Communications of the Association for Information Systems

Volume 17 Article 32

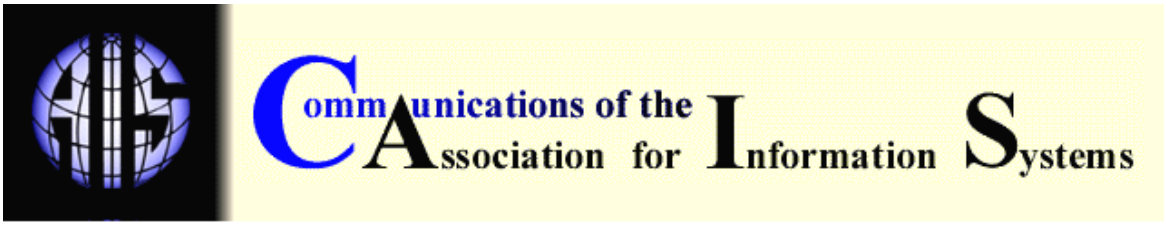
5-22-2006

Developments In Practice XXI: IT in the New World of Corporate Governance Reforms

Heather A. Smith
Queen's School of Business, Queen's University, hsmith@business.queensu.ca

James D. McKeen
Queen's School of Business, Queen's University, jmckeen@business.queensu.ca

Recommended Citation
Smith, Heather A. and McKeen, James D. (2006) "Developments In Practice XXI: IT in the New World of Corporate Governance Reforms," *Communications of the Association for Information Systems*: Vol. 17 , Article 32.
DOI: 10.17705/1CAIS.01732
Available at: https://aisel.aisnet.org/cais/vol17/iss1/32



DEVELOPMENTS IN PRACTICE XXI: IT IN THE NEW WORLD OF CORPORATE GOVERNANCE REFORMS

Heather. A. Smith
James D. McKeen
School of Business
Queens' University
hsmith@business.queensu.ca

ABSTRACT

In the past, IT was only marginally affected by regulatory matters. Today, however, IT is in the middle of a whirlwind of corporate governance reforms. New standards for internal controls are affecting almost every aspect of IT work. These, in turn, have significant implications on how IT is managed and on IT costs and productivity. For example, many IT organizations have been so involved in developing and implementing Sarbanes-Oxley (SOX) procedures that very little has actually been accomplished for the *business* itself.

This paper explores how new compliance frameworks and governance reforms, mandated by governments and/or industry groups, are changing IT work. It examines what IT managers perceive to be *most significant* issues these reforms present IT in their particular organizations. This paper is *not* designed to provide detailed information about IT controls and how to achieve them. Instead, it is intended to be a general introduction to the changing expectations of IT and how these are affecting IT work, structure and governance. It looks at the new effects regulatory issues are having in IT, and then examines the key issues IT managers face in an increasingly regulated environment. Next, it identifies the key areas within IT that are affected and the types of activities that need to be addressed by managers in order to achieve effective controls. Finally some recommended good practices are presented.

The authors conclude that there is no question that new laws and regulations governing organizations, their finances and their information are having a huge impact on IT. IT managers are struggling to implement new controls and document existing ones, while still ensuring business as usual and trying to develop the new systems their companies need. The world is requiring IT to become thoroughly professional about what it does. The IT of the future will therefore of necessity be increasingly controlled, standardized and bureaucratized. It remains to be seen whether or not management will be able to use this "new and improved" IT for competitive advantage.

Keywords: Compliance, corporate governance, Sarbanes-Oxley, privacy, IT regulation, COBIT, IT management

I. INTRODUCTION

Just when it seemed that IT could breathe a little easier after the craziness of the e-business "bubble" and Y2K, along comes the Sarbanes-Oxley Act (SOX). Designed to protect stockholders, employees and consumers from inaccurate or misleading financial reports, SOX became law in the United States in July 2002. It makes CEOs and CFOs explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal controls over financial reporting and disclosure. Any company trading in the United States is subject to these rules. (Subsequently, many other jurisdictions have prepared and are enacting similar legislation.) Along with new privacy laws enacted in the European Union, Canada and many U.S. states, specific industry controls (e.g., governing pharmaceuticals, certain manufacturing, chemicals etc.) and new, strict security measures to guard against terrorism, hacking, and illegal internet activities, *all* organizations are increasingly subject to a growing number of legal acts, regulations and ethical expectations that weren't even on corporate radar screens a few years ago.

