

A Roadmap for Corporate Governance in Canada: How Process Automation Drives the Financial Reporting Control Framework

An MKS White Paper

A Roadmap for Corporate Governance in Canada: How IT Process Automation Drives the Financial Reporting Control Framework

Introduction

The US Security and Exchange Commission's Sarbanes-Oxley Act has heightened financial reporting standards for US public companies. Canada has followed suit with Bill 198 encompassing Multi-lateral Instrument MI 52-111: Reporting on Internal Control over Financial Reporting and Multi-lateral Instrument MI 52 109: Certification of Disclosure in Issuers Annual and Interim Filings.

Both Sarbanes-Oxley and Canada's Bill 198 require certification of internal controls over financial reporting. Included in the overall internal control framework are the internal controls as they relate to IT processes and technology. Since the vast majority of financial data within financial reports is generated by IT systems and their related processes, the effectiveness of IT processes and controls must be verified. Through defined and verifiable standards and procedures, CEOs and CFOs gain confidence that the financial information that they certify is derived from well-maintained and effectively controlled software applications.

With solid process automation and technology in place to enable compliance, business benefits beyond compliance can be achieved. In a recent study¹ done by the Information Technology Process Institute ("ITPI"), high-performing IT organizations tend to spend less time on compliance activities than their middle or low performing counterparts.

In another key finding, the ITPI survey identified a subset of controls used by the best-performing information-technology groups that were least observed by the mid-level-performing groups. The top half-dozen controls that separate the two groups are:

- Monitoring systems for unauthorized changes
- Having defined consequences for intentional unauthorized changes
- Using a formal process for configuration management
- Utilizing an automated process for configuration management
- Tracking the change success rate
- Maintaining complete and accurate information about infrastructure configurations

As demonstrated with the ITPI study, there are three key elements for any compliance effort within IT: the context of IT vis-à-vis the compliance legislation, methodologies or frameworks that enable IT compliance efforts and unify the compliance objectives across the organization, and the technological platform necessary to implement a compliance framework.

Compliance effort needs to be mapped across an organization beyond the Finance department and IT is the track that binds many areas together. The first section of this paper discusses the role that IT will play in complying with Canada's Bill 198. This paper examines the regulation from an IT perspective, and illustrates why IT is integral to key decisions about corporate governance.

The second portion of this paper describes three popular frameworks or methodologies that may be employed to establish internal controls to achieve compliance with either Sarbanes-Oxley or Bill 198. These methodologies or frameworks provide the roadmap to reach compliance – the final destination. The discussion of COSO, COBIT and maturity models illustrates the various approaches to process control and IT governance. These frameworks are discussed in descending order of specificity, meaning COSO is represented as the broadest approach to internal controls for financial reporting, while the

¹ Doug Bartholomew, *Better Controls Yield Better Performance*, August 28, 2006, [Baseline Magazine](#).

COBIT framework and maturity models are detailed methodologies used in the self-assessment and benchmarking of processes in IT.

Finally, this paper introduces MKS Integrity, an application lifecycle management platform that assists organizations to achieve reliable process control, satisfy many of the recommendations set out in COBIT and automate compliance in your organization. A unifying technological platform becomes the engine that drives compliance efforts across the organization. MKS Integrity performs requirements management and version control, ensures process compliance, provides audit trails, enables implementation of approval cycles and automates manual tasks to guarantee the reproducibility of software applications. Alone, the MKS platform will not guarantee compliance with Sarbanes-Oxley, Bill 198 or any other regulation, but satisfies prescribed IT controls and provides a disciplined and controlled IT governance model.

The Compliance Terrain: Bill 198

The intent of Bill 198, introduced by the Canadian Securities Administrators (CSA) is similar to the Sarbanes-Oxley legislation, specifically, Section 404. It requires that the management of public companies evaluate the effectiveness of internal controls over financial reporting. In Canada, unlike the United States, there is no requirement for an auditor to review and express an opinion on management's assessment of controls.

