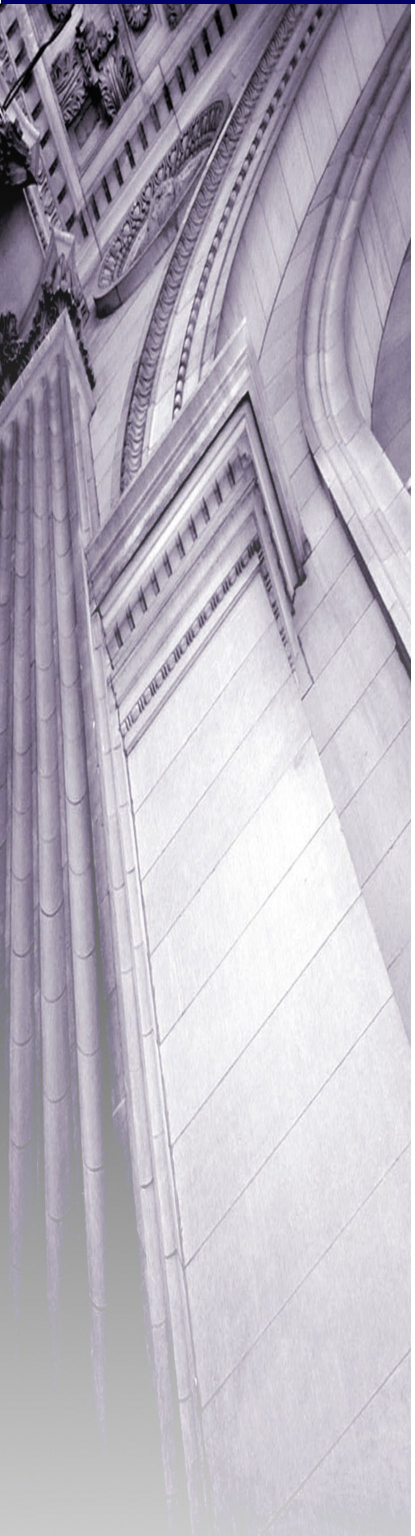
Special Report: Global Compliance
www.KahnConsultingInc.com

Addressing Compliance in Global IT Organizations

Strategies for CIOs and IT Leaders



1. Introduction

Compliance plays a growing role in the way IT systems, digital information and data are used and managed in organizations worldwide. For the CIO, compliance requirements are increasingly likely to affect purchasing, planning, and management decisions. No longer are IT compliance requirements limited only to organizations operating in highly-litigated or traditionally regulated jurisdictions and sectors. Today, in a global economy, compliance requirements derive from a variety of sources that may be new and unfamiliar. For example, while companies in the US face a new regulatory climate resulting from corporate failures such as Enron and WorldCom, EU companies face new laws such as the "8th directive" in the wake of scandals like Parmalat. Growing markets like China and the EU accession countries similarly face new challenges in modernizing regulations and controls to address the use of IT.

While some CIOs may feel that compliance issues are an unwelcome – if not overwhelming – addition to an already full roster of responsibilities, they should not be intimidated. Although there are a growing number of laws, regulations, standards, and best practices that affect IT management, many of their requirements address issues that have long been central to the CIO's role. At the same time, there clearly are compliance issues that require new levels of cooperation between IT and Legal professionals.

> *"We need to see security as a business enabler . . . [but] improvements in interconnectivity makes us all vulnerable to new threats big and small."*
>
> *Erkki Liikanen, European Commissioner for Enterprise and Information Society*[1]
>
> *"These are inside jobs: top executives, branch managers, loan officers and thousands of everyday employees have been running off with billions in customers' money."*
>
> *Wave of Corruption Tarnishes China's Extraordinary Growth, New York Times, March 22, 2005*

Many organizations addressing compliance requirements for the first time make the mistake of taking an approach that is too narrowly focused. While there are instances where "compliance triage" may be needed to address specific, immediate issues, a successful long-term solution requires a more comprehensive approach. Failing to address compliance issues at the right trajectory can seriously impact the bottom line. In fact, a recent survey found that failing to take a holistic approach to compliance is a major source of cost for organizations that operate in multiple legal and regulatory jurisdictions.[3]

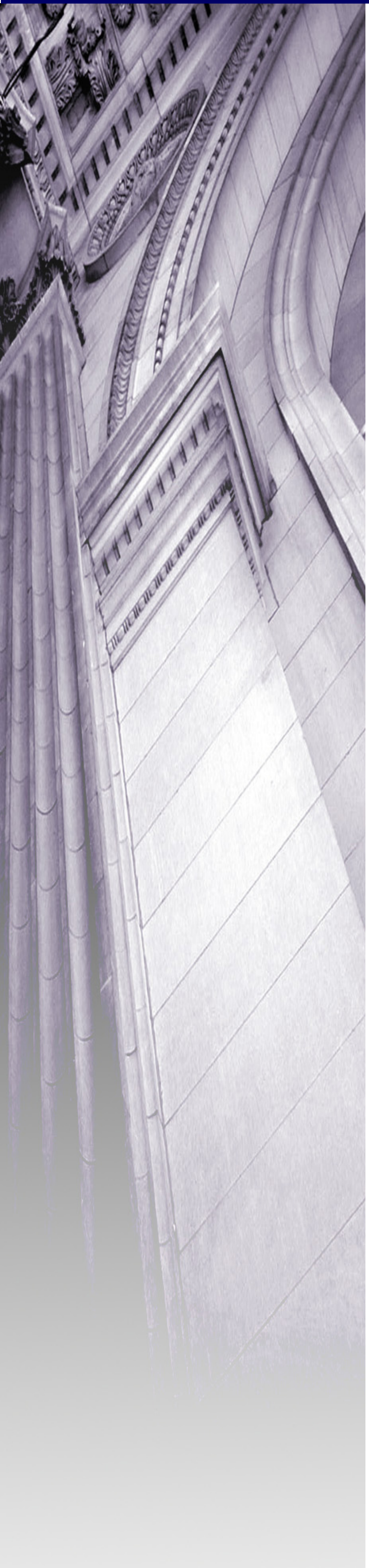
Not a legal opinion or legal advice. For all questions regarding compliance with specific laws and regulations seek legal counsel.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

Sponsored by Sun Microsystems **July 2005**

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM



This paper outlines a strategy for CIOs tackling compliance issues in their organization. Rather than focus exclusively on specific laws or regulations, it explores a high-level approach to IT compliance that can be applied in any organization addressing compliance issues - regardless of the laws or regulations in play.

