual controls. 404 therefore corrals 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, such as ERP systems, but also local databases and personal spreadsheets developed and used on an ad hoc basis. Consequently, compliance and regulatory issues are something that CIOs need to understand, address and certainly not neglect (see inset box).

SOX and 404 focus the mind

Reports suggest that the costs of implementing 404 on for the average large US company is US$ 5.1 million in the first year and then a further US$ 3.7 million on an on-going basis (Maitland 2004). This cost appears to be very large considering that dollars spent deliver little tangible value to customers or, arguably, shareholders. However, Chief Executive and Chief Financial Officers face severe penalties - from US$1,000,000 or up to 10 years imprisonment to US$5,000,000 or up to 20 years imprisonment – if convicted of accounting and reporting violations. When compared with such potential penalties, the implementation costs pale significantly.

404 requires CIOs to work closely with CFOs, CEOs and Auditors. Auditors have to attest and report on management's assessment of the internal controls. This attestation is required to be in accordance with standards for attestation engagements issued by the PCAOB. At the very least, financial reporting processes have to be mapped and tested. This has to be done to a level that ensures consistent and accurate financial reports are provided to shareholders and potential investors. This requires some of the business analysis skills that many IS departments already have. However, it also requires audit and control skills typically found in finance departments. Thus, achieving 404 compliance requires CIOs to understand the nature of the relationships they have with the CFO, CEO and auditors and the tactics they can use, when working with these players, to implement 404.

NATURE OF RELATIONSHIPS

Working relationships between the senior-most officers in an organization are not neutral (Donovan 1988). Such relationships are characterised by a number of dimensions: authority, centralization, decision rights, participation in decision making, and politics. (Jasperson et al. 2002) refer to these dimensions as power. Power has to do with relationships between two or more actors in which the behaviors of one is affected by the behaviors of the other (Hall 1999). We use power relationships as the basis for our analysis because previous empirical research shows that CIOs have relatively little power in organizations (Lucas 1984).

We adapted Jasperson et al's power relationships taxonomy to differentiate between power and influence. Individuals exercising power impose their will or interests by use of force; whereas, influence occurs when an individual (A), in a relationship, frames others' choices in terms of outcomes or interests they (A) expect to achieve; however, the individual (in this instance A) cannot impose these outcomes and interests by force (Castells 1998). Power and influence can be used by individuals to 'Push' their outcomes and interests or to encourage and convince others to 'Pull' their outcomes and interests. In order to gain deeper insights into relationships, we created the FRIN framework (see Figure 1) which has two power relationships – **F**ormal and **R**adical – and two influence relationships – **I**nterpretive and **N**egotiated.

Insert Figure 1 about here

INSERT FIGURE 1 ABOUT HERE
Figure 1 The FRIN Framework.

Formal power relationships are based on the structural positions that individuals have in the organization hierarchy. Typically, individuals in these power relationships assume that there is a single, most appropriate set of goals to be achieved and that people strive towards these goals. Individuals that take actions to reach other goals or objectives are considered irrational. Such actions are assumed to be taken because people have incomplete information, and consequently, the focus turns to giving people more information and education. These power relationships are used to stimulate 'demand' for the interests and outcomes of those exercising power.

Radical power relationships are based on achieving objectives and goals that impact the wider institutional context. Power is assumed to exist separately to the organizational context and yet, affects the actions of individuals within the organization. Radical power relationships are aimed at contributing to the overthrow of wider societal and organizational structures. This power relationship is characterised by individuals using sheer force to impose their will. These power relationships are used to 'push' the outcomes and interests of those individuals who use this power.

Negotiated influence relationships are based on individuals' abilities to affect the behaviours of others who have different or potentially conflicting interests or who seek different outcomes. Individuals use dialogue and political processes, such as negotiation and compromise, to reconcile divergent interests and to bring others around to pursue their direction. This relationship assumes power to be an objective reality, which often takes the form of resources or control over resources. Individuals using this influence relationship use resources to 'push' their interests and the outcomes they want to see happen.

Interpretive influence relationships are based on individuals' controlling and constructing the shared assumptions and interpretations that prevail across the organization. Individuals influence others by controlling meaning and shaping perceptions through the use of symbolic activities, stories and metaphors, the introduction and use of language and rituals and new procedures. Outcomes and interests, in this type of relationship, are achieved by manipulating the organization's subjective reality instead of formal, hierarchical authority or control over resources. Individuals use Interpretive relationships to create 'demand' for the outcomes and interests they hold.

The FRIN Framework combines the ideas of power and influence with pull and push, thereby providing a lens through which to understand relationships between key players, the Chief Executive, CFO, CIO and Auditors, involved in 404 implementation. We conducted case study research of these relationships in six organizations. We used a survey instrument as the means of collecting data, so that we could compare data across the organizations. As relationships are bi-directional we asked respondents to describe the relationship from both directions. Given the sensitive nature of both SOX compliance and ability to identify specific individuals from each organization, we use the names of States / Provinces, based on each organization's home country of incorporation, as pseudonyms for the organization name.