In the past, IT has been only marginally affected by regulatory matters. Most organizations designed their record-keeping systems as they wished, and smart programmers enabled key inputs, such as tax rates, to be easily modified. Today, however, IT is in the middle of a whirlwind of corporate governance reforms. New standards for internal controls are affecting almost every aspect of IT work – from who is able to work on what, to IT processes, and how work is approved. These, in turn, have significant implications on how IT is managed and on IT costs and productivity. For example, many IT organizations have been so involved in developing and implementing SOX procedures that very little has actually been accomplished for the *business* itself.

To explore how new compliance frameworks and governance reforms, mandated by governments and/or industry groups, are changing IT work, the authors convened a focus group of senior IT managers from a variety of organizations. Participants were asked to prepare a presentation describing the *most significant* issues these reforms present IT in their particular organizations. Since this was a broad topic, participants were asked to concentrate on five general areas:

1. Regulatory acts affecting their organizations and their general implications for IT;
2. Their short-term IT impact;
3. Their impacts on IT processes, e.g., data access, security controls, change management routines, audit trails;
4. Impacts on IT structure and governance; and
5. The longer term impacts on IT, including how these impacts can best be minimized.

This paper is *not* designed to provide a detailed look at IT controls or how to achieve them, although it will direct readers to where they can find this information. Instead, the paper is intended to be a general introduction to the changing expectations of IT and how these are affecting IT work, structure and governance. The first section looks at the new effects regulatory issues are having in IT, and the second section examines the key issues IT managers face in an increasingly regulated environment. Section Three examines the key areas within IT that are affected and the types of activities that need to be addressed by managers in order to achieve effective controls. The final section describes some recommended good practices from the focus group that could assist IT managers in implementing appropriate controls.

II. IT AND REGULATORY LEGISLATION: WHAT'S NEW?

Many industries and organizations have long lived in a regulated or self-regulated world. For banks, insurance companies, pharmaceutical makers, hospitals and manufacturers (to name just a few), adhering to government legislation is simply a way of life. "Ninety percent of what we do is dictated by some law," stated a focus group member in one of these industries. "They tell us what we can or cannot do and where we are free to choose but must let regulators know." Increasing layers of regulation have been applied by governments over time and organizations have

gradually adapted to them. So why does it now seem that new control, privacy and security legislation is such a challenge for IT?

There are currently three major new aspects of regulation that are causing serious concern amongst IT managers:

1. **Extensive External Scrutiny.** In recent years, legislators and other regulatory bodies have become increasingly aware of the impact electronic information and systems can have on organizations and the public. Overnight, it seems, IT has had a huge effect on business practices (e.g., online business, offshore call centres). Systems provide the bulk of financial reporting data, can easily transport sensitive personal information across organizational and national boundaries, and produce inaccurate or invalid information that could mislead (either unwittingly or on purpose) auditors, tax officials, inspectors and members of the public. As a result of several recent corporate scandals where this occurred, there is a perceived need for improved controls over systems – how they operate and the information they produce (COBIT, 2000). "There's definitely a new attitude when we deal with regulatory agencies," said a group member. "In the past, there was more trust of the information we provided. Now it's 'show me how you got this.'" The concern with much recent legislation is that it is extremely wide-ranging, affecting almost every organization and industry. Furthermore, in some cases, the legislation has been passed hastily and therefore its implementation has not been properly thought through. Focus group members expressed concern that many new regulations did not make sense for companies, resulting in a great deal of work for no real benefit.
2. **Greater Difficulty Making System Changes.** The current crop of laws *is* more difficult for IT to adjust to internally. In the past, systems were developed after (or at the same time) as regulations affecting a business. Furthermore, these regulations affected smaller, often isolated, areas of work. Today's organizations typically already have significant amounts of automation. More recent legislation not only affects many different systems but also how they work together. Thus, it has a broader impact on work than previously – even beyond the organization itself. As well, organizations are not only more dependent on automated information and processes, but through networking, are also increasingly vulnerable to security threats. Interruptions therefore have a much larger ripple effect than in the past. Finally, systems are increasingly global in nature and are therefore affected by the laws of many different countries. Companies doing business with the European Union, for example, must respect strict EU privacy standards, even if their systems operate in the United States. Canadian and EU companies doing business in the U.S. must adhere to the Sarbanes-Oxley Act. In short, new legislation affects more systems and business practices than previously, and this makes it more difficult and expensive for IT to respond appropriately.
3. **Confusing Interpretations of Key Regulations.** SOX and privacy laws are considered the *most generically onerous* reforms affecting IT at present. But each member of the focus group was also facing other new, industry-specific legislation covering such varied issues as: impact on the environment, access to persons with disabilities, capital management, and homeland security. However, all agreed that *the single most challenging new regulation* is Section 404 of the Sarbanes-Oxley Act, which mandates an annual evaluation of internal controls and procedures for financial reporting. It requires that the CEO and CFO must personally certify these controls and that external auditors independently attest to their effectiveness (Damianides, 2005).