> *"More than 80 percent of the world's largest and most complex companies studied are unsuccessful in capturing the full returns on their global investments . . . Compliance drivers [are] often overlooked."*
>
> *Global Benchmark Study, February 2005*[2]

2. Identifying Sources of Compliance Criteria

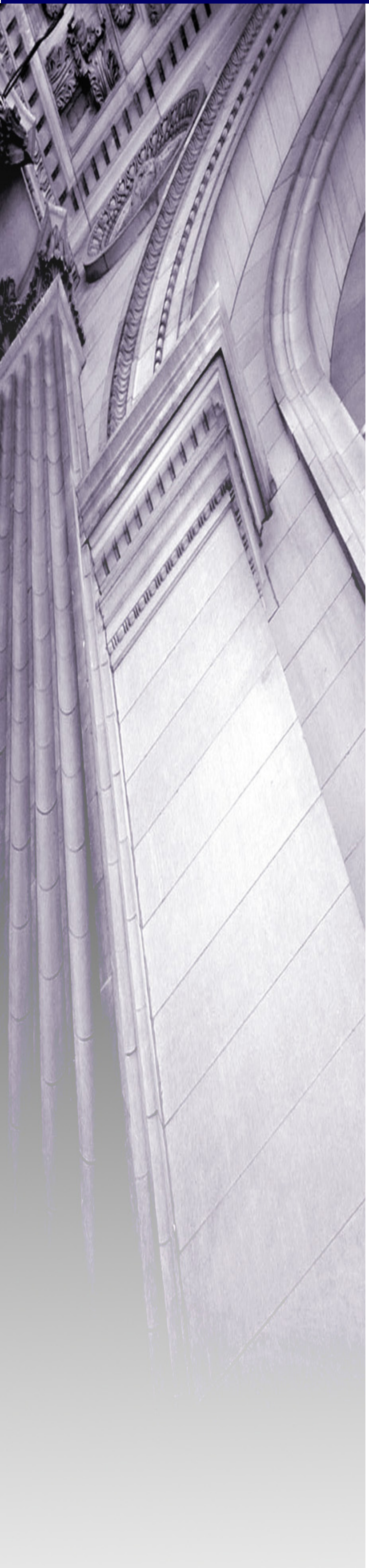
Identifying potential sources of compliance criteria can be one of the most challenging aspects of compliance for any organization. For global organizations operating in multiple jurisdictions through multiple lines of business, the challenge is even greater. Consider, for example, the reach of the Sarbanes-Oxley Act, which generally applies to **any** company listed on a US stock exchange, US-based or not. With approximately 450 non-US companies listed on the New York Stock exchange alone (representing a market capitalization of over 5 trillion euros) the international impact is very real.[5] Similarly, the impact of the Basel II accord (see below for more information) on US-based financial institutions is profound - despite the accord's international provenance.

Even local laws and regulations can have an international impact. For example, the California Database Protection Act,[6] a law enacted in 2003 in the US state of California, applies to any company doing business with the citizens of the state. The citizens of California live in one of the largest economies in the world - one that trails only the US itself, Japan, Germany, the UK, and France in GDP.[7] This law, which requires the disclosure of security breaches involving unauthorized access to protected personal information (among other things) clearly has an impact far beyond those companies based in that state.

When identifying compliance criteria that may be applicable to the activities and responsibilities of the IT department, CIOs must recognize that compliance criteria can stem from more than just laws and regulations. Traditionally, the concept of compliance was often understood to mean the process of complying with specific laws and regulations. However, for the purposes of IT compliance, this definition may be too narrow. CIOs should view compliance as a process designed to ensure that the IT organization meets a broad range of compliance criteria that may come from laws and regulations, as well as from applicable best practices, standards, industry codes, and internal directives. After all, the processes used to implement and monitor compliance controls are similar regardless of the source of the criteria.

CIOs should work hand in hand with their Legal department to identify the laws, regulations, and other compliance criteria that may apply to activities throughout the IT department. In addition, CIOs should identify specific areas of their operations that will most likely be impacted by compliance criteria – including standards and best practices. In particular, IT operations that involve the creation, use, and storage of business records (such as purchasing information), sensitive data (e.g., customer records), and other

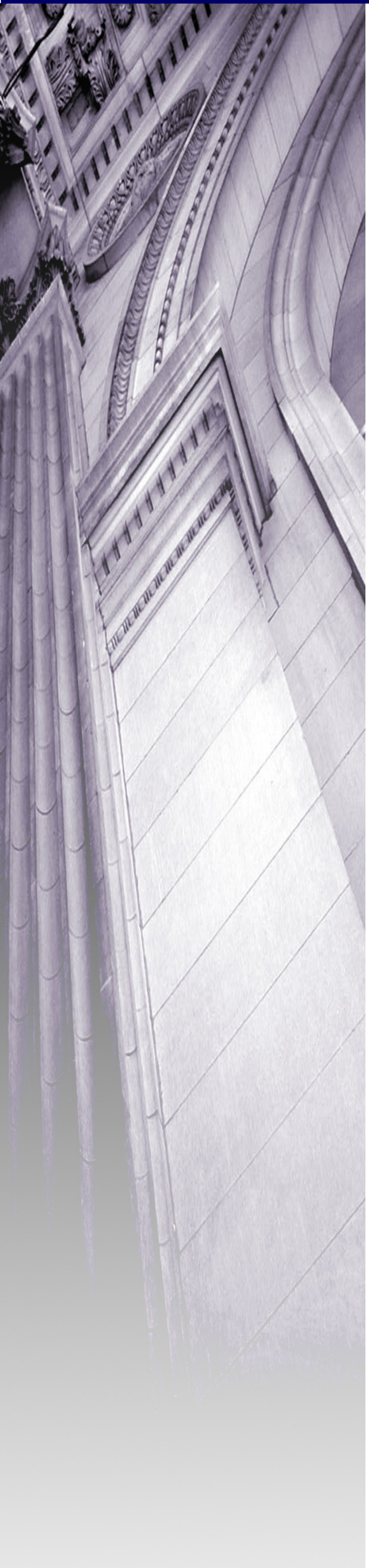
> *"Firms would do many of the things that regulation obliges them to do, even in the absence of regulation."*
>
> *UK Financial Services Authority Study on Compliance Costs*[4]



information that has legal, regulatory, and business value are those that the CIO should focus on when identifying the sources of compliance criteria and their impact on IT operations.