INSIGHTS INTO CIO RELATIONSHIPS

Alabama – this organization is the UK subsidiary of a Fortune 250 US-based home building company whose shares are traded on the New York Stock Exchange.

Alabama's CIO has an Interpretive relationship in the direction of the CFO whereas the relationships is Negotiated in the opposite direction. They both use influence to change and adapt each others' behaviors to achieve 404 outcomes. The CFO's influence is directed at pushing 404 requirements on to the IT department; whereas the CIO seeks to create the environment for the Finance Department to understand IT. There is a pull-push dynamic which indicates that this pair has different outcomes in mind and that they using different influence mechanisms to pursue their respective outcomes. Alabama's CIO has no direct relationship with the CEO, which can be of concern especially where the CIO has a significant role to play in the implementation of 404. It implies, as well, that the CIO has access to the CEO via the CFO which gives the CFO a political edge over the CIO. The relationship between the CIO and the Auditor is based on a Negotiated relationship, which suggests that the CIO is getting the Auditor to accept the controls and activities that they have in place. The Auditor, on the other hand, is using force to push specific 404 requirements in the direction of Alabama's CIO. She/he is in a weaker position in terms of the CFO and Auditors, both of whom are likely to have direct and strong relationships with the CEO (see Figure 2 I).

Tuscany – this organization is a wholly owned UK subsidiary of one of the world's largest manufacturers and distributors of premium eyewear, incorporated in Italy with a 21 per cent stock listing on the New York Stock Exchange.

The CIO has a Negotiated relationship with the CFO which suggests that influence is being used to push the IT aspects of 404 towards the finance department. This is a symmetrical relationship as the CFO has a Negotiated relationship in the direction of the CIO. This has the potential for conflict as both the CIO and the CFO will tend to push their own interests and outcomes; neither seems to want to create conditions for encouraging demand for their 404 outcomes – this would require one or the other to adopt an Interpretive relationship. Instead, the CIO appears to have an Interpretive relationship with the CEO. This suggests that the CIO is providing the CEO with information that affects the underpinning assumptions in the organization. The Auditors have a Radical relationship with the CIO suggesting that they are able to regulate the activities of the functions and activities of the IT department. Section 404 gives Auditors significant powers in terms of checking the adequacy of internal systems controls (see Figure 2).

<u>*Insert Figure 2 about here*</u>

Surrey – this organization is a leading supply-chain management company for the home entertainment industry. It is wholly owned by a UK gaming and entertainment company whose stocks are quoted on the London Stock Exchange and NASDAQ.

The CIO had different relationships with the CFO and CEO but is faced with the same relationship from both these players. In relation to the CFO the CIO has a Negotiated relationship which suggests that Surrey's CIO uses resources such as knowledge of systems, IT personnel and budgets to ensure IT's outcomes are achieved. The CFO has a Formal relationship with the CIO, indicating that the CFO uses force where necessary to create demand for the outcomes sought by the Finance Department. The CEO has a Formal relationship with the CIO suggesting that power is used push the outcomes that the CEO wants. This suggests that Surrey's CIO is in a vulnerable position as power can be exercised in their direction but they can only use influence to achieve their outcomes. This position is exacerbated with the Auditors that are using influence to push the outcomes they want from the CIO (see Figure 2).

Alsace **–** is a waste management division of a global environmental services company, incorporated in France with stock listings in Paris and New York.

We see the same pattern of relationship between the CIO and CFO as Tuscany above. Both have Negotiated relationships. The CEO too has a Negotiated relationship with the CIO and vice versa. This suggests that these players are engaged in influencing one another to take on their outcomes. This can lead to potential conflict between the players where the outcomes are significantly different. Where these differences persist the CEO might well have to use Formal or even Radial power to bring about a unified direction. The CIO has a symmetrical Interpretive relationship with the Auditors. This shows that both are trying to influence each other into wanting to adopt their outcomes, which can be positive where these are the aligned (see Figure 2).

Texas – this organization is a UK subsidiary of a global leader in secure electronic payment technologies. The parent company, incorporated in the US, has a New York Stock Exchange listing. The CIO has an Interpretive relationship with the CFO; whereas the CFO has a Negotiated relationship with the CFO. This pattern is the same as Alabama above. Both use influence to achieve there outcomes. The CFO has a symmetrical Formal relationship with the CEO; whilst the CIO has no direct relationship with the CEO. This suggests that the CIO relies on the CFO to influence the CEO. The Auditors have no direct relationship with the CIO. Instead they have a direct relationship with the CFO, which again suggests that the CIO has to go through the CFO in order to achieve IT-related outcomes (see Figure 2).

Ontario – this organization is the UK division of a Canadian financial services company, listed on the Toronto and New York Stock Exchanges. Ontario provides insurance and wealth management products and services.

In this case we find relationships that are based only on the use of power. The relationship between the CIO and CFO is symmetrical and based on Formal power. This is the same for the relationship between the CEO and CFO. The CIO has no direct relationship with the CEO. Thus, it appears that each player is pushing for the outcomes that he / she wants to achieve using force to get their way. The use influence to persuade colleagues is not apparent. The CIO appears to be fairly isolated as the CFO is key to exercising any power or influence over the CEO. The CFO – Auditor relationship is Radical which suggests that both sides are using force to push their outcomes on to the other. This would lay the groundwork for an antagonistic relationship (see Figure 2).