Like Sarbanes-Oxley, Bill 198 requires:

- A statement of management's responsibility for establishing and maintaining adequate internal controls over financial reporting
- Management's assessment of the effectiveness of internal control
- Disclosure of any material weakness of internal control over financial reporting

Due to the potential civil and criminal penalties involved, CIOs and IT executives should be concerned with their company's ability to satisfy IT controls, financial controls, and meet compliance objectives. CEOs and CFOs have a serious responsibility and will need to place an enormous amount of trust in the people and systems that produce their company's financial data.

The View From the Top

Given the potential penalties for non-compliance, CEOs and CFOs are taking ownership of the application of the Sarbanes-Oxley legislation and now, Bill 198. Organizations must monitor a tremendous amount of data to ensure accuracy of financial statements. IT is a fundamental organizational resource to collect, store and compile this data from all areas of the company and transmit it to the appropriate people.

It is interesting to note how CEOs and CFOs view these regulations from a compliance perspective. Surprisingly, an informal survey by CIO Magazine of the top 19 companies on the Fortune 100 list revealed that most executives in the US viewed compliance as a finance issue, not a systems issue². Rather than being seen as a critical component to meet compliance requirements successfully, IT is rarely acknowledged in its instrumental role. Examples of successful compliant organizations always include IT in the implementation of controls for financial reporting.

² Ben Worthen, *Playing by New Rules – Sarbanes-Oxley: Your Risks and Responsibilities*, May 15, 2003, [CIO Magazine](#)

With the later introduction of Canadian legislation, Canadian companies have had the advantage of observing their US counterparts as they struggled to meet compliance demands and to learn from their mistakes.

Getting IT on the Map: What Regulatory Compliance Means to IT Executives

Bill 198 provides longer-term benefit to organizations. At the senior management level, IT is a key player in regulatory compliance. According to CIO Magazine, CIOs must be proactive in getting the attention of their CFOs so that they understand how important IT systems are to data integrity. One way to do this is by demonstrating a detailed understanding of the regulatory requirements and the part IT can play in achieving compliance – without claiming that IT holds all the answers. Seats at the senior management table “are usually reserved for CIOs who can explain the business value of technology changes, but who are also able to put on their business hat and review potential IT work in the context of the broader business needs.”³

From a departmental perspective, be prepared for greater financial reporting scrutiny. This process depends heavily on internal software systems to generate and transmit the necessary financial data. IT processes, therefore, can be considered an “internal control” that must be audited to ensure compliance with the law and, equally important, that they are secure, comprehensive and repeatable. The benefits of such an audit extend beyond compliance with the law to the overall quality and reliability of your company’s systems. This, and imposing deadlines, should be incentive enough to start the auditing process now.

Compliance to regulations such as Bill 198 and Sarbanes-Oxley often provide the catalyst some organizations require to improve IT governance. Organizations that seek to automate IT control processes to realize compliance find that the effort pays dividends in terms of organizational efficiency, team productivity and bottom line savings. Too often process maturity initiatives are viewed by executives as ‘nice to have,’ and are prioritized lower in the context of other business needs. But when positioned as a pathway to compliance, process maturity and automation initiatives have a greater chance of approval and funding.

Leading global consulting firm Deloitte & Touche LLP agrees. In a presentation entitled “Sustained Compliance – the IT Imperative,” the firm is clear that companies must face the fact that compliance is a new state of normal in public companies, and that CIOs must move away from a “once and done” mentality to one of “sustained compliance.” A sustained compliance approach allows companies to navigate through a myriad of regulatory and legislative requirements, i.e. Basel II, FDA regulations, Environmental Health and Safety Regulations, HIPPA, Graham-Leach Bliley. According to Deloitte, the value and economic returns of automated processes for IT control actually increases the larger and more complex the business.

Once IT is integrated into an organization’s overall compliance initiative, there are several methodologies and tools to assist in providing a framework for standardizing processes and control and establishing auditing capabilities.