The following chart provides some examples of activities for which IT plays a major role; examples of compliance criteria that commonly apply to those activities; and examples of their the impact on IT.

Subject Area	Possible source of compliance criteria	The impact on IT: Examples
Information Security	Information security standards, such as *ISO 17799, BS 7799.*	Establishment of security policies and controls to "ensure the confidentiality, integrity, and availability of both vital corporate information and customer information." (BS 7799)
Data protection and privacy	Laws and regulations governing the use and protection of information, such as the *EU Data Protection Directive,* and the *Russian Federal Information Act.*[8]	The implementation of controls and directives designed to identify and protect certain types of information from loss, alteration, unauthorized disclosure or access.
E-Commerce, E-Contracting	Laws, regulations, and standards regarding electronic signatures, contracts, and invoices, such as *EU E-Commerce Directive, UK Electronic Communications Act 2000,* and *EU Directive No. 2001/115.*	Development of procedures for the management of data relating to cryptographic keys and digital certificates. Retention of trustworthy electronic records and contracts.
Cyber Crime	Laws and regulations regarding liability and prosecution related to computer crimes, such as the *Council of Europe Convention on Cyber Crime.*[9]	Establishment of directives and controls designed to prevent corporate IT resources being used to commit crimes.



Managing public records (for government entities)	Freedom of Information Acts (e.g., *UK Freedom of Information Act 2000*).[10]	Segregating public from non public records, providing efficient access to public records, protecting confidential information from inadvertent access
System Management	Corporate governance and auditing laws and standards (e.g. *EU's 8th Directive*).	Implementing controls and processes that ensure that systems creating and storing financial records are trustworthy.

3. The Impact of Compliance on IT Activities

> *"Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality or quality assurance."*
>
> *European Commission regulation*[11]

Depending on the size of the organization and the type of business activities it conducts, compliance issues may need to be considered in nearly every operation that involves the creation, use, storage, and management of data. Regardless of the specific requirements of particular laws and regulations, compliance generally requires IT organizations to take control of their systems and the information those systems contain in ways they likely never have before. Consequently, CIOs need to seek out new capabilities in their management processes, controls, and technologies to make this happen.

CIOs should evaluate their processes and technologies against 8 key considerations when working to ensure IT compliance, and should address them clearly in company policies and procedures and provide regular training to help employees get it right.

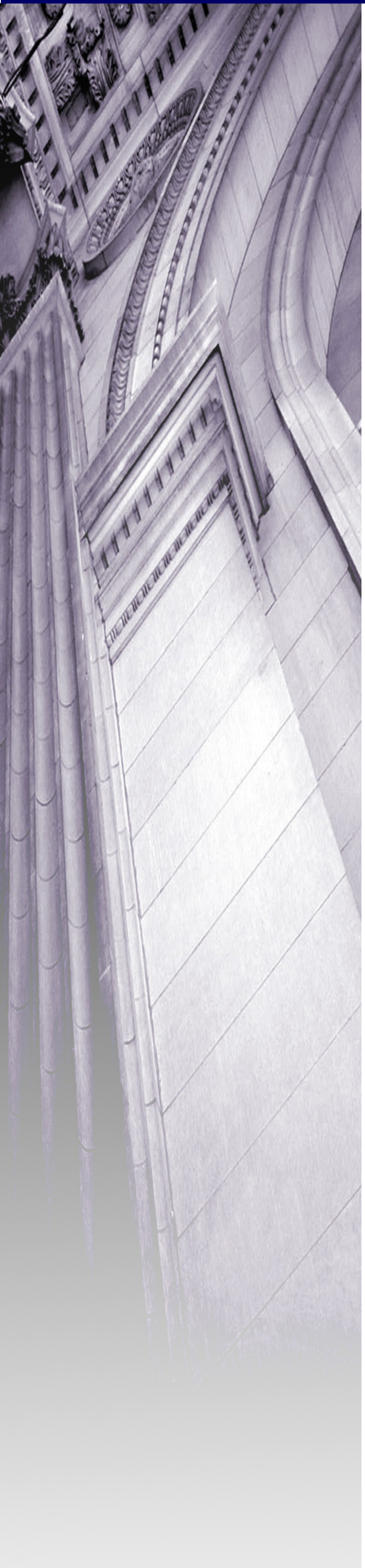
3.1 Access Controls

CIOs must have the ability to control user access to data contained within the organization's systems. This requires IT to control the access privileges of users and to identify specifically the types of data that need special protection (such as private, confidential, and trade secret data).

Establishing comprehensive and secure access controls can pose a challenge for IT. This is because for access controls to be effective, it is essential that each user in the system follow established policies and procedures. For example, procedures for password management or instructions to log off the network before leaving a terminal unattended can be difficult to enforce at the user level.

In light of this, IT must carefully consider how it intends to distribute user privileges throughout the organization. For example, access to enterprise data should be structured to limit employee to information to that which they need to do their job.

Similarly, user privileges that grant individuals the ability to make global changes or alter system configurations should be limited to a select few. In addition, IT systems should be configured so that such changes are monitored using audit trails or logs and should require the involvement of more than one administrator to make important changes to the system where possible.



3.2 Content Security

Securing enterprise data requires more than effective password management. The flexibility of digital information, its varied use, and the increasing volumes of electronic records and communications that are generated and received by the enterprise each day means that the company must manage its information across a broad spectrum of locations, technologies and devices.

CIOs need to address the risks that come with managing critical information in such an environment. Network applications and operating systems must be kept current and secure through timely patch management, and must be carefully selected with security features and potential vulnerabilities in mind. Policy and training must clearly address the acceptable use of portable devices to do business.

