Reducing Sarbanes-Oxley Operational Risk

Using

A Document Management System

30th June, 2011

Prepared by: John V. Ashley, CEO,
Cheq Information Technology, Inc.

This white paper reviews the Sarbanes-Oxley Act and discusses the reduction of Operational Risk associated with managing information required by the Act using an Enterprise Document Information Management System.

It has been nine years since Congress passed the Sarbanes-Oxley Act (SOX) and, yet, questions continue about how to effectively comply with the Act and what documents need to be retained and for how long. When Congress passed SOX in July 2002, it imposed new accounting and financial reporting requirements on publicly traded companies. These requirements impact all companies traded on US exchanges with revenues in excess of $75 million and also apply to private companies to some degree.

A record, under SOX, is any material that contains information about the company's plans, results, policies or performance. Thus, anything about the company that can be represented with words or numbers is considered a business record and companies are now expected to retain and manage every one of those records, for several years or in some cases permanently depending on the nature of the information. The need to manage potentially millions of records annually creates many new challenges for business, every department head and especially the IT department who must develop solutions to securely store, maintain and manage all this data.

Sections 302 and 404 have the greatest business impact in terms of ongoing compliance obligations. Section 302 became effective with the original Act and Section 404 became effective in 2004. Section 302 pertains to corporate responsibility for financial reporting, and requires that the CEO and CFO personally stand behind the accuracy of their company's quarterly and annual financial statements. In order for the CEO and CFO to certify that the financial statements are 100% correct, systems must be developed and in place to pull together all of the business performance data from all across the company – even if that data resides in various departments, business units, in separate data centers or on different networks and in different countries.

At the end of each quarter, all of the business information must unite into one comprehensive and accurate financial view of the business. In many instances the numbers are created on spreadsheets and flow back and forth between departments and business units as final numbers are revised. During this process and depending on the size of the company, potentially hundreds of people have input into the final data to be reported. All of these spreadsheets, as well as all of the documents and emails that were used to arrive at the final financial conclusions, are considered records under SOX and must be maintained.

For example, let's say an accountant in one of the company's divisions is working to finalize the division's quarterly sales and receives an email from the division sales manager to change a sale for Customer A from $20 million to $30 million. That email now becomes a business record under SOX, and so does every other record in the company that may be used to shape or influence the company's financial reporting. It must not only be retained but is also auditable in the event of any investigation. Before the CEO and CFO sign off on the company's financial statements there should be a process in place to manage all of the records that went into creating the financial statements. They both face severe penalties, including prison, if serious errors or fraud is discovered in the financial reporting.

Section 404 requires that annual reports contain a discussion of the effectiveness of internal controls. This places a major responsibility on the CFO, the company's Chief Compliance Officer, and the company's external auditors who must provide a public opinion about the reliability and effectiveness of the company's internal controls. Internal control not only includes policies and processes but also the company's IT systems and record retention. A lack of good records retention or document management technology might imply a serious lack of reasonable internal controls to an auditor or investigator.

Although SOX does not spell out technology requirements for records retention, it does clearly imply that companies are expected to exercise strong control over all the records and information that is used to produce financial statements. This not limited to just the financial statements and accounting records. It includes marketing and sales reports, internal memos, and even instant messaging, and just about every type of file produced by company employees.

Section 409 mandates significantly expanded disclosure requirements, with disclosures made as quickly and completely as possible after an event affects the company's performance. SOX makes the assumption that companies have almost real-time visibility into their company's data, including all sorts of situations and business transactions that are outside the direct control of the accounting or finance functions. For example, let's say that a marketing manager in your Topeka office is made aware that a large shipment of product is going to be recalled due to a defective part. The recall will very likely have a material effect on the company's financial performance. As soon as the company is aware of this event, SOX requires that it be disclosed publicly, generally within a matter of a few days.