2. Creating a Roadmap for Compliance: IT Governance and Auditing

IT is pervasive in today’s business environment and plays a critical role in regulatory compliance. The IT sphere includes software and hardware, but more importantly, the processes that govern their use. There are some reputable, established methodologies and guidelines to bring IT processes under control and ready to be audited. ISO 9000 is a well-known generic management system standard concerned with how an organization goes about its work, and not directly the result of this work. This

³ *Playing by New Rules*, p. 6

standard can be applied to any organization, large or small, whatever its product or service in any sector of activity, including business, public administration, or government. If you consider financial reports as internal end products, then ISO standards can be helpful for achieving a high level of quality overall. There are specific frameworks and methodologies that address financial reporting or IT processes.

The three frameworks, or methodologies, discussed below are a good starting point for establishing financial reporting and IT process guidelines. COSO, as mentioned, is an approach for establishing internal controls over financial reporting. COBIT is an IT governance framework that can be applied to the entire IT realm and its processes in general, and maturity models represent a more detailed approach to controlling individual processes within the IT realm. While there are guidelines, there are no "one-size-fits-all" frameworks. The three methodologies are listed below in descending order of granularity specific to process control activities.

a) COSO – When speaking of corporate governance, COSO is the leading approach, especially after the US SEC's June 2003 announcement recognizing it as its preferred framework. COSO (The Committee of Sponsoring Organizations of the Treadway Commission) was established in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. The Commission was an independent private sector initiative, which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

COSO issued a groundbreaking report entitled *Internal Control – Integrated Framework* in 1992, which identified the establishment of internal controls as a means for helping a company achieve numerous objectives. The objectives include achieving its performance and profitability targets, preventing loss of resources and ensuring reliable financial reporting. The reason this report has become entwined with regulations such as Sarbanes-Oxley and Bill 198 is its assertion that internal controls help ensure that the company complies with laws and regulations, avoiding damage to its reputation and other consequences. Many companies used this report as the basis for their immediate response to these regulations.

In the summer of 2004, COSO released the most comprehensive update of its 1992 report. To date it incorporates and expands on the 1992 report to address Enterprise Wide Risk Management (EWRM). The new framework emphasizes the importance of identifying and managing risks across the enterprise. According to one expert organization that has seen advance copies of the framework, COSO's new ERM framework consists of eight components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. The three new components of the COSO framework are objective setting, event identification, and risk response. And the five taken from the control model are broader in their descriptions and in terms of the practical guidance.⁴

COSO and its findings are mentioned often in conjunction with regulations such as Sarbanes-Oxley because of the role COSO has played in establishing financial reporting controls, yet COSO remains only a guide for the entire organization and offers little about how IT organizations, in particular, can meet their unique challenges. The following frameworks represent the actual processes that IT organizations can use to establish effective internal controls in preparation for IT audits.