Not only must the network be carefully controlled to prevent intrusion from hackers, viruses and spam, it must also be configured to prevent internal theft or disruption by employees. In some instances, data protection may require the use of technologies such as encryption to protect sensitive information. In addition, secure access controls require a physical security component to prevent physical access to the organization's IT infrastructure.

And even with the most advanced technical protections in place, the human element and its affect on security must be carefully considered. For example, an international data management recently allowed access to the personal information of 145,000 persons by mistake – a case which has attracted attention internationally, and the condemnation of UK watchdog group, Privacy International.[12]

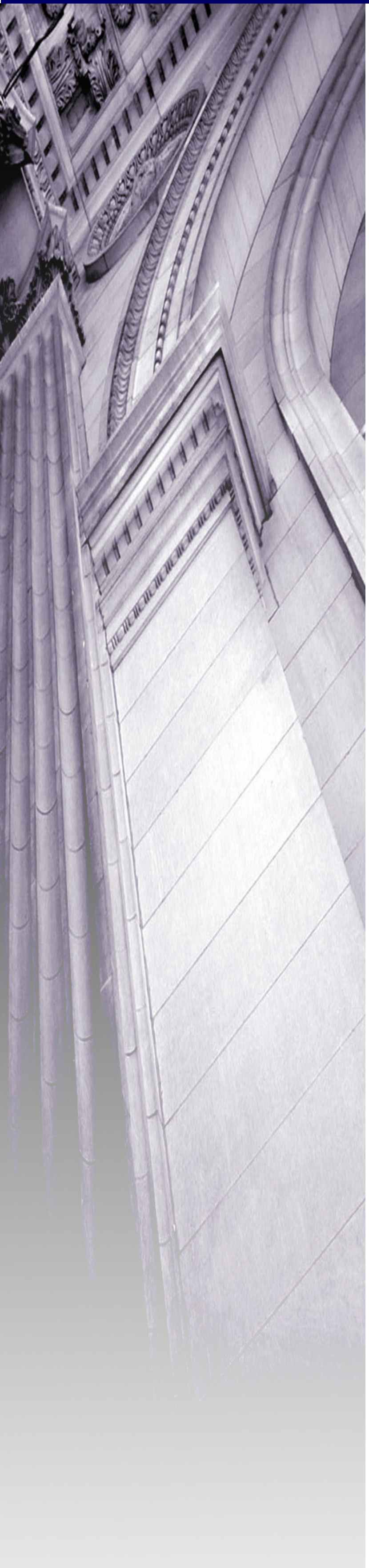
3.3 Data Classification

Proper classification of data supports the business and enables the organization to comply with compliance requirements regarding records retention, disposition, data protection, and other information management needs. In addition, data classification may be essential to complying with certain legal and regulatory requirements. For example, France recently enacted a directive requiring companies to retain electronic contracts that relate to goods and services valued at over 120 euros for ten years.[13]

Properly classifying company information as privileged, , confidential, or trade secret data, allows such information to be managed and labeled appropriately, sending a clear message to employees that access to this information should be limited to select parties within the organization and that it may need to be handled differently than other kinds of data.

For example, organizations managing personal health information should have the capability to identify and secure that category of information, while at the same time limiting access only to select employees who have authorization and have received the proper training to handle such data. Furthermore, the protection of data needs to extend throughout its entire lifecycle, from the time the data is created and stored, to the time it is disposed of.

In addition, organizations should ensure that they properly classify their business applications according to the value of the information that passes through them, and that they secure and manage those applications in a way that's commensurate with the risk.



3.4 Retention

The value of all company information comes from its content. Evaluating the content of information is a critical step in determining which information created by the organization has ongoing value and which does not. For example, an email message may have ongoing business and legal value to an organization if it was used to negotiate a contract, or very little value, if only to arrange a luncheon or send out a meeting request. Once the value of information has been determined according to its content, that information can be effectively controlled and managed to meet the organization's business and legal needs.

Some organizations may already have the capabilities to do this in place. For example, IT organizations that have implemented Information Lifecycle Management (ILM) will likely have some ability to make data management decisions based on the types of information they store. ILM, with its focus on implementing storage infrastructure based upon the kinds of information being stored, may prove useful in classifying data in a more detailed way and retaining it in a secure form for records management and compliance purposes throughout the lifecycle of the information.

3.5 Disposition

Managing the growth of electronic information within an organization is difficult unless sound decisions are made about how long information should be stored.. As a result, many organizations decide to "keep everything forever" without thoroughly considering the wisdom of keeping data that can no longer be easily accessed, data that no longer has any value to the organization, and data that represents a source of unnecessary and unmanaged expense and liability.

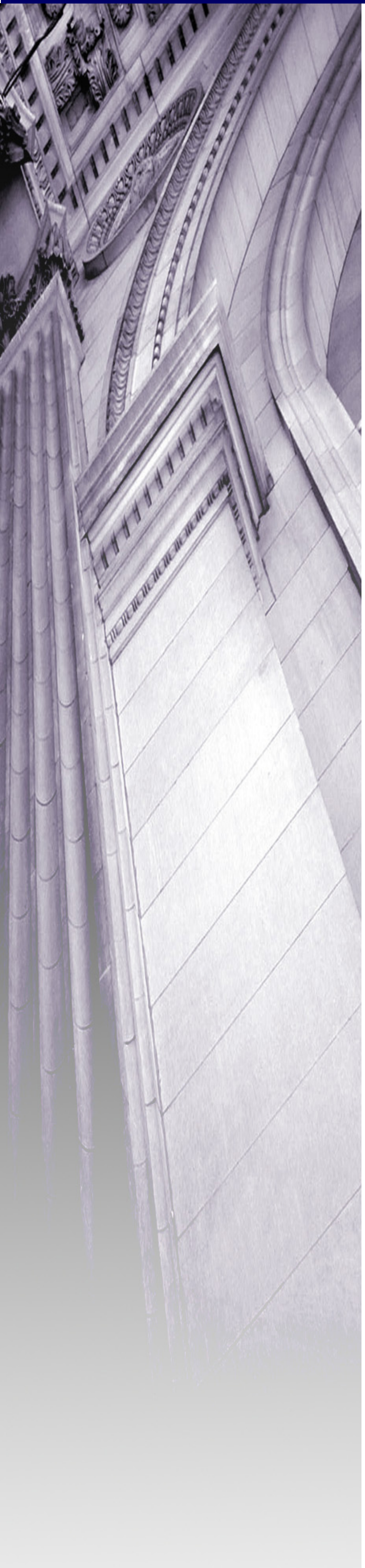
Once it has been properly classified according to its content, information that no longer has business or legal value to the organization, or is otherwise no longer required for litigation, investigations, or audits should be disposed of. Properly disposing of information that the organization is no longer required to retain or preserve is a necessary and useful component of any information management program as it helps ensure systems continue to function properly and that unnecessary storage space isn't wasted on information that has no ongoing value to the organization. Without proper classification at the outset, organizations will find it difficult to implement a meaningful and manageable disposition policy.

3.6 Access and Retrieval

Retaining data serves little purpose unless that data can be accessed by the people and applications that need it, when they need it. Moreover, certain laws and regulations demand that organizations consistently provide ready access to information in a format acceptable to a court, regulator, or other party.

Solving the access and retrieval problem begins at the point where information is captured and stored. At this stage, it is important that adequate metadata is also generated and captured. A failure to capture metadata can seriously impede its future retrieval, so CIOs should develop formal metadata policies that define what metadata will be captured and retained.

Data access also relies on storage technologies that are capable of detecting errors in data while it is being stored. Automatic detection and repair of file corruption and other mechanisms that maintain the health of stored information, indexes, metadata, logs, and other information required to access and retrieve records are also valuable for compliance purposes.



3.7 Preservation

As discussed above, CIOs should seek the tools that will allow their organization to accurately and consistently classify and retain electronic information. This capability enables the business to capture and store the information that truly has ongoing business, legal, and/or compliance value.

"A survey of IT directors from 100 UK-based organizations found that almost half would not be able to retrieve a company email more than three years old."

CNET Networks, June 2004[14]

However, organizations also need the ability to find, protect, and produce records and other information that may be relevant to lawsuits, investigations, audits, and other proceedings. In this context, organizations may need to cease the disposition of records that otherwise would be destroyed in the normal course of business, and to capture and preserve information that normally would not be retained. In the electronic age this has proved confounding, inconvenient, and expensive for organizations all over the globe.

"All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review."

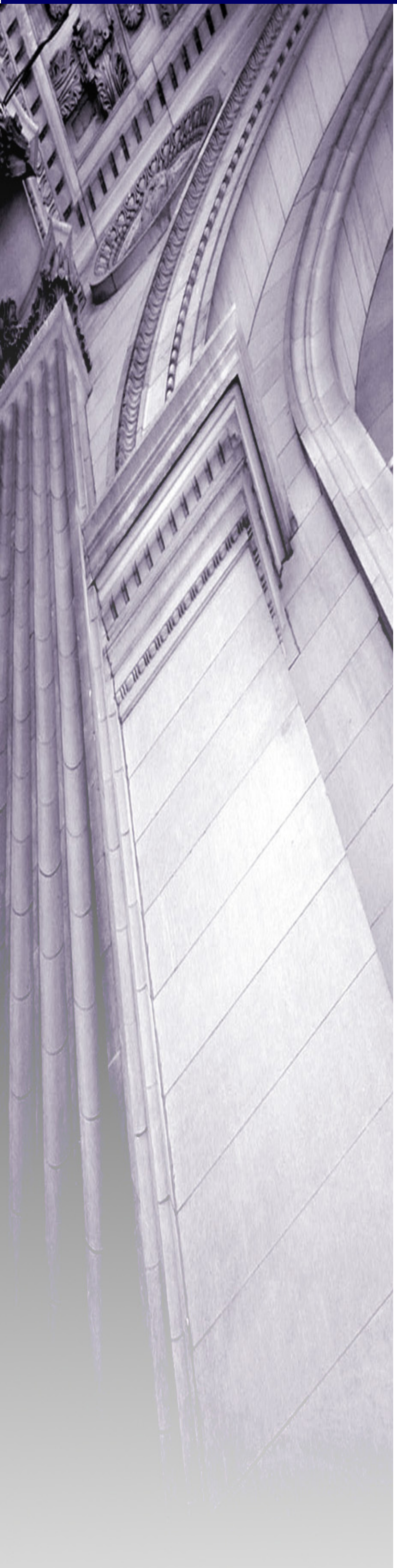
International Organization on Computer Evidence[15]

Given that outside parties, and the organization itself, are likely going to rely on information preserved in this context as electronic evidence, it is also important that the processes and tools used to find, protect, and produce this information do so in a trustworthy manner. At a minimum, CIOs should look for tools that can help them demonstrate a clear "chain of custody" for electronic evidence – from who created it, altered or accessed it, to how it was retrieved – and that protect such evidence from unauthorized access and alteration.

3.8 Auditing and Monitoring

A massive financial institution established by the US federal government was recently criticized by its regulators for "deficiencies" in the way it managed its electronic records. Among other things, the institution "agreed to 'adopt appropriate internal controls' on any 'overwriting' of database records by technical-support employees at the direction of management to make changes or corrections. Those changes would have to be properly documented."[16]

IT must develop its systems in a way that consistently tracks and monitors user compliance to prove the organization is doing what it takes to get it right. In addition to frequent monitoring, policies and procedures must be adequately enforced to send the message that compliance is a priority that is taken seriously at all levels.



4. Orienting the IT Organization to Compliance

Beyond identifying compliance criteria and developing the capabilities to address those criteria, CIOs also face the challenge of orienting their IT organization to compliance. For many IT groups, compliance may be an entirely new exercise, or one that was formerly limited to a portion of the group's activities. Moving forward, for many organizations, compliance must instead become a core function of the IT group, with its requirements considered a routine component of project activities and management responsibilities. This section explores tools for CIOs seeking to orient their IT group to compliance.

> *"At a broad level the [study] showed the advantages of keeping it simple. Prominence and profile are not necessarily the same thing as compliance efficiency."*
>
> *UK Financial Services Authority Study on Compliance Costs*[17]

4.1 Documentation and New Directives

CIOs should pursue a strategy of documenting formal procedures and directives for compliance-related activities wherever possible. Part of any successful compliance exercise is being able to demonstrate that a formal process was properly followed. Evidence of compliance processes establishes the organization's position and can help protect it against allegations of compliance failures or other problems.