   In order for these controls to be considered effective, SOX requires that controls:

   - be suitably designed to achieve their objectives using established criteria;
   - be appropriately documented (internal focus group document, 2004).

To meet these requirements, the act strongly recommends that companies follow a framework for internal controls, known as COSO[1], originally developed in 1985. To assist IT in implementing this framework, in 1998, the IT Governance Institute developed its own Control Objectives for Information and related Technology (COBIT). Since COBIT is an open standard and is widely used, it is the primary IT control framework companies are using to provide the "reasonable assurances" required by SOX and as a foundation for meeting other regulatory requirements (see Appendix A for an general overview of these controls; more specific information should be obtained from the sponsoring organizations as their elements are continually evolving). In addition, there are a number of other more focused control models for IT, such as the Information Technology Control Guidelines[2] and the Security Handbook[3] to which companies are turning for specific guidance.

While frameworks provide a basic skeleton on which to build controls, the amount of control that is appropriate depends on the size and complexity of the organization involved (Fredericks and Tegethoff, 2005). At present, it is the job of a company's external auditors to determine if its controls are "reasonable." Unfortunately, in many cases, accounting firms' interpretation of internal controls is extremely strict, and auditors are performing massive reviews not tailored to a company's size or risks (Solomon and Gullapalli, 2005). This is leading to an increasing number of complaints from companies (Stewart, 2005; Powell, 2005). It is also driving IT managers crazy and forcing them to focus on "a minutiae of operational details" embedded in both their companies' information handling systems *and* in their own internal IT processes.

III. KEY ISSUES IN COPING WITH REGULATION IN IT

In the end, *all* regulations, frameworks and guidelines tend to land at least partially in IT's court to implement. "Different regulations affect our business units differently, but they *all* impact IT," said a focus group manager. "While the business has different teams for each set of regulations, everyone in IT is affected." As regulations become more numerous and complex, some of the focus group organizations are finding that *only* IT-based controls are effective in ensuring compliance. Because of the way it is being interpreted and implemented, SOX legislation is having the largest impact on IT at present. However, the IT management issues associated with this act are applicable to many other regulations. Focus group members identified a number of negative impacts of regulation and a few positive ones:

1. **Financial Costs.** There is no question that complying with the many new regulations imposed on organizations has led to significant IT costs. A recent survey of large U.S. companies found that they spent over $US5 billion in 2004 alone meeting SOX requirements and that $1 billion of this was in IT (Surn, 2004). The same study found that many firms had underestimated the costs involved, and a majority of those surveyed planned to increase their compliance budgets in the future. One CEO of an insurance company estimates that just addressing SOX will cost his firm $30 million per year (Stewart, 2005). Another study estimates large companies are spending about $35 million a year on SOX compliance, while the impact on smaller firms is proportionately greater (Powell, 2005).
2. **Productivity Costs.** Compliance clearly involves huge costs for IT. However, these involve much more than just money. New regulations generally mean that "IT takes an enormous

[1] Committee of Sponsoring Organizations of the Treadway Commision.

[2] From the Canadian Institute of Chartered Accountants

[3] From National Institute of Standards and Technology, United States.

productivity hit… It is a huge distraction and an enormous drain." (Koch, 2004). With SOX, for example, "all work on enhancements to systems had to be stopped for two months, while we were documenting our existing controls," according to a focus group member. The increased rigor required also adds to new project costs and lengthens their development schedule. "The business case payback is changing with SOX," said another manager. "Small projects are no longer cost effective, and manual processes are sometimes more attractive than automated ones."

3. **Training Costs.** Regulation affects everyone from the CIO to the most junior IT-staffer. CIOs must personally attest to the effectiveness of IT's internal controls and quality of information produced by systems. They must also ensure their function is able to provide the right information to both internal and external auditors and to their CEO and CFO. There are steep learning curves for every member of the organization (Leon, 2005). One focus group member stated, "an IT person has to understand the whole gamut of regulations. The learning curve tends to be all-consuming and takes a long time to build into the mindset of staff." In this organization (a highly regulated one), typically two weeks per year are devoted to training each staff member in compliance issues.

4. **New Skills.** Because of SOX's emphasis on documentation, the skills required of IT staff are also changing. "Written communication skills are becoming more important," explained a manager. This can be problematic because English is often not the first language of many technical staff, and editing is not a skill that has been valued in IT. "Documentation is the bane of our existence!" complained one focus group member. Keeping documentation up-to-date after it has been produced is essential as well. Many organizations are having to develop document retention strategies and knowledge bases of process and system documents. "In some cases, where regulations have been built into a legacy system, we are having major problems documenting what actually happens," said another manager. "The regulations are embedded and the developers have disappeared long ago." When combined with stiffer requirements for testing and quality assurance, the total cost of ownership for systems has increased dramatically after implementation.

5. **Duplication of Effort.** Two particularly challenging aspects of SOX and privacy legislation are the segregation of duties requirement and restrictions on who has access to data. The first requires that a person who makes a purchase or develops a system should not be the same person who accepts the purchase or the system. The second relates to who can view and change data. Both require substantial analysis of systems, personnel and data to identify who should be doing what.

6. **Morale.** Finally, there is a significant morale impact on IT staff. "People don't like all the shifting goals and they don't like oversight," said a focus group manager. Regulation has led to policies and procedures within IT that have "upped the bar" of what is expected of IT staff. It is important to watch out for "malicious compliance" (or work to rule) said another. If people simply mechanically follow processes, mistakes will be made. They must understand, and accept, *why* they are being asked to do this. At more senior levels, there is a danger that leaders will focus more on processes than on common sense (Stewart, 2005). Morale issues are often enhanced by frustration when staff cannot get the answers they need from their firm or external auditors. "In many cases, it's hard to find out what 'compliance' really means," said a manager. A common problem at all levels of IT is that because auditors don't truly understand how to interpret the legislation themselves, they are not able to provide clear guidance about what should be done (Koch, 2004). Often they err on the side of nitpickiness and are "overly cautious and mechanical" (Solomon and Gullapalli, 2005). The result is driving up costs out of fear and causing a massive waste of resources (Powell, 2005).

7. **A Strategic Opportunity.** On the other side of the ledger, there are some who see that an increased focus on controls for systems and information will eventually lead to benefits for the organization. “We can take either an opportunity or a fear mindset towards regulation,” said a manager. “There are many positive improvements we can make in our practices that will deliver benefits to the organization.” Companies that see compliance from a purely tactical perspective will likely not see the value of increased controls. If, however, they see regulation as a chance to streamline and revamp business processes and IT governance, some believe that compliance costs will eventually decline (Koch, 2004). Others even see compliance as strategic. “Companies need to redirect their focus from compliance as a necessary evil to compliance as a competitive advantage.” (Daimianides, 2005).

8. **Elevated Attention to IT Issues.** The recent spate of regulations, particularly SOX, has dramatically elevated board and executive attention on IT (although not necessarily in the way IT managers have been hoping for) (Damianides, 2005). They have also increased the relative importance of many elements of IT, such as security, quality, data architecture, and change management, which have previously been given short shrift by business people. Nevertheless, in most companies, controls are still seen as overheads. Focus group members stressed the need to put a positive “spin” on them. “We emphasize that improved controls and processes will lead to improved quality, simpler audits and easier learning curves for staff,” said one. Another noted that audits are an opportunity to “demonstrate how good we are.”

9. **A More Effective IT Organization.** Ideally, regulation should help organizations have the proper people, policies, and overall control structures in place to create an environment that ensures confidentiality, integrity and the availability of critical information (Fredericks and Tegethoff, 2005). Properly implemented, a strong internal control program ensures the following benefits, some of which IT has been trying to achieve for a long time (Damianides, 2005):

    - Improved overall IT governance,
    - Enhanced understanding of IT by senior executives,
    - Better business decisions based on more accurate information
    - Improved IT alignment with business
    - Reduced risk of system security breaches
    - Reduced difficulty complying with new regulations
    - More efficient and effective operations
    - An integrated approach to security
    - Enhanced risk management competencies.

Focus group managers all agreed on the costs of compliance but had mixed feelings about the benefits of new regulations on IT. All felt that IT had “room to improve” in certain areas in each of their organizations. “There’s always a need to find better ways to do our work,” stated one. However, while trying to look on the bright side in the long-term, most were feeling thoroughly overwhelmed by the new elements of IT they had to implement or upgrade and the new roles and responsibilities they had to take on to address immediate regulatory needs.

IV. ELEMENTS OF EFFECTIVE COMPLIANCE IN IT

The focus group identified five major areas of IT where managers should assess their compliance with regulations. These are:

1. Activities enabling IT work
2. Activities affecting new systems
3. Activities affecting information

4. Activities affecting daily operations
5. Controlling IT work

ACTIVITIES ENABLING IT WORK

These are the "basics" that IT must have in place in order to do the rest of its work.

- **Physical and Virtual Access.** Most organizations already have some physical and virtual access controls, but these now need to be extended to all office areas and buildings, work stations and company data and better integrated with each other. "We do this well in some areas, but in others changes can take weeks," admitted a group member. Procedures for granting and denying access need to be streamlined to dynamically and immediately enable new staff to be added, departing staff removed and role-based access provided (Smith and McKeen, 2005a).

- **Security Architecture.** Protection of systems and data is of rapidly escalating concern to organizations in our networked world. Today's hardware, software and data are more and more vulnerable to threats from both a sophisticated army of hackers, viruses, worms, and bots and from insiders (whether malicious or inadvertent) (Smith and McKeen, 2005b). To address this risk, organizations need a planned, integrated and evolving set of practices for dealing with these threats, rather than the patchwork approach that has developed in too many companies.

- **Business Continuity Planning and Disaster Recovery.** Organizations got wake-up calls in this area from the September 11 disaster and the 2003 blackout, and most have implemented improved plans and practices to address disasters affecting operations and data. New regulations require these plans to be tested, validated and kept up-to-date as new vulnerabilities are identified.

- **IT Governance.** Governance is the structure of relationships and processes that enable the enterprise to direct and control IT in order to achieve enterprise goals while balancing risk versus return (COBIT, 2000). In practice, this means the structure, roles, procedures and internal and external relationships that ensure that IT is well-managed and can provide the necessary information to run the organization. Whereas in the past, enterprise governance was supported by IT, today it is widely acknowledged that IT governance also has a strong influence over what the enterprise knows and is able to do (COBIT, 2000). Therefore, much more attention must be paid to ensuring IT governance is effective, both internally within IT and externally in collaboration with that of the organization.

- **HR Management and Training.** Along with new controls and needed capabilities come new roles and competencies to be filled and developed. A significant amount of compliance awareness training must also be developed and provided to all IT staff to ensure they truly understand the nature and importance of their responsibilities in this area.

- **IT Finance.** IT is a large and growing part of the enterprise's budget. Many SOX regulations around segregation of duties, risk assessment and quality affect how IT budgets are spent. IT managers must put processes in place to ensure that IT funds are spent wisely and are properly monitored.

ACTIVITIES AFFECTING NEW SYSTEMS

These address the work that is done to develop new applications or to acquire them.

- **IT Strategic Planning.** To ensure IT resources are effectively deployed, all new development must be mapped against business strategies (Damianides, 2005). While IT organizations have been trying to do this for several years, there are still many organizations where this is not being done or is being done badly, often because of the lack of a clearly articulated business strategy (Smith and McKeen, 2003a).

- **Risk Assessment.** Focus group members agreed that this is a major area where IT capabilities need improvement. Practices and procedures need to be put in place not only to identify the risks that need to be understood and mitigated in each IT project, but also to manage these on an ongoing basis throughout a project's life cycle.

- **Project Management.** Most IT organizations already recognize this as a key skill, but many do not have the procedures to properly monitor projects or to ensure that controls applying to new projects are effectively addressed. Attention also needs to be paid to adding appropriate control documentation in each phase of a project's development

ACTIVITIES AFFECTING INFORMATION

These elements address all data and information produced and/or stored by IT. However, since much of it comes from and is used by the business, this is a huge area of overlap with business controls.

- **Information Architecture.** Organizations have only just begun to address the huge amounts of data and information that exist in a wide variety of forms today. The number of paper documents, data, reports, web pages, and digital assets has literally grown exponentially in recent years, and very little has yet been done to control or organize it (Smith and McKeen, 20003b). Until companies know what information they have, how it is produced, who has access to it and how it is used, it is extremely difficult to control information access – a key requirement of much privacy legislation. "This is a huge culture shift for organizations," explained a focus group manager. "We have to develop data ownership awareness and recognition of the data owner's responsibilities." It is also a substantial analysis job.

- **Access to Data.** This is another area where most focus group members are experiencing problems. Because few have a complete information architecture and limited experience with information management, they are only just beginning to grapple with the issues involved in determining who in their organizations has and should have access to which data.

- **Document Retention.** New regulations and recent lawsuits are leading organizations to comprehensively address which documents and electronic information (e.g., email) are kept, where they are stored, and for what period of time. Different industries have different requirements in this area, but document retention is one area that most focus group members agreed needs to be better understood and more effectively, comprehensively and consistently managed. In some industries, said one manager, a requirement to produce for regulators *all* records (both paper and electronic) within days (or even hours) when requested is leading to the conclusion that retention practices alone are not enough and that there is a need for entirely new retrieval systems. Furthermore, regulations in many jurisdictions (e.g.,

British Columbia, Ireland) now require that data be stored within geographic borders, adding further complexity to this challenging issue.

ACTIVITIES AFFECTING DAILY OPERATIONS

These are the elements that run existing hardware, software and networks and ensure ongoing operations, as well as those that make needed changes and deal with problems as they occur.

- **Operations and Infrastructure Support.** Much work has been done in this area already by IT professionals, but some are better at ensuring high service levels and low costs than others. Operations staff need training in their regulatory responsibilities just as much as other IT staff, according to the focus group. Often, companies need to look more closely at how they identify and allocate costs in this area, what metrics are collected and reported, how third party services are managed, and how problems and incidents are addressed at the root cause.

- **Help Desk.** Help desks are the front line of business support. As such, they are often the first to identify problems and risks with systems, operations and information. At one focus group company, Help Desk staff must take 20 modules of training about the regulations applying to their work and how they are expected to respond to a wide variety of circumstances. Help desk training and documentation for each new system is also an essential control process and should be considered part of every new initiative.

- **Change Management.** Controlling how enhancements are made and implemented to existing systems has become extremely important to prevent major system disruptions. Processes to ensure the proper testing and validation of changes and integration with other operational systems create much extra work but can also save significant headaches. Segregation of duties is especially important to ensure that all control procedures have been properly followed.

CONTROLLING IT WORK

These are elements that ensure that all work done in IT is properly completed, meets all control standards, and can be demonstrated to do so with “reasonable assurance.”

- **Testing and Validation.** This is one of the most important areas of control. It is also one that is growing exponentially in cost, complexity and impact on the organization, stated the focus group. Ensuring that all IT outputs – systems, information, hardware, software and networks – are working as expected, meet established requirements and will not disrupt other parts of the business, is becoming fundamentally important to IT. Many organizations have now created a standard test environment and data sets to ensure this. As well, it is no longer possible for users to shirk their responsibilities in this area. Acceptance testing *must* now be completed by properly trained and qualified users who sign off on the accuracy of the results.

- **Documentation Management.** As noted earlier, documentation of *everything* is rapidly becoming a standard for IT. Processes that were once “understood” must now be written down and maintained as they evolve. Project documents and sign-offs must be retained and catalogued and different versions accessible by auditors. As a result, some IT organizations are creating new roles for librarians and document administrators.

- **Quality Assurance.** Finally, many companies also have an IT quality assurance group (sometimes external to IT, sometimes internal) that ensures compliance with all controls and corporate standards.

V. GOOD PRACTICES IN ENABLING IT COMPLIANCE

There are really no such things as "best" practices as yet in how IT copes with regulation. The legislation that is most disruptive to the majority of IT organizations (i.e., privacy and SOX) has only recently been passed. Like everything else in IT, as managers learn what works and what doesn't, practices will evolve. Expectations about IT will also change as auditors learn from their own experiences and legislation is amended or re-interpreted. However, we can still learn a great deal from those organizations (particularly in the banking and pharmaceutical industries) that have made significant progress in this area. Focus group members suggested five sets of practices will be helpful:

1. **Organize for Compliance.** Compliance cannot be something that is "tacked on" to an existing IT structure, stated the focus group. While different organizations will approach it differently, all agreed that compliance takes dedicated responsibility from a core group. Since it is an ongoing process, IT managers should recognize that after an initial "remediation phase," there will still be a considerable amount of work to do to reduce the ongoing costs of compliance, ensure procedures are followed, and of course, deal with new regulations. At the most senior level, many companies have SOX (or other) Steering Committees on which the CIO sits (Koch, 2004). CIOs also need to educate their Boards of Directors and Executive Committees about the changes and costs and opportunities of compliance (Damainides, 2005). To assist them in these matters and provide a consistent approach, many focus group companies now have Directors of Compliance within IT.

   Unfortunately, it has often been difficult for IT staff to get answers to compliance questions from either their own internal audit staff or their external auditors. Dedicated internal compliance staff can develop expertise that can be leveraged across all parts of IT. IT managers may also need to add other staff functions related to controlling IT work, e.g., quality assurance, creating and maintaining a standard test environment, and documentation management. Greater attention to security and information may also require the creation of dedicated staff groups with specialized expertise in these areas. Finally, there was strong consensus that while many IT development and support staff can be decentralized, IT compliance functions should be centralized.