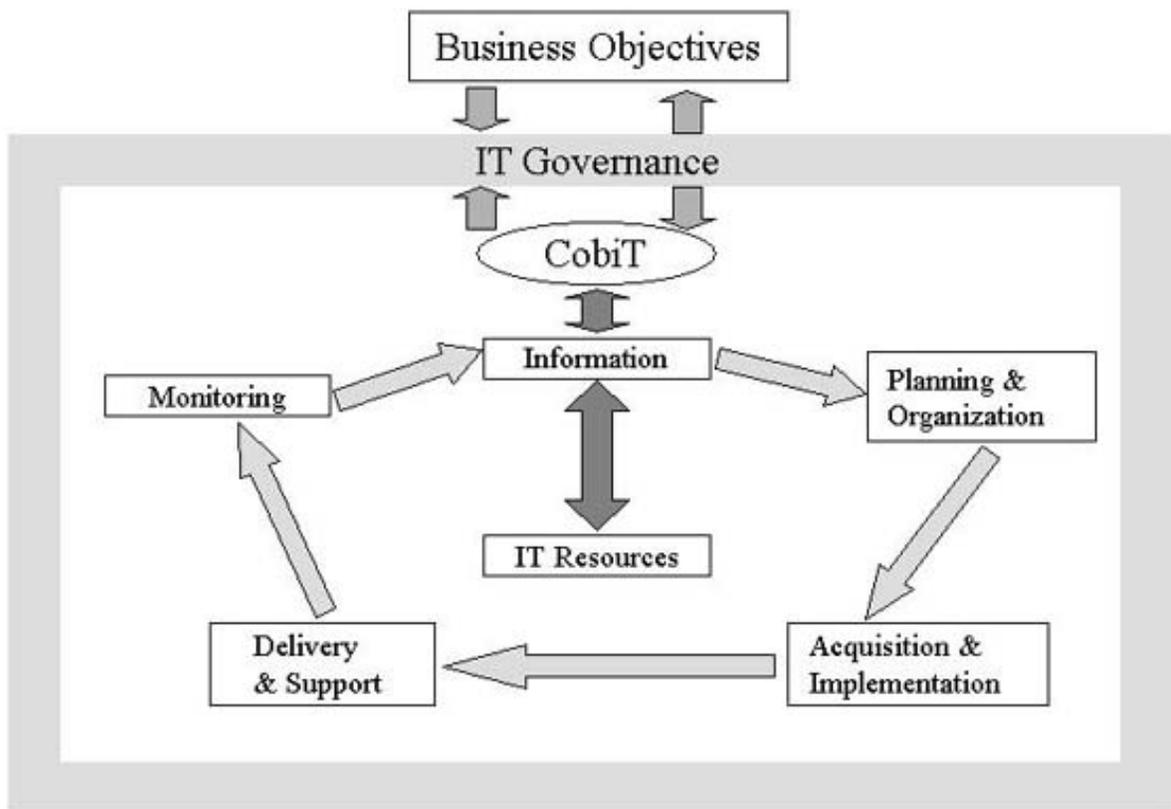
b) COBIT – COBIT (Control Objectives for Information and Related Technology) was developed by the IT Governance Institute as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners. The institute was founded in 1998 by the Information Systems

⁴ D'Arcangelo & Co.,LLP, Certified Public Accountants (D'Arcangelo Software Services website) http://www.darcangelosoftwareservices.com/media/inthenews/COSO_update.htm

Audit and Control Association (ISACA) as a not-for-profit organization dedicated to sharing better practices for IT governance.

According to COBIT, IT governance is a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes⁵. COBIT provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives.

COBIT's framework for IT governance identifies 34 key, naturally grouped IT *Control Objectives*, which fall under one of four broad domains: planning and organization (11), acquisition and implementation (6), delivery and support (13), and monitoring (4). Each control objective can be regarded as a separate process to which COBIT's *Management Guidelines* are applied. The management guidelines are governed by a generic maturity model that allows managers to map where the organization is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organization wants to be. The following section discusses maturity models, and in particular the Software Capability Maturity Model, as a means for controlling software development processes.



Source: ISACA-need year

⁵ COBIT 3rd Edition – Executive Summary, July 2000, p. 3.

COBIT represents an excellent reference point for improving IT governance, assessing current internal process controls and implementing new and improved ones. Such an IT governance model is a worthy long-term goal but to comply with the Act, more immediate and short term actions can and should be taken.

c) Maturity Models - Like any business process, IT processes lend themselves to auditing activities that track their effectiveness in achieving business goals. Key to this measurement is the use of maturity models for self-assessment and benchmarking. Maturity models are effective tools for determining the current status of the organization's processes and how they should evolve. They provide both the goals to strive for and the means of measuring the attainment of those goals. If you are planning to audit your IT processes, maturity models provide one of the readiest and effective tools for preparing for an audit. There are five levels that comprise the generic maturity model:



Generic maturity model levels – Source: Software Engineering Institute (year)

The Capability Maturity Model (CMMI)

To understand how maturity models are applied in business, consider the example of software development processes. For a number of years, software development organizations have used the Capability Maturity Model[®] Integration (CMMI[®]) as the de facto standard for assessing and improving software processes. Developed by the software community under the stewardship of the Software Engineering Institute (SEI) at Carnegie Mellon, it describes the principles and practices underlying software process maturity and is organized into the same five maturity levels as the generic model.