> *"Community law - in the directives on electronic signatures and electronic commerce now recognises electronic communications in a number of fields as equivalent to traditional paper communication."*
>
> *Court of Justice of the European Communities, Republic de Finlande v. Commission of the European Communities*

In some cases, existing directives may be sufficient (e.g.., it is likely that most organizations have a policy dealing with password administration). In other instances, new directives will be required – especially when dealing with the retention and management of electronic data for which the IT group now holds primary responsibility. The creation of such directives will be most successful when they result from a collaborative process that involves IT, Legal, Compliance and those groups that "own" the business applications that IT delivers and supports.

In addition, IT groups should work with the Compliance department and consider compliance issues as a standard part of the IT implementation process – from product evaluation and purchasing, through employee training and implementation. IT should be aware of the compliance issues that the product or application being built, purchased, and configured might raise, as well as the compliance requirements that their new technologies might help to address.

4.2 Liaise with Legal

CIOs should establish a formal, ongoing process for communicating with the Legal, Compliance, Audit, and other departments that can provide valuable input into how IT addresses the organization's compliance needs. Guidance from these groups will be essential to ensuring that legal and regulatory compliance criteria are identified and addressed as required as part of IT purchasing, implementation, configuration, and administration activities. CIOs should plan for

a period of mutual education to allow employees on both sides of the table to understand each other's priorities, methods, and even the technical terminology or specialized vocabulary that's unique to other business units

CIOs may even want to consider creating a specific role within the IT group that is focused on identifying compliance issues and liaising with the Legal department. In the US state of Delaware (where many US and multinational corporations are registered), the federal court is recommending that companies appoint an "electronic discovery liaison" who is intimately familiar with the organization's databases and other systems that create and house information of potential relevance to lawsuits, investigations, and audits. This liaison is expected, for example, to be "knowledgeable about the technical aspects of e-discovery, including electronic document storage, organization, and format issues."[18]

4.3 Communication and Training

CIOs should plan and budget for training members of the IT group on compliance issues. System administrators, for example, need to understand the impact of their activities within the systems they are responsible for. For example, a storage administrator may allow backup tapes containing information relevant to a lawsuit to be recycled unless they receive training on electronic discovery procedures and the necessity of preserving such information.

> *"Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilises computers."*
>
> *EU Good Manufacturing Processes[19]*

In addition, training should be reinforced by consistent communications to employees that compliance is a priority to be taken seriously. Both the organization's compliance strategy and its IT governance strategy should be disseminated widely so that the goals of these departments, as well as the risks of compliance failure, are understood and can be addressed throughout the enterprise.

5. Select Laws and Regulations

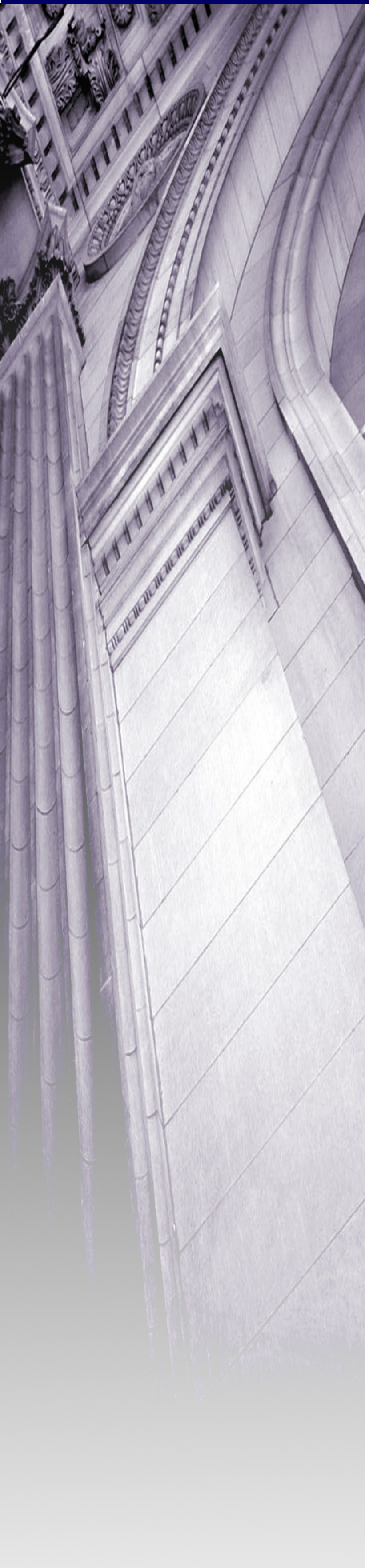
Each organization faces a unique set of laws and regulations that they must comply with based on their size, operating jurisdiction, structure, lines of business, and other factors. As such, it is critical that organizations conduct a complete analysis of their specific compliance environments.

At the same time, there are a number of laws and regulations that are worthy of study and investigation, for a number of reasons: they affect a great number of organizations; they contain novel requirements that are universally instructive; they have established an approach that is followed by other criteria; or for other reasons.

The following section provides a brief list of such laws and regulations.

5.1 EU 8th Directive on Company Law

Often described as "Sarbanes-Oxley" for Europe, the EU's proposed updates to the 8th Directive on Company Law is a corporate governance and accounting reform regime that has some similarities to the US Sarbanes-Oxley Act of 2002 (which was enacted there in the wake of corporate failures similar to Enron). Like Sarbanes-Oxley, the 8th Directive addresses financial



audit procedures, auditor independence, and oversight of the audit function (among other topics). Also like Sarbanes-Oxley, the 8th Directive implies that organizations need to ensure that the systems that create and house financial and other information are trustworthy and can be relied upon.

Furthermore, the 8th Directive states that EU members "shall provide effective, proportionate and dissuasive civil, administrative or criminal penalties . . . where statutory audits are not carried out in conformity with this Directive." (Article 30)

"The recent spate of scandals in the US and the EU have emphasised that statutory audit is an important element in ensuring the credibility and reliability of companies' financial statements."