EXPLORING TACTICS CIOs USE TO ADDRESS RELATIONSHIPS

We turn our attention to a discussion of the tactics CIOs use in each power relationship (King et al. 1994). We studied the tactics CIOs use when implementing 404 using Institutional theory as the conceptual lens (DiMaggio & Powell 1983;King et al. 1994;Robey & Boudreau 1999). There are six broad categories of tactics:

1. *Knowledge Building* – creating a knowledge base necessary to develop an innovation and its use.

2. *Knowledge Deployment* – disseminating knowledge and developing an understanding of knowledge among people.
3. *Innovation Directive* – actions that command an organisation to produce innovations and set out orders to use the innovation.
4. *Mobilization* – actions taken to persuade decentralised players and subsidiaries to use an innovation.
5. *Standardization* – agreements between organisational members that privilege and sustain certain course of action.
6. *Subsidies* – funding implementers' costs during innovation development and users' costs during deployment and use.

The tactics used vary depending on the type of relationship. We found that CIOs in:

- Formal power relationships use Subsidies, Standardization and Innovation Directives.
- Radical power relationships deploy Knowledge Deployment, Subsidies, Standardization and Innovation Directives
- Interpretive influence relationships use Knowledge Deployment, Subsidies and Mobilization
- Negotiated influence relationships use Knowledge Building, Knowledge Deployment, Subsidies and Innovation Directive

Where the same tactic is adopted in different relationships, the ways in which the tactic is deployed varies considerably. Figure 3 condenses our findings of the differences in the ways in which the tactics were used. It shows that in Negotiated relationships knowledge deployment can be enacted by creating a central repository of knowledge, making SOX documents available electronically, holding seminars and workshop and establishing internal SOX forums. Knowledge deployment, in Interpretive relationships, involves moving individuals between subsidiaries on secondment. The secondments can span a few weeks to up to six months. In another example, Radical relationships use innovation directive tactics to 'name and shame' subsidiaries and individuals who are not achieving SOX compliance or who fail to follow prescribed procedures and methods. The overall tone of communications is that of 'telling' people what needs to be done. The same tactic in Formal relationships is used encourage bottom-up implementation, involving people from different levels in the organization. The tone of communications is 'selling' the importance of complying with prescribed procedures and methods. Innovation directive tactics in Negotiated relationships take the form of guidelines and templates that people use and follow to ensure compliance.

<u>*Insert Figure 3 about here*</u>

CONCLUSIONS

CIOs play an increasingly vital role in achieving 404 and other forms of compliance. CIOs need to have an insight into the type of relationships they have each of the key players that are involved with compliance implementation. They have a range of tactics they can use to achieve the outcomes that they seek. However, the relationships CIOs have with the other players means that they will be using a range of tactics to achieve the outcomes they seek. These may or may not be in the best interests of the CIO and the IT department. Where the outcomes are aligned, we anticipate that a compliance implementation will go smoothly. However, where the outcomes are not aligned each player will use power and influence tactics based on the perceived type of relationships. CIOs need to understand how to use power-based implementation levers. These levers are directed at affecting behaviours through the use of sanctions and force. Influence levers are based on tactics that change behaviour through education and social processes. Our findings show that CIOs are often isolated from the CEO and Auditors, relying on the CFO for direction. We suggest CIOs need to widen their base of relationships and develop new internal power and influence relationships when implementing 404 compliance. In fact, we argue that these relationships will become essential capabilities for CIOs as they are likely to be brought into the executive management team and made accountable for the quality of the financial data processed by the information systems they manage; no CEO or CFO is going to take the fall alone because of bad data from the CIO.

Finally, one consequence of the globalization of technology and processes, exemplified by off-shoring, is that compliance and governance are becoming a global phenomenon. The FRIN framework has been developed in relation to implementation of SOX in organizations with parent companies in different countries. Arguably, the framework can be applied to other types of compliance initiatives that involve the use of power and influence for implementation.

References

Berghel, H. 2005, "The two sides of ROI: Return on investment vs. risk of incarceration", *Communications of the ACM*, vol. 48, no. 4, pp. 15-20.

Castells, M. A. 1998, "Rejoinder: On Power, Identities and Culture in the Network Society", *New Political Economy*, vol. 3, no. 3, pp. 473-483.

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.

Donovan, J. J. 1988, "Beyond Chief Information Officer to Network Manager", *Harvard Business Review*, vol. 66, no. 5, pp. 134-140.

Hall, R. H. 1999, *Organizations: Structures, Processes, and Outcomes*, 7th ed. edn, Prentice Hall, Upper Saddle River, NJ.

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 metatriangulation review", *MIS Quarterly*, vol. 26, no. 4, pp. 397-459.

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.

Lucas, H. C. J. 1984, "Organizational power and the Information Services Department", *Communications of the ACM*, vol. 27, no. 1, pp. 58-65.

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

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.

[1] The PCAOB's mission is to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports.