The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Laws and regulations affecting information management and frameworks for assessing compliance

David Luthy and Karen Forcht
College of Business, Utah State University, Logan, Utah, USA

Abstract

Purpose – This paper aims to consider a number of key laws and regulations that have implications for information management and internal control systems.

Design/methodology/approach – The paper is a discussion of the key laws and regulations. It also considers a number of frameworks that may be useful for assessing compliance with applicable laws and regulations.

Findings – Organizations worldwide are impacted by an increasing number of laws and regulations. Many of them have important implications for information management and internal control systems even though they may lack explicit references to information management. This is because information technology (IT) has become pervasive in modern organizations, and it is self evident that awareness of applicable laws and regulations, along with their potential impacts on information management systems, is critical for compliance.

Originality/value – The paper shows how the increasing number of laws and regulations impact on the information management functions of organizations in a variety of ways.

Keywords Information, Data security, Information management, Regulation, Laws

Paper type Research paper

Introduction

A growing number of laws and regulations have implications for information management and related internal control systems. Much legislative activity has occurred in the USA because of some unfortunate company failures and scandals where investors and other stakeholders suffered tremendous loss. The US Sarbanes-Oxley Act (SOX, 2002) is an example of legislation that resulted, in large part, from these failures and from perceived weaknesses in internal controls that may have prevented them. The operations of US companies, regardless of location, are subject to SOX making this legislation an important consideration worldwide. The global nature and interconnectedness of IT makes it important for organizations with international operations to understand the laws and regulations wherever they do business. For example, European Union data-protection legislation has implications for companies that have operations or customers in Europe even though the company may be based in Australia. In addition to the legal and regulatory requirements that force organizations to comply, a general desire to mitigate risk of loss worldwide may encourage organizations to implement legislative provisions so that they can remain competitive in their industries.

Information laws and regulations may impact information management and internal control systems in a number of ways. First, financial reporting requirements

Information Management & Computer Security
Vol. 14 No. 2, 2006
pp. 155-166

0968-5227
DOI 10.1108/09685220610655898

may be affected where internal control requirements apply to an organization as a whole, including any foreign operations. The need to comply with various reporting authorities becomes imperative. Second, trading relationships may be affected where information exchanges may contain information about individuals where privacy laws are applicable. This requires special attention when laws and regulations are not comparable between trading partners. Third, even though a law or a regulation may not mention information technology (IT) specifically that does not mean that there is no concern with regard to information management. Even though a law or a regulation may be neutral with regard to the technology used in business processes, there is general recognition that IT is pervasive in modern organizations. IT is the core vehicle for handling business processes, and the implication is clear that IT and related internal controls cannot be ignored. A final observation is that a narrow reading of specific laws and regulations may lead to the conclusion that some elements of IT controls are not included or applicable to a specific organization. For example, it may be interpreted that privacy and business continuity issues are not included in the provisions of SOX and do not apply because they are not mentioned specifically in the legislation. However, information management systems that do not consider all areas of risk faced by an organization may bear unacceptable risk that may lead to adverse consequences.

There is a clear need to understand the laws and regulations and any related impact on information management and internal control systems. Therefore, this paper outlines a significant US Law; the SOX (2002) and a global regulatory treaty; the Basel (2004) II Accord. They are presented as representative examples where there are significant impacts or implications for information management. The objective of this presentation is to provide a general understanding and appreciation for the actual and potential impacts of laws and regulations on the design and operation of information management systems.

Associated with laws and regulations is the need to assess compliance with their various provisions. This paper, therefore, outlines two frameworks that can be used to assess compliance. "Internal Control – Integrated Framework" (COSO, 1994) which is a general internal control framework and "Governance, Control and Audit for Information and Related Technology" (COBIT, 2000) which is more focused on information management. These two frameworks are presented as important representative examples of a number of frameworks related to various information management issues.

Laws and regulations

Sarbanes-Oxley Act of 2002

SOX was enacted in response to a number of high-profile scandals and failures where investors and other stakeholders suffered tremendous loss. SOX is concerned with the accuracy and reliability of financial statements and other issues related to financial reporting by public companies. The Public Company Accounting Oversight Board (PCAOB) was created by SOX to establish standards and conduct activities as specified by SOX. The intent is to mitigate the risk of loss associated with publicly held companies.