European Commission, April 2004[20]

5.2 21 CFR Part 11

This US Food and Drug Administration regulation, which impacts pharmaceutical and other companies operating inside and outside the US that sell into US markets, lays out a number of detailed requirements related to electronic systems. The regulation's criteria address, for example:

- System validation
- Electronic copies
- Records protection
- System access
- Secure, computer-generated, time stamped audit trails
- Operational sequencing checks
- Authority checks
- Device checks
- Written polices for signature users
- Documentation controls

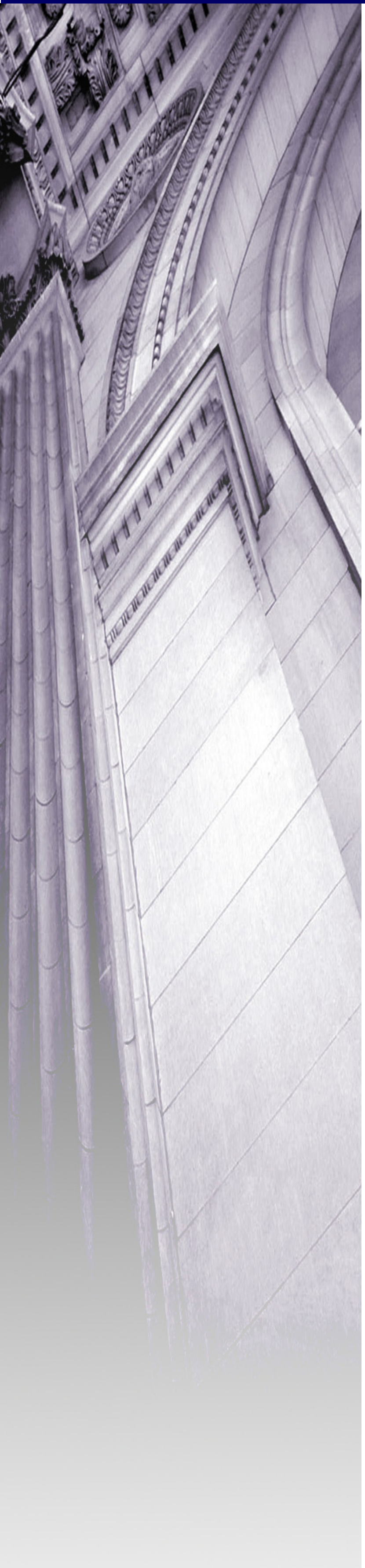
The regulation emphasizes the need for organizations to have very tight control over their IT systems and the data generated and stored by those systems.[22]

And, the FDA takes the regulation's requirements seriously. In fact a Swedish pharmaceutical facility was shut down by the FDA because, among other things, there were serious problems in the way it was managing IT systems and electronic information. The FDA found that:

- a critical computer system "lacked the capacity to retain electronic data . . . information was overwritten due to the storage capacity of the equipment's hard drive."

". . . provides criteria for acceptance by the FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper.

FDA 21 CFR Part 11[21]



- IT systems used for managing critical data "lacked adequate validation and/or documentation."

EU directives on the use of computerized systems in the pharmaceutical industry take a similar approach. For example, these directives make clear that, "before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results."[23]

5.3 Basel II (International Convergence of Capital Measurement and Capital Standards: a Revised Framework)

Basel II[24] is a standard established by the Basel Committee on Banking Supervision (comprised of central bank representatives from the G10 countries) that relates the amount of capital that international financial institutions must maintain to the risk profile of the organization. In the EU, it is expected that Basel II will be implemented into law for all credit institutions and investment businesses.

Basel II is important across the financial services sector because of the emphasis that it places on risk assessment and management. Given that this section tends to be one that relies heavily on IT throughout its operation, proper management and control of IT systems and data clearly plays a large role in the overall risk management process of organizations subject to Basel II's requirements.

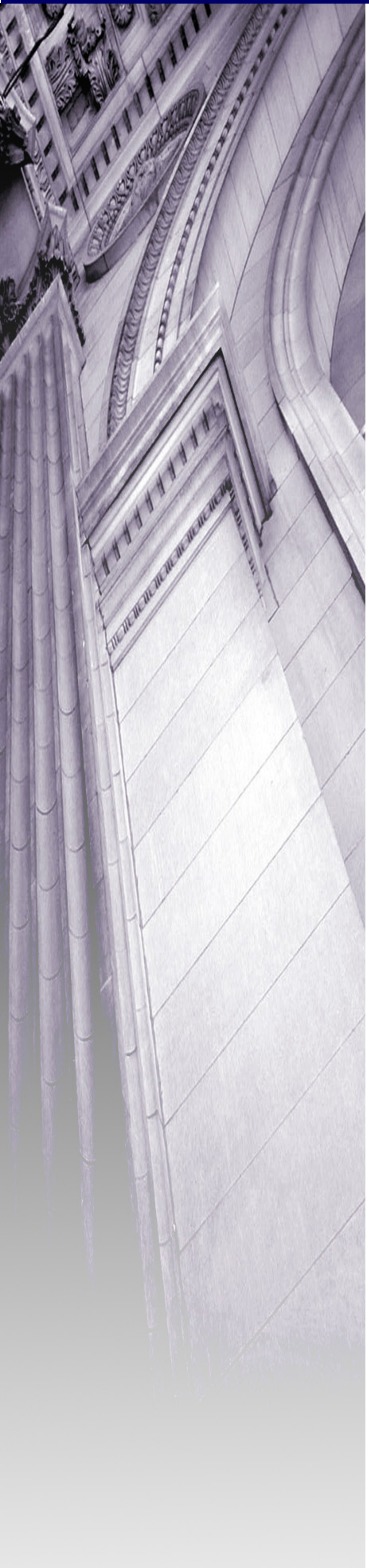
More specifically, one of the categories of risk that organizations must assess under Basel II is "Operational Risk," which includes, "the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events." Clearly, poorly managed IT systems, incomplete documentation, inadequate policies, and other IT-related weaknesses should be considered in this category. As such, it is important for CIOs in organizations subject to Basel II to ensure that its requirements form part of the criteria used to establish and implement IT management procedures and tools.