CMMI is a model to assess the engineering processes of an organization and to identify the practices required to increase the maturity of these processes. The CMMI describes the principles and best practices underlying a mature engineering process and is intended to help organizations improve their processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined processes. The CMMI is organized into five maturity levels:

1) Initial

The Initial maturity level is by default where organizations are when they start their journey towards process maturity improvement. The software process at this level is characterized as ad hoc, and occasionally even chaotic. Few processes are defined and success depends on individual effort and heroics. Often even the processes that are in place are ignored. This is not a level that is “achieved,” so it is not covered within the CMMI as the other levels are.

2) Repeatable

At maturity level 2, the repeatable level, basic management processes are established to plan and track project cost, schedule, risks and functionality. Quality auditing and traceability of requirements throughout the entire development lifecycle are also emphasized during this phase. The necessary process discipline is established to repeat earlier successes on projects with similar applications. There are seven maturity level 2 Practice Areas (PAs) and they form the basic foundation for all future improvement areas.

3) Defined

At maturity level 3, the processes for both management and engineering activities are documented, standardized, and integrated into a standard process for the organization. Each development lifecycle approved for use within the organization is documented. At maturity level 2 every major project or application group could conceivably use different processes as long as they were documented and used consistently within their own group. At level 3, however, the focus is on having an organizational standard, and all projects must follow the organizational standards or an approved, tailored version of those standards for developing and maintaining software. At level 3, the maturity level 2 compliant processes remain in place, with at least 11 more maturity level 3 PAs added for CMMI-SE/SW. Besides the focus on establishing organizational standard processes and repositories, the level 3 PAs also cover all of the engineering practices from requirements development through implementation, verification and validation, organizational training, managing process improvement at the organizational level and some advanced project management practices, e.g., risk management.

4) Managed

Organizations that achieve a CMMI maturity level beyond level 3 are considered highly mature. At maturity level 4 sophisticated measures of the process performance and product quality are collected and analyzed to stabilize and improve key processes and product quality. This level includes two PAs, but many companies utilize aspects of level 4 even if their goal is not to actually attain this level.

5) Optimizing

At maturity level 5, continuous process improvement becomes deeply embedded within the organization’s culture. As in level 4 a heavy reliance on measurement is used to identify what to improve through the implementation of innovative ideas and technologies, the results of which are also measured. There are three PAs at this level.

3. Driving Compliance Across the Enterprise With a Technology Engine: Using MKS for Process Automation and Auditing

A main goal of regulatory compliance is to improve companies’ internal control over financial reporting. Application Lifecycle Management (ALM) provides a cohesive platform to monitor the creation and maintenance of all software applications that support internal processes such as financial reporting. ALM provides control over IT processes to make them more verifiable and auditable, satisfying a number of control objectives set out in COBIT, including requirements management, software

configuration management, process management, and release management offering an effective way of controlling IT processes at a modest price. ALM was designed to provide assurance that a company's mission critical software applications and systems are not exposed to potential failure due to human error, staff turnover or sabotage. Through the evolution of organizational best practices, the ALM discipline has become better understood and applied with the emergence of a secondary but vital role. ALM captures, tracks, creates version control and reports on changes, ties request for changes to business requirements, shepherds and triggers approvals for that change and ultimately secures any process or system in an IT setting.

MKS Integrity can help you bring your IT processes under control, so they are ready for Sarbanes-Oxley and Bill 198. MKS Integrity can also play a role in realizing process maturity goals and in assessing and measuring the evolution and progress of your processes maturity efforts.