This legislation is neutral with regard to the use of IT in organizations. However, it is generally recognized that IT is pervasive in modern organizations, and it follows

that a well-controlled IT environment is essential for reliable financial reporting. Therefore, IT controls are a significant element for assessment under SOX as specified by the PCAOB.

The focus of SOX on financial reporting means that there may be some areas of concern for information management that are not specific to financial reporting. For example, risks associated with privacy and business continuity may not be assessed for strict SOX compliance. Therefore, a more comprehensive assessment than specified by SOX may be indicated when considering all aspects of information management. The following briefly describes the provisions of SOX that relate to information management and related internal controls.

Internal control standards (sections 103 and 802). SOX and the PCAOB have specified standards for internal controls that encompass IT including the internal control structure, procedures, and records. Imbedded in the design provisions specified by the PCAOB is a requirement concerning the recording and retention of transaction records. This requirement relates directly to information management and the way in which transaction records are captured, maintained, and retained. The intent of this requirement is to ensure that information processes result in financial statements that are prepared in accordance with generally accepted accounting principles.

The use of external auditors as IT auditors (section 201). SOX requires that a company's external auditors be independent of the company's they audit. This precludes auditors from performing non-audit services for an audit client except in very limited circumstances. Specific mention is made of services related to the design and implementation of information systems. These have been significant activities of many public accounting firms. Also, the practice of outsourcing IT audits to their external auditors is precluded in instances where companies do not wish to employ their own IT auditors.

The role of audit committee members relative to IT (section 301). SOX establishes certain rules that concern the audit committees of publicly held companies and the independence of their members. Similar to the provisions related to the independence of external auditors, members of audit committees are precluded from receiving fees for consulting or advisory services. This includes IT services. SOX specifies that audit committees are to establish procedures for receiving, retaining, and treating complaints concerning questionable matters. This refers to what are otherwise known as "whistle-blower" complaints. Such complaints may arise from issues related to IT controls or from issues that involve the information management function itself. Regardless, requirements regarding whistle-blower complaints present important issues for data capture, retention, and reporting.

Internal control design and operation (section 302 and 404). Chief executive officers and chief financial officers are required by SOX to certify that they are responsible for establishing and maintaining the company's internal controls. This is arguably the most important provision of SOX for information management. Top management must certify that they have evaluated the company's system of internal controls. They must report publicly on their evaluation of internal controls and any post-evaluation changes that could have a significant affect on internal controls. This report covers all IT controls including such items as data protection, access controls, program logic, and related change controls. This report must disclose significant deficiencies in the design and operation of the internal control system that could adversely affect the recording,

processing, summarizing, and reporting of financial data. This report must also disclose any fraud, whether or not material, that involves employees or member of management who have a significant role in the operation of internal controls.

The PCAOB requires that the assessment of the effectiveness of a company's internal controls be based on a control framework that is recognized and established by a body of experts after having been reviewed and revised in a process that invited comment from interested parties. The PCAOB goes on to suggest that "Internal Control – Integrated Framework" (COSO, 1994) is a suitable framework for purposes of management's assessment along with other suitable frameworks that the PCAOB does not mention by name. Widespread usage of the COSO framework (Coe, 2005) and its specific mention by the PCAOB are reasons why it is outlined in the assessment frameworks section of this paper.

Movement toward continuous monitoring/reporting (section 409). The current information disclosure system for most public companies subject to SOX is built around "periodic" rather than "continuous" reporting of information useful for external stakeholders. Periodic reporting is consistent with the use of manual and older methods of data processing to compile and publish financial information. However, many believe that current IT provides the opportunity to report almost continuously. The requirements of SOX move companies in the direction of continuous reporting. For example, companies are required to disclose certain pieces of information on a "rapid and current" basis. That is, the number of triggering events has risen from 12 to 22 types under SOX for disclosing information within a shortened four-business-day period. Continuous reporting has significant implications for information management.

Basel II Accord of 2004

The Basel II Accord is the most recent formal development in a process that began with the 1988 Basel Committee (Basel I). The original agreement specified that banks must have enough money held in reserve to cover potential losses from banking transactions. Like SOX, the intent of the Basel accords is intended to mitigate the risk of loss in the financial industry.

Basel I established rules for calculating a risk-weighted amount below which a bank's total capital should never fall. Over time, it has been recognized that in a modern financial world of interconnected and complex IT systems risk has a number of dimensions. As a result, Basel II specifies a measurement and reporting system that incorporates a number of different types of risks where the use of information management systems is an essential component for compliance. In addition to the impact on data collection, information processing, audit trail, and database management requirements, Basel II impacts IT systems with regard to security, fraud, system failure, and service delivery. Related areas such as business disruption, employment practices, and legal factors are also affected. Although focused on the banking industry, there are indications that many of the requirements of Basel II may eventually extend to all financial institutions.

At the heart of Basel II is the development of an integrated risk management approach that supports both internal control functions and regulatory requirements. The typical situation with banks (and businesses in general) is that the issuance of financial reports and the filing of regulatory reports have been primarily accounting functions, and IT systems have been designed, primarily, to facilitate transaction

processing and external reporting. Because of this historical focus, many risk management systems, and other types of internal decision-support systems, have not been fully integrated with historical transaction processing and reporting systems. However, for Basel II compliance, risk management systems must be enhanced and integrated with the reporting system. For example, the automatic availability of information about collateral that is used in support of loans has not been a requirement for all banks. However, requirements under Basel II indicate that not only information about collateral but also information about risks associated with collateral must be developed, maintained, and made readily available. Such requirements have a direct impact on information management systems.

There are two general information management issues that are central to Basel II's focus on integrating risk management and regulatory reporting. First, the definition and calculation of certain components of risk requires integration and coordination of components of information management systems that have been separately maintained by many banks. Second, the collection and maintenance of various types of historical data over multiple years in support of risk measurement and reporting requires that databases be properly designed and maintained. These issues are discussed below in more detail in connection with various components of risk.

Components of risk. Basel II specifies multiple types of risks that must be calculated as the basis for determining a bank's minimum capital requirements. The most important types of risk, from an information management view, are credit risk, market risk, and operational risk. *Credit risk* is the risk that a loan will not be repaid. Traditional accounting information systems have considered credit risk and related bad debt expense for many years. Even though credit risk requires considerable attention there are established tools for dealing with it. Therefore, from an information management view, traditional methods for dealing with credit risk, except for its integration into the bank's total risk management system, may be sufficient for Basel II.

Market risk is associated with a banks investment decisions and the fluctuations of financial markets in response to changing economic conditions. Various types of banking assets may be affected by market risk. As with credit risk, market risk continues to be an important consideration for management. Also, information requirements and decision tools to manage market risk are not particularly new to information management systems, and there are established tools to deal with it.

Operational risk concerns any loss that could have been prevented had there been internal controls in place to prevent the loss. For example, operational risk relates to losses ranging from forged checks to ATM machine failures. Operational risk is an area that may require considerable new attention to comply with Basel II because of rapid advances in the use of IT in the financial world where there is already such high reliance on IT.

Operational risk is a key aspect of one of the most important elements of Basel II called the advanced management approach (AMA). The AMA allows banks to develop their own methodology, within guidelines, for controlling and calculating operational risk. This methodology and calculation are subject to audit and regulatory oversight. A benefit to the bank is that an investment in information management and controls that reduces operational risk results in the bank having a lower capital requirement. Another benefit that should be expected when information management is enhanced

is that bank operations will improve and information will be available for better decision making.

Basic provisions of AMA include the following elements. The first element specifies that senior management be involved and that the bank have an enterprise-wide risk management system including processes, policies, and procedures. Sufficient resources must be provided to manage operational risk, and the bank must have an operational risk function that is responsible for various items such as:

- designing and implementing methodology, policies, procedures, and controls;
- developing ways to identify, measure, monitor and control operational risks within a cost-benefit framework; and
- designing and implementing an operational risk reporting system that includes loss experiences.

As indicated, the elements of the operational risk must be integrated with the bank's overall risk management processes and must be reviewed regularly by internal and external auditors.