Sections 103, 801(a) and 802 are the core of SOX's record retention rules. Section 103 relates to audit work papers and evidence. Sections 103 (a) and 801 (a) require public companies and registered public accounting firms to maintain audit work papers, documents that form the basis of an audit or review, and all information supporting conclusions for at least 7 years.

Section 802 addresses the retention and destruction of records, with implied penalties. Under Section 802 it is a crime for anyone to intentionally destroy, alter, mutilate, conceal, cover up, or falsify any records, documents, or tangible objects that are involved in or could be involved in, a US government investigation or prosecution of any matter, or in a Chapter 11 bankruptcy filing. Section 802 stresses the importance of record retention and destruction policies that affect all of a company's e-mail, e-mail attachments, and documents retained on computers, servers, auxiliary drives, e-data, web-sites, as well as hard copies of all company records. The rules state that any employee who knows their company is under investigation, or suspects that it might me, must stop all document destruction and alteration immediately. And, the employee must create a company record showing that they have ordered a halt to all automatic e-data destruction practices.

Private companies are also expected to comply with SOX §802. Private companies now face fines plus up to twenty years imprisonment for knowingly destroying, altering or falsifying records with the intent to impede or influence a federal investigation.

E-mail under SOX is considered a business record and must be maintained. There are four key components to ensure compliance under SOX. E-mail must be tamper proof. It must be password protected, read-only and non-deletable, encrypted and digitally signed. It must exist in a closed system both on and off-line. E-mail must follow the defined policies of the business. Policies include what e-mail is archived, retention period and how e-mail is protected. E-mail must have full audit ability of access and movement. It must have the ability to be audited by a third party. And finally, e-mail must be fully indexed and provide full search capability. Specifically, e-mail archiving must be index-based on capturing standard RFC-822 header information.

In conclusion there are still businesses that are not in compliance with SOX. Failure to follow SOX records retention requirements is now considered an obstruction of justice and can result in either fine or imprisonment up to 20 years, or both. Like most practices that business does not understand, they typically delegate to the credit department. However, the credit department is one of many departments within the company whose reporting information and records is included in the creation of the company’s financial reporting. The responsibility for creating a SOX compliant system rests with company management and the IT department (See Note 1).

A recent review of the InfoRouter Enterprise Document Management Solution determined that it is uniquely positioned to provide corporations with the technology to meet the stringent information management and reporting needs of SOX as described above and most importantly reduce operational risk.

Technology at this level of complexity has traditionally been viewed as very costly. This is not the case with the InfoRouter System. The cost of acquisition has been structured to provide maximum performance at a price that is about a quarter of comparable systems. However, as is always the case with information technology based solutions; acquisition is only one part of the total cost. The other part is implementation.

The InfoRouter System has been designed as an intuitive highly secure system with simple configuration tools. Not only has implementation been simplified, but from a user perspective the screen displays have been designed to emulate the highly popular Microsoft Windows™ display architecture. This makes for ease of use thus ensuring reduced training costs and a high level of productivity.

The InfoRouter attributes are extensive so rather than list them all, below are the comments from a user that we interviewed and who has been using InfoRouter to automate their SOX information for the last five years.

In our interview with Ms. Danyel Webley; Director of Internal Audit and the primary InfoRouter user for audit control at Lakeland Industries, Inc., a multidivisional, publicly-held producer of quality, high-performance protective garments for industry in both domestic and worldwide markets, she commented:

“We acquired the InfoRouter System in 2006 to replace our existing multiple PC, user controlled, system. The PC system was difficult to manage as there were key financial documents, some with no version control, spread across multiple PCs. In order to account for all the high level documents for audit purposes. I had to keep a listing of every PC and the relevant files wherever they were located. The auditing process was demanding and very time consuming.

When the InfoRouter System was supplied, I personally installed it using the documentation on the website. This was a very easy process and I did not require the services of IT staff. After I had installed it, all I had to do was give the appropriate staff a couple of training classes and we were fully operational. Today, the only role that our IT staff performs is the implementation of software updates which we receive from time to time."