5.4 EU Data Protection Directive

The EU Data Protection Directive (Directive 95/46/EC)[25] is designed to "protect the fundamental rights and freedoms of natural persons and in particular the right to privacy, with respect to the processing of personal data."[26]

The Directive requires organizations handling private information to "implement appropriate technical and organizational measures to protect personal data against . . . loss, alteration, unauthorized disclosure or access"[27]

As discussed above, the requirements of the Directive mean that organizations need to implement tools and processes to ensure that private data is properly identified, classified, used, and protected.



6. Conclusion

Global organizations face new compliance requirements and challenges from a variety of new sources. The CIO must play a leadership role in ensuring that these organizations adequately address relevant IT compliance criteria. This may require CIOs and other IT leaders and professionals to re-orient their activities towards compliance, or to appoint individuals with specific responsibilities for understanding the impact of laws, regulations, standards, and other sources of compliance criteria in IT operations and activities.

> *"But CIOs should look before they leap into purchasing . . . supposedly ready-made answers. It isn't easy to put compliance in a box."*
>
> *CIO Insight, May 2004*[28]

Regardless of the specific compliance requirements that international organizations face in their various operating jurisdictions, much of what must be done to comply is already understood by IT professionals. CIOs have always been concerned about ensuring that data is available, secure, and has integrity. That being said, new laws, regulations, and other compliance developments provide new incentives to invest in applications and infrastructure that help to ensure these qualities exist, and indeed provide new consequences for failure. As a result, global organizations need to evaluate their approach to IT management to ensure that they are prepared for the new requirements of IT compliance.

7. About Kahn Consulting

Kahn Consulting, Inc. (KCI) is a consulting firm specializing in the legal, compliance, and policy issues of information technology and information lifecycle management. Through a range of services including information and records management program development; electronic records and email policy development; Information Management Compliance audits; product assessments; legal and compliance research; and education and training, KCI helps its clients address today's critical issues in an ever-changing regulatory and technological environment. Based in Chicago, KCI provides its services to Fortune 500 companies and government agencies in North America and around the world. Kahn has advised a wide range of clients, including Time Warner Cable, Ameritech/SBC Communications, the Federal Reserve Banks, International Paper, Dole Foods, Sun Life Financial, Kodak, McDonalds Corp., Hewlett-Packard, United Health Group, Prudential Financial, Motorola, Altria Group, Starbucks, Mutual of Omaha, EMC Corp., Merck and Co., Sony Corporation, and the Environmental Protection Agency. More information about KCI, its services and its clients can be found online at: www.KahnConsultingInc.com.

8. Endnotes

[1] "European Network Security," Mr Erkki Liikanen, speech given to Stonesoft EMEA partner meeting, Helsinki, 10 October 2003.

[2] Unlocking the Value of Globalisation: Profiting from Continuous Optimisation," Deloitte Research, February 2005.

[3] "Unlocking the Value of Globalisation: Profiting from Continuous Optimisation," Deloitte Research, February 2005.

[4]"Costs of Compliance: A Report by Europe Economics" for the UK Financial Services Authority, June 2003 (www.fsa.gov.uk/pubs/other/cost_compliance.pdf).

[5] New York Stock Exchange webpage. Online at: http://www.nyse.com/about/listed/listed.html?ListedComp=NONUS

[6] California Civil Code §1798.29 and 1798.82 - 1798.84

[7] "Cal Facts 2004, California's Economy and Budget in Perspective," California Legislative Analyst's Office, 2004. Online at: http://www.lao.ca.gov/2004/cal_facts/2004_calfacts_econ.htm

[8] Federal Act No. 24-FZ, "On Information, Informatizaion and Protection of Information," February 20, 1995.

[9] Council of Europe Convention on Cybercribe, Convention on Cybercrime, Budapest, 23.XI.2001

[10] Freedom of Information Act 2000, 2000 Chapter 36.

[11] Annex 11 (Computerised Systems) of Volume 4 (Good Manufacturing Practices) of the rules governing medicinal products in the European Union.

[12] "PI Announces U.S. Big Brother Awards winners for 2005," Privacy International, April 15, 2005. Online at http://www.privacyinternational.org

[13] Decree No. 2005-137, February 16, 2005.

[14] "UK Banking Firms in breach of FSA email regulations," Andy McCue, Silicon.com, June 24, 2004.

[15] Principles For The Procedures Relating To Digital Evidence, International Organization on Computer Evidence. Online at: http://www.ioce.org/

[16] "Fannie Mae Is Cited for 'Deficiencies'; Regulator Sets Conditions To Correct Internal Controls; Office of Compliance Created," James R. Hagerty. Wall Street Journal. (Eastern edition). New York, N.Y.: Mar 9, 2005. pg. A.3

[17]"Costs of Compliance: A Report by Europe Economics" for the UK Financial Services Authority, June 2003 (www.fsa.gov.uk/pubs/other/cost_compliance.pdf).

[18] "Default Standard for the Discovery of Electronic Documents," Ad Hoc Committee for Electronic Discovery of the United States District Court for the District of Delaware. Online at www.ded.uscourts.gov/Announce/AdHoc-Disc.pdf

[19] Annex 11 (Copmuterised Systems) of Volume 4 (Good Manufacturing Practices) of the rules governing medicinal products in the European Union.

[20] "Proposal for a Directive Of The European Parliament And Of The Council on statutory audit of annual accounts and consolidated accounts and amending Council Directives 78/660/EEC and 83/349/EEC," Explanatory Memorandum, 16.3.2004.

[21] 21 CFR, Part 11, Electronic Records; Electronic Signatures.

[22] The FDA has provided detailed guidance on 21 CFR Part 11. Online at: http://www.21cfrpart11.com/files/fda_docs/part11_final_guidanceSep2003.pdf

[23] See, for example Annex 11 (Copmuterised Systems) of Volume 4 (Good Manufacturing Practices) of the rules governing medicinal products in the European Union, and related EC directives, such aas Directive 2003/94/EC, of 8 October 2003 (pharmacos.eudra.org/F2/eudralex/vol-4/home.htm).

[24] International Convergence of Capital Measurement and Capital Standards: a Revised Framework, June 26, 2004. Online at: http://www.bis.org/publ/bcbsca.htm

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[26] (Article 1(1)).

[27] The Directive went into effect on October 25, 1998, and gave EU member states three years to adjust their laws as required to conform.

[28] Eric Nee, "Sox in a Box: Due Diligence," CIO Insight, May 1, 2004.