The requirements for risk calculations make it is clear that there is a heightened need for information management systems that provide both quality and quantity risk management data over multiple periods from both internal and external sources of data. In addition, the system must be capable of developing information to assess low-frequency but high-impact risk events such as terrorist attacks. If a bank does not have enough of its own information, it must acquire data from external providers. There is an expectation that external data and expert opinion will be used for scenario analysis to evaluate and control against high-impact risk events.

Database considerations. Several provisions of Basel II require special consideration for the design and maintenance of databases. In addition to traditional transaction data, a bank's database must capture and maintain both performance data and internal loss data. For example, data about system failures and incidents must be maintained. Internal loss data must be maintained from three to five years depending on circumstances, and internal loss data must be linked to current business activities. This means that the database management system must be designed to accommodate various types of data and various data sources in addition to traditional transaction data types and sources. Also, retention of data for use in risk assessment presents an additional dimension for database design and maintenance. Where traditional transaction data are maintained for specified periodic reporting cycles, other types of data such as loss data must be maintained for extended periods of time. These requirements for capturing and maintaining data may not be consistent with traditional transaction cycles and may require special consideration for information management systems. For example, Basel II has disclosure requirements that go beyond the traditional financial disclosure of banks. Policies, objectives, and strategies for each area of risk are examples of additional required disclosures.

Frameworks for assessing compliance with laws and regulations

Laws and regulations typically carry with them requirements for assessment of compliance. However, specific requirements concerning information management and internal controls are not typically included. Rather, published standards or

frameworks are used against which compliance can be measured. For example, SOX, as implemented by the PCAOB, requires companies to select and implement an internal control framework suitable to their organization. The PCAOB refers to a framework for internal control titled "Internal Control – Integrated Framework" known as COSO (1994) because of its sponsoring organization. Because of SOX's prominence as a piece of legislation impacting information management and because of COSO's general acceptance and widespread use in connection with SOX (Coe, 2005), COSO is outlined in this paper.

Another framework known as COBIT that is titled "Governance, Control and Audit for Information and Related Technology" (IT Governance Institute of the Information Systems Audit and Control Association, 2000) is also outlined in this paper because of its widespread use (Coe, 2005) and because it is complimentary to COSO with regard to information management issues. Finally, there are other frameworks that could be considered for use in organizations. The two frameworks outlined in this paper are considered sufficient to be illustrative of information management issues from both organization-governance and IT-governance views.

The COSO framework

The target audience for COSO includes the directors and management of organizations. Helping these people better control the entities they manage is a main objective of COSO. A general definition of internal control is provided by COSO that is sufficiently comprehensive so that it can serve many different types of organizations. A description of the major components of internal control is also provided. These components provide criteria against which internal control systems, including information management systems, can be evaluated and improved. COSO discusses what internal controls can and cannot do. The roles and responsibilities that should be assumed by boards of directors, management, internal auditors, and others are outlined. Finally, a set of evaluation tools are provided that may be useful for assessing and improving internal control systems in organizations.

The COSO definition of internal control reflects the fundamental concept that internal control is a process and not an end in itself. Internal control is affected by people at every level in an organization. Reasonable assurance, not absolute assurance, should be the expectation for internal control relative to the cost of controls and how intensively they are implemented. Finally, internal controls should reflect an organization's objectives related to effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.

The COSO framework views internal control as having five interrelated components:

(1) the control environment that comprises the ethical values, integrity, and the individual attributes of the people in the organization;

(2) risk assessment that is an awareness of the risks that an organization faces and the mechanisms used by the organization to identify, analyze, and manage those risks;

(3) control activities including policies and procedures that are necessary to address the risks that the organization faces and to achieve the objectives of the organization;

(4) information and communication of information needed to manage the organization and control its activities; and

(5) monitoring of internal processes and the environment so that the organization can adapt to changing conditions.

A system of internal controls is considered to be effective if all of these components are present and functioning appropriately.

COSO is published in two volumes. Volume 1 is mainly a discussion of the COSO framework that is outlined above from an organization-wide view. Volume 2 consists of an inventory of evaluation tools associated with specific objectives of internal control and its components as they relate to the components of the COSO framework. The discussion in Volume 2 is at two levels. The first level deals with the interactions of an organization with its external parties such as vendors, customers, and investors. The second level deals with an organization's internal value chain and infrastructure activities. At each level, the control objectives for each activity are stated. The risks that relate to that objective are then outlined. Finally, control activities are suggested that might lessen the stated risks and achieve the stated control objectives. Information management controls are relevant at each level described in Volume 2. The following contains an excerpt from each of the two levels of evaluation tools.

Components of the COSO framework

- Control environment.
- Risk assessment.
- Control activities.
- Information and communication.
- Monitoring.

Examples of COSO evaluation tools

Example 1 – Inbound activities.

Activity. Manage logistics.

Objective. Ensure that materials received and related information are processed and promptly made available to production, stores or other departments.

Risk. Information on materials received is not entered into the information system accurately or on a timely basis.

Control activity. Maintain procedures for promptly updating inventory records.

Example 2 – administrative activities

Activity. Manage IT.

Objective. Capture, process and maintain information completely and accurately and provide it to the appropriate people to enable them to carry out their responsibilities.

Risk. Data files are subjected to unauthorized access.

Control activity. Establish a security policy stating senior management's commitment on information security; demonstrate such commitment through appropriate actions.

(Committee of Sponsoring Organizations of the Treadway Commission (1994). *Internal Control – Integrated Framework*, Evaluation Tools Volume, p. 57 and 93.)

These excerpts were selected for presentation in this paper because they relate to information management controls at each level and are representative of the level of specificity contained in COSO for information management.

It seems clear from the examples given above that the level of specificity of IT control activities described in COSO is relatively general. More detailed and specific IT control activities are not specified in COSO. For example, COSO does not contain a listing of common data input edit checks that might be used during the capture of data. In contrast, it will be observed that the COBIT framework provides guidance at a more detailed level than the COSO framework. This suggests that guidance from more than one framework may be useful, if not necessary, as organizations consider compliance issues.

The COBIT framework

The target audience for COBIT consists of the management of organizations, users of IT services, and auditors; including IT auditors. The importance of IT in organizations is recognized where IT has become an integral part of an organization's strategy rather than being simply an information provider. The role of IT in organizations is explained. That is, enterprise governance drives and sets IT governance and IT objectives. The necessity of aligning IT governance and objectives with enterprise governance and objectives is emphasized. It follows that organizational objectives should foster appropriate use of IT resources as well as responsible management of IT-related risks.

With the foregoing as a backdrop to the COBIT framework, the IT Governance Institute makes it very clear that COBIT is a model of IT governance, not organization governance. COBIT is not intended to be either a model of general business control or a model focused only on specific IT control activities. Rather, COBIT is intended to bridge between the two ends of a control continuum running from general management issues to very specific control activities. This becomes clear as we compare the COSO and COBIT frameworks. In any event, it should be remembered that the discussion of the COBIT framework that follows relates to IT in organizations, not organization-wide governance.

The COBIT framework can be visualized as having three dimensions: IT processes, IT resources, and information criteria. IT processes include domains (discussed in more detail below), processes, and activities. IT resources include people, application systems, technology, facilities, and data. Information criteria include the overriding concerns of quality, fiduciary, and security along with the following attributes of information: effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability.

Each of the dimensions of the COBIT framework is incorporated, for IT control purposes, within four domains (high-level classifications) of IT processes. These domains include the IT processes of:

(1) planning and organizing;

(2) acquisition and implementation;

(3) delivery and support; and

(4) monitoring.

Each domain has a set of high-level control objectives (34 intotal) that relate to an IT process. For example, within the "deliver and support" domain one of the high-level control objectives is "ensure systems security." Each high-level control objective is

then mapped against the "Information Criteria" and "IT Resources" associated with them to indicate:

- the degree that control measures will satisfy different information criteria; and
- the degree to which control measures impact IT resources.

For example, "ensure systems security" has the following mapping to information criteria.

- efficiency (could be applicable);
- effectiveness (could be applicable);
- confidentiality (directly impacts);
- integrity (directly impacts);
- availability (indirectly impacts);
- compliance (indirectly impacts); and
- reliability (indirectly impacts).

This mapping for IT resources indicates that control measures are applicable to all IT resources.