2. **Use Standards and Frameworks.** There are several reasons to use these. First, there is no point trying to reinvent the wheel, agreed the focus group, when there are good, generally-accepted frameworks available. Already, organizations are converging around a number of key standards, such as COSO and COBIT and are mapping their existing control procedures against them (Fredericks and Tegethoff, 2005). This mapping can help identify gaps in current control procedures and a set of accepted practices against which to benchmark. Second, they provide critical success factors, tools, and key performance indicators that offer auditors "reasonable assurance" that controls are effective (COBIT, 2000). Third, external auditors are advising that control and compliance programs based on standards and frameworks are more likely to be deemed acceptable by regulators. Finally, they help to establish a common perspective between the external auditor and the organization, thus avoiding misunderstandings (Fredericks and Tegethoff, 2005).

3. **Emphasize Training and Awareness.** Training is essential to ensure that all staff understand their responsibilities in complying with regulations. "Compliance is everyone's

job," agreed the focus group. Training fosters a common sense of purpose, enables everyone to make better decisions and helps staff understand the implications of IT work for the organization as a whole. Employees who truly understand what controls are trying to achieve can sense the right ways to comply without going about it mechanistically. "People who are aware and informed, will be proactive and will be predisposed to ensure compliance every day in many small ways," stated one manager. Training should be geared to roles as well as creating general awareness. One highly-regulated organization has specific training programs for system and process owners, development, and help desk staff. "It's extremely important that people understand *why* we have the controls we do," stated the manager involved. "Becoming a compliant organization is a huge culture change, and it takes a long time to develop." Furthermore, since regulations, standards and strategies for addressing compliance are still in a constant state of flux, managers recommended developing a comprehensive general visibility and communications strategy around these matters.

4. **Ensure Appropriate Business Resources.** Business staff have an important role to play in IT compliance. From ensuring that business strategy is properly communicated so that IT strategy can support it, to taking ownership for systems and processes and being responsible for their outcomes and results, to knowledgeably signing off on key system development documents and test results, business staff must be actively involved in enabling IT staff to comply with regulations affecting their company. While in the past, IT staff have often "helped" in these areas (i.e., largely done it for them), today's controls require knowledgeable and qualified users who must be accountable for their own systems, information and decisions. While this increases overhead in the business areas, it is the only way that assurances about the effectiveness and efficiency of systems and the accuracy of information can be given.

5. ***Caveat Emptor* Regarding Compliance Technology.** The shortcomings of most IT organizations tend to revolve around gaps in policies, standards and documentation (Fredericks and Tegethoff, 2005). Thus, most of the challenges facing IT around compliance can *not* be solved by adding more technology. Compliance tools can help, but only after detailed analysis to understand what control elements are lacking and what is required (Leon, 2005). There is no shortage of tools on the market to help organizations become SOX compliant. Focus group members have found tools can be helpful in some key areas, such as in tracking, documenting and retaining evidence. In addition, they noted the value of a central repository for project documentation, where it could be retained as a living document as enhancements and changes are made. Interestingly, the focus group felt there were excellent tools available for development work that assisted them in achieving compliance. These are lacking, however, for enhancement work. Finally, they have also found tools which document work and information flows and connections between systems to be helpful.

In the future, the focus group foresees the need to assist the business with the automation of some of its compliance processes to save the time and expense of controls. However, they are proceeding cautiously in this area at present, as it is still unclear how control standards will evolve.

VI. CONCLUSION

There is no question that new laws and regulations governing organizations, their finances and their information are having a huge impact on IT. As enterprises become increasingly dependent on systems and electronic information, they become more vulnerable, and government legislation becomes necessary to protect the public. Unfortunately, the regulation is coming fast and furiously, and the pace is increasing. As a result, in many organizations, a significant amount of IT time and resources are being spent on the "overhead" of compliance. Almost every area of IT is

affected, and IT managers are struggling to implement new controls and document existing ones, while still ensuring business as usual and trying to develop the new systems their companies need. As with other "firsts" affecting IT, after an initial period of turbulence and uncertainty, managers are likely to get the situation under control with a combination of standards and frameworks, common sense, hard work and the judicious application of technology. But when the dust settles, it is highly unlikely that the fast and freewheeling world of IT of the past few decades will remain. The world is requiring IT to become thoroughly professional about what it does. The IT of the future will therefore of necessity be increasingly controlled, standardized and bureaucratized. It remains to be seen whether or not management will be able to use this "new and improved" IT for competitive advantage.

REFERENCES

Damianides, M. "Sarbanes-Oxley and IT governance: new guidance on IT control and compliance", *Information Systems Management,* Winter 2005, Vol. 22, No. 1, p. 77.

Fredericks, P and E. Tegethoff. "Compliance hindsight: what organizations have learned from early compliance approaches", *CIO*, April 6, 2005.