ALM Satisfies COBIT Control Objectives

The functions found in an ALM platform like MKS Integrity support or satisfy many of the control objectives set out in the COBIT framework. Here are the features that are supported:

1. Complete secure versioning & audit history of software process, policy and processes change
2. Developing a formal systems development methodology
3. Requirements management with user and IT approvals
4. Maintenance and versioning of project documentation
 - a. Systems requirement definition
5. System acquisition and change approach addressing:
 - a. Security risks
 - b. Data conversion
6. Ensuring separation of development from production activities
7. Process modeling and automation
8. Rigorous testing including use cases
9. Control over movement of applications by development personnel from test to production
 - a. Automated approval process ensuring management review and approval of IT solutions prior to implementation
10. Post implementation review of process for system modifications made in an emergency
11. Enforcement of formal policies and procedures that define system security
12. User account security parameters are in place and enforced

MKS Integrity Platform Components

To satisfy an IT auditor, organizations must be ready and able to answer the following three questions:

1. Do you have a process?
2. Is that process followed and non-circumventable?
3. Can you prove you follow the process?

MKS Integrity for ALM and its features enable IT organizations to answer the above questions with confidence. Through a range of feature sets that span the entire application lifecycle, MKS offers a cohesive, single platform to manage information throughout the organization. The single data repository holds the history of every software activity and change and is readily audited. Here is some additional detail about the MKS feature sets that enable compliance.

MKS Integrity for Process and Workflow

MKS Integrity creates flexible process and workflow management that allow an IT organization to automate manual processes through the implementation of configurable workflows. MKS maintains an audit trail of every change and/or action made by every person involved in a given process, from the initiator of change to the final approval, providing valuable details about “who’s done what and why”. The workflows are completely enforceable, meaning that a process cannot be subverted. Go/no-go gates are the mechanisms that provide managers with the ability to enforce workflows and decide when the process can proceed and when it must remain stopped until another person in the process completes his/her action. Finally, MKS Integrity comes with a graphical workflow modeler to make for easy graphical editing of workflows while providing a clear overall picture of the people and actions involved.

MKS Requirements

Within the same workflow engine, MKS has built-in capabilities for requirements management, allowing auditors to view within one system the initial business requirement associated and immutably linked to all downstream development, testing, deployment activities. The role played by each member of the team is clearly identified, along with the necessary approvals required at each stage in the process. Within this format, an IT auditor can quickly and easily track a change deployed to a production system directly back to reason the change was initiated in the first place.

MKS Source

MKS Source is a cross-platform software configuration management (SCM) solution that provides traditional SCM and version control functionality. It plays a central role in software development with its ability to version any type of file, guarantee the reproducibility of an application, and provide audit trails for illustrating migrations throughout the software development process.

MKS Source provides value for regulatory compliance through its versioning capabilities and its integration with MKS Integrity’s process and workflow. In a typical company, processes and workflows are defined and documented, and implemented, in that order. MKS Integrity allows you to implement and enforce those processes, while MKS Source performs the versioning of the process documents and the components together deliver a complete audit trail. Monitoring and managing change to systems and to processes is not a trivial task. As processes improve and evolve, process documents will undergo almost constant revision. In an audit, separation of duties and a clear audit trail must illustrate that IT processes are up to date and in synchronization with what is being practiced by staff. An audit trail of approvals is critical for demonstrating that internal controls are working properly.

MKS Deploy

Release management, the discipline that governs the hand off of software and system change to the production environment can be one of the thorniest areas for any IT department when it comes to compliance. Even the largest of organizations have lacked discipline and control in this area. Poor practices include allowing developers to directly promote change to production; insufficient or no audit trails surrounding deployments; lack of roll back or fail over in the event of production errors; and the ability to contravene manual deployment procedures. MKS Deploy provides server-based control over the deployment process, ensuring the deployment of change to production environments is both secure and risk is minimized. Coupled with MKS Integrity’s role based permission model, separation of duties can be clearly defined within the system, ensuring adherence to role specific approval policies.

4. Compliance: More than a destination

A disciplined approach to internal process controls and good IT governance are the keys to complying with Canada's Bill 198. The regulatory climate today calls on companies to identify the framework used by management to evaluate the effectiveness of their internal control and then to attest to the effectiveness of these controls in the year-end financial report. This paper discussed a framework, COSO, which can be used to establish internal control over financial reporting. COBIT and maturity models, such as the Capability Maturity Model for software, are IT governance frameworks aimed at establishing good IT governance practices and assessing and measuring the effectiveness of IT processes.