The COBIT high-level control objectives discussed above are further subdivided into detailed control objectives that are suitable for a number of IT-related purposes such as control design, organization management, and system auditing. Detailed control objectives are comprehensive in that they have a direct connection to and align with business process requirements. They also relate to applicable detailed control activities. For example, "ensuring systems security" satisfies the business requirement that access to information systems, programs, and data are enabled and controlled with specific IT activities such as the use of firewalls, encryption, need-to-know, and user authorization and authentication. There are 318 detailed control objectives that are presented in COBIT as indicated above.

Finally, for each of the detailed control objectives COBIT provides *Management Guidelines* and *Audit Guidelines*. *Management Guidelines* suggest a model for developing an approach to implementing controls including critical success factors, key goal indicators, and key performance indicators. *Audit Guidelines* provide guidance for preparing audit plans, reviewing IT controls against established control criteria, and having a basis for assessing the status of IT controls. A general outline of the components of the COBIT framework is shown below:

Components of the COBIT framework for IT governance
Domains (4)

- Planning and organization.
- Acquisition and implementation.
- Delivery and support.
- Monitoring.

High-level control objectives (34)

- Information areas.
- Resources areas.

Detailed control objectives (318)
Combined example
Domain. Delivery and support.
IT process. Ensure systems security.
High-level control objective. Safeguard information against unauthorized use, disclosure or modification, damage or loss.

Information areas.	Confidentiality = primary;
	integrity = primary;
	availability = secondary;
	compliance = secondary;
	reliability = secondary;
	effectiveness = not applicable;
	efficiency = not applicable.

Resources areas.	People = applicable;
	application systems = applicable;
	technology = applicable;
	facilities = applicable;
	data = applicable.

Detailed control objective. Security of online access to data. In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

(IT Governance Institute of the Information Systems Audit and Control Association (2000). *Governance, Control and Audit for Information and Related Technology*, Control Objectives Volume, pp. 20-1 and pp. 100-1.)

COBIT and COSO are compared by the IT Governance Institute (2005) and Chan (2004) with several items of interest for this paper. Based on these comparisons and the above examples, there are some general conclusions that can be drawn. First, both COSO and COBIT take an organization-wide view but COBIT only considers an organization-wide view to the extent of ensuring that IT governance is aligned with overall business objectives and organization governance. With regard to the specification of detailed IT controls, COSO provides some guidance, but only a limited set of specific IT controls are included. On the other hand, COBIT provides very detailed IT control suggestions within its presentation of detailed control objectives. Once again, the observation is offered that it may be useful, if not necessary, to use more than one framework for assessing compliance. COSO has a realm of applicability as does COBIT and these frameworks have considerable overlap. However, COSO on its own may not provide sufficient guidance for organizations and auditors as they consider compliance with laws and regulations.

Conclusion

An increasing number of laws and regulations impact the information management functions of organizations in a variety of ways. The US SOX of 2002 and the Basel II Accord of 2004 are prime examples. Even though a law or a regulation may be silent about information management issues, the pervasiveness of IT in organizations makes it necessary to be informed of potential impacts as described in this paper.

Associated with legal and requirements is the need to assess compliance with their provisions. A number of frameworks are available for this purpose including those promulgated by the committee of sponsoring organizations of the treadway

commission and the IT Governance Institute of the Information Systems Audit and Control Association. These frameworks illustrate slightly different target audiences and purposes. However, they are complimentary with regard to information management issues, and may be used together or separately depending on the needs of an organization. Awareness of applicable laws and regulations and frameworks for assessing compliance provide a valuable resource for information managers.

References

Basel II Accord (2004), *International Convergence of Capital Measurement and Capital Standards*, Basel Committee on Banking Supervision, Basel.

Chan, S. (2004), "Mapping COSO and COBIT for Sarbanes-Oxley compliance", *IT Audit*, Vol. 7.

Coe, M.J. (2005), "Trust services: a better way to evaluate IT controls", *Journal of Accountancy*, Vol. 199 No. 3.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1994), *Internal Control – Integrated Framework*, COSO, San Jose, CA.

IT Governance Institute of the Information Systems Audit and Control Association (COBIT) (2000), *Governance, Control and Audit for Information and Related Technology*, COBIT, Chicago, IL.

Sarbanes-Oxley Act (2002), *Public Company Accounting Reform and Investor Protection Act*, US Public Law 170-204.

Corresponding author
David Luthy can be contacted at: david.luthy@usu.edu