IT Governance Institute, *COBIT Executive Summary (third edition)*, July 2000.

Koch, C. "The Sarbox conspiracy", *CIO,* July 1, 2004.

Leon, M. "Hard-won lessons from the compliance front", *InfoWorld,* April 4, 2005, Vol. 27, No. 14, p.42.

Powell, S. "Seeking a cure for Sarbox", Barron's, May 2, 2005, Vol. 85, No. 18, p. 41.

Smith, H.A. and J. D. McKeen. "Developments in Practice XV: Information Delivery: IT's evolving role", *Communications of the Association of Information Systems,* Volume 16, Article 9, February 2005a.

Smith, H.A. and J.D. McKeen. "Strategic Information Risk Management", IT Management Forum, Volume 11, Number 1, School of Business, Queen's University, Kingston, Canada, K7L 3N6, 2005b.

Smith H.A. and J. D. McKeen, "Developing IT strategy for business value", IT Management Forum, Volume 13, 3, 2003a.

Smith, H. A. and J.D. McKeen. "New Developments in Practice VIII. Enterprise content management: what's your strategy?" *Communications of the Association of Information Systems,* Volume 12, Article 2, May 2003b.

Solomon, D and D. Gullapalli. "Moving the Market: auditors get Sarbanes-Oxley rebuke", *Wall Street Journal*, May 17 2005, p. C3.

Stewart, S. "Manulife chief lashes out at 'onerous governance'", *Globe and Mail,* May 6, 2005.

Surn, J. "The rising cost of compliance", *CIO,* August 15, 2004.

APPENDIX A

RECOMMENDED COBIT CONTROLS

(IT Governance Institute, 2000)

- Plan and Organize (IT Environment)
- IT strategic planning
- Information architecture
- Determine technological direction
- IT organization and relationships
- Manage the IT investment
- Communication of management aims and direction
- Management of human resources
- Compliance with external requirements
- Assessment of risks
- Manage projects
- Manage quality.
- Acquire and Implement (Program Development and Program Change)
- Identify automated solutions
- Acquire or develop application software
- Acquire technology infrastructure
- Manage changes
- Deliver and Support (Computer Operations and Access to Programs and Data)
- Define and manage service levels
- Manage third party services
- Manage performance and capacity
- Ensure continuous service
- Ensure systems security
- Identify and allocate costs
- Educate and train users
- Assist and advise customers
- Manage the configuration
- Manage problems and incidents
- Manage data
- Manage facilities
- Manage operations
- Monitor and Evaluate (IT Environment)
- Monitoring
- Adequacy of internal controls
- Independent assurance
- Internal audit

ABOUT THE AUTHORS

Heather A. Smith is Senior Research Associate with Queen's University School of Business, specializing in IT management issues. A former senior IT manager, she is a founder and co-director (with James McKeen) of the IT Management Forum, the CIO Brief, and the KM Forum, which facilitate inter-organizational learning among senior executives, and co-author (with James McKeen) of *Management Challenges in IS: Successful Strategies and Appropriate Action* (1996). She is also a Research Associate with the Lac Carling Conference on E-Government, the Society for Information Management, and Chair of the IT Excellence Awards University Advisory Council. Her research is published in a variety of journals and books including *CAIS, JITM, Information and Management, Database, CIO Canada,* and the *CIO Governments Review.* Her book, *Making*

IT Happen: Critical Issues in IT Management with James McKeen was published by Wiley in January 2003 and she is co-author of a new book, *Information Technology and Organizational Transformation: Solving the Management Puzzle* published by Butterworth-Heinemann.

James D. McKeen is Professor of MIS at the School of Business, Queen's University at Kingston, Canada and is the Director of The Monieson Centre – a research centre which studies knowledge-based organizations. He received his Ph.D. in Business Administration from the University of Minnesota. His research interests include IT strategy, user participation, the management of IT, and knowledge management in organizations. His research is published in a variety of journals including the *MIS Quarterly*, *JITM*, *CAIS*, the *Journal of Systems and Software*, *the International Journal of Management Reviews, Information & Management*, *CACM*, *Computers and Education*, *OMEGA*, *Canadian Journal of Administrative Sciences, JMIS*, *KM Review*, *JIST*, *KM Research and Practice* and *Database*. He currently serves on the Editorial Board of the Journal of End User and Organizational Computing and was the MIS area editor for the *Canadian Journal of Administrative Sciences* for seven years. Jim and Heather Smith's most recent book: *Making IT Happen: Critical Issues in IT Management* was published in January 2003 by Wiley.

.

Communications of the Association for Information Systems

ISSN: 1529-3181