She continued by saying: "With the introduction of the InfoRouter System, which was like having a large central electronic filing cabinet, we were able to realize some key benefits. For example, one of the early benefits was to impose a discipline on how we managed our critical documents; Using the security capabilities we have been able to limit access to our most important documents to our key executives and our Board of Directors; Audit trails are easy to follow and automatic version control has eliminated the lack of control we had with our previous system. We also have manufacturing plants in China. In late 2006 I hired an Internal Auditor who I brought online to the InfoRouter System and she has helped train some of the other key employees in China. Sensitive information from China in now added directly to the system. This avoids using our email system and zipping and unzipping files. Viewing relevant information that is specific to that facility was also enabled."

She went on to say "One of the aspects of a SOX audit is the sensitive information that is needed. The multiple levels of security that InfoRouter uses are very good and meet all our needs in this area. Further, when the external auditors want to know who has had access to what documents, for example, all we have to do is use the InfoRouter report tool which keeps a variety of key data and automatically generates the report. When it comes time for an audit, we establish a portal for them and that reduces our costs as they are able to perform their audit without the added expense of physically being on our site."

She concluded by saying "Today, Lakeland Industries has continued to expand the use of the InfoRouter System into other document management areas. We now use it to manage all our ISO 9000 documentation, where the workflow component of InfoRouter has proved a very valuable tool. In addition we are expanding its use into our operations in Mexico and setting up product portals for our clients.

Overall, we have achieved a major leap forward in the management and control of our documents, reduced our operational risk associated with the sensitive information we work with as well as benefiting from improved productivity and cost reduction."

In addition, according to Ms Amanda Walley who is Accounting Assistant and uses it to post monthly reports and the VP of Finance's journal entries at Lakeland Industries, Inc., "I have worked with the InfoRouter System from the beginning and after I had received a couple of training classes, we used it right away to manage our financial information and it has functioned since that time with no problems whatsoever."

On the Lakeland Industries website is a link to "Financial Information" **-** www.lakeland.com/financial.shtml

At the bottom of this page is a small panel called "**More Lakeland Financial Information**". Within this panel is an important link – Sarbanes Oxley (www.lakeland.com/financialboardassets.shtml).

We recommend that readers review the contents of this web page as it clearly defines the ***"Protection and Use of Company Resources", "Information Security", "Trademarks and Brands Usage"*** and ***"Business Continuity".*** Further, if they do not currently exist, we would strongly suggest that readers consider whether they should implement similar instructions that they tailor to their own specific corporate needs within the Sarbanes-Oxley framework.

Notes:

(1) Our thanks to David Balovich, CEO of 3JM Company (**www.creditworthy.com/3jm/index.html**) who wrote the article "Sarbanes-Oxley Document Retention And Best Practices" and which was published in Creditworthy News on 9/05/07 and who gave us his permission to use it.

(2) Our thanks to Ms. Danyel Webley, Director of Internal Audit and Ms. Amanda Walley, Accounting Assistant from Lakeland Industries, Inc. who graciously gave up time from their busy schedules to discuss their use of the InfoRouter System as it applied to their auditing requirements.

(3) The information provided above is for educational purposes only and not provided as legal advice. Legal advice should be obtained from a licensed attorney in good standing with the Bar Association and preferably Board Certified in either Creditor Rights or Bankruptcy.

============

About the Author:

Mr. Ashley has been involved in Information Systems Design, Advanced Technology Development, Process Re-engineering and Automation Integration for over thirty-five years. He has successfully managed the implementation, integration and marketing of major multi-million dollar systems in Europe, the USA, Canada and Asia/Pacific for both Government and Industry. Mr. Ashley has also been used in the USA and internationally as a strategic resource by several major consultancy houses where his operational process design skills were required.

Information:

For further information on this white paper, please contact John V. Ashley at john.ashley@cheq-it.com.

For information on the InfoRouter System, please contact marketing@custdata.com.