An ALM platform, such as MKS Integrity, supports your compliance efforts by recording, managing, enforcing and auditing the IT processes that form your internal control mechanisms, and beyond compliance can actually accelerate productivity, efficiency and visibility across your IT organization.

Legislation has become a catalyst for many organizations to speed up the journey that they were already on. Many leading companies are implementing frameworks, processes and unifying technology platforms as a matter of good business practice. Compliance is not just a destination that once achieved can be dismissed. Rather, compliance is a means to ensure ongoing, continuous processes that are disciplined and owned by senior management as an outcome of a well-run business with solid processes in place. With the proper frameworks and technology in place, rather than an encumbrance, compliance can be built seamlessly into mature business processes and become a business enabler.

About the Author:

Douglas M. Sawatzky
Chief Financial Officer

Douglas Sawatzky is Chief Financial Officer of MKS, responsible for leadership of all financial functions within the company. Doug joined MKS in October 2001, and previously held the positions of Corporate Controller and Vice President of Finance.

Prior to joining MKS, Doug held positions with United Rentals of Canada Inc., and ATS Automation Tooling Systems, Inc. Doug also spent one year in the Corporate Finance practice and five years in the assurance practice of KPMG.

Doug earned his CA Designation 1994, CBV Designation in 1998, holds a Bachelor of Mathematics from University of Waterloo.

Helpful Online Resources

The Committee of Sponsoring Organizations of the Treadway Committee (COSO) - <http://www.coso.org/>

The Information Systems Audit and Control Association & Foundation (ISACA) - <http://www.isaca.org>

IT Governance Portal – <http://www.itgovernance.org/>

Sarbanes-Oxley Information Center – <http://www.sarbanes-oxley.com>

United States Securities and Exchange Commission – <http://www.sec.gov/index.htm>

PWC's CFO Direct Network (Sarbanes-Oxley Info Center) – <http://www.cfodirect.com>

Carnegie Mellon SEI (SW-CMM) – <http://www.sei.cmu.edu/cmm/cmm.html>

KPMG's Audit Committee Institute – <http://www.kpmg.com/aci/gov.htm>

MKS Inc. – www.mks.com

References

¹ Doug Bartholomew, *Better Controls Yield Better Performance*, August 28, 2006, [Baseline Magazine](#).

[Committee of Sponsoring Organizations of the Treadway Commission \(COSO\)](#), *Internal Control – Integrated Framework, Volumes I & II*, American Institute of Certified Public Accountants (AICPA), 1992.

[Comrie, George R.](#), *Software Development is Risky Business – Is it Audit Ready?*, 2001, ISACA InfoByte - ISACA Website.

[International Organization for Standardization](#), *Demystifying ISO 9000 and ISO 14000*, ISO Website - <http://www.iso.ch/iso/en/iso9000-14000/tour/magical.html>

[Thomke, Stefan](#), *R&D Comes to Services: Bank of America's Pathbreaking Experiments*, Harvard Business Review, April, 2003.

[IT Governance Institute](#), *COBIT 3rd Edition – Executive Summary*, July, 2000.

[IT Governance Institute](#), *COBIT 3rd Edition – Management Guidelines*, July, 2000.

[KPMG](#), *Sarbanes-Oxley Section 404: Management Assessment of Internal Control and the Proposed Auditing Standards*, March 2003.

[MacSweeney, Greg](#), *Governance Falls Into CIO's Lap*, *Wall Street & Technology Online*, May 29, 2003.

[PriceWaterhouseCoopers](#), *Navigating the Sarbanes-Oxley Act of 2002 – Overview and Observations*, March, 2003.

[PriceWaterhouseCoopers](#), *The Sarbanes-Oxley Act of 2002: Strategies For Meeting New Internal Control Reporting Challenges*, 2002.

[Worthen, Ben](#), *Playing By New Rules – Sarbanes-Oxley: Your Risks and Responsibilities*, CIO Magazine, May 15, 2003.

Deloitte & Touche LLP, *Sustained Compliance – The IT Imperative*, Presentation, February 2, 2006