

Financial Controls and Sarbanes-Oxley

A Framework for Automation and Simplification

A Lawson White Paper

Prepared by Grant Ostler, Vice President
Internal Audit and Compliance
Lawson

Meeting Sarbanes-Oxley (SOX) Section 404 and 409 financial auditing and reporting requirements is a major challenge for publicly traded companies in the United States. Similar legislation introduced by the European Union adds to the challenge for multi-national businesses. Extensive reviews of financial controls by hundreds of companies during 2004-2005 revealed that for mid-market and larger businesses, “control” over SOX auditing and reporting requirements requires identifying and monitoring thousands of interactions involving employees, financial accounting and ERP applications, other IT systems, third-party outsourcers and subcontractors. Lawson Software suggests a framework for putting the SOX compliance challenge into perspective and simplifying and streamlining the process by leveraging the power of ERP, workflow automation, and automated SOX control management activities.

Contents

Financial Controls and Sarbanes-Oxley	1
Contents	2
Introduction	3
Section 404	3
Section 302	4
Section 409	4
Compliance and auditing concerns.....	5
Manual versus automated system controls.....	5
Lessons learned	6
IT: The components of compliance	7
Transactions	7
Security	7
Reporting.....	7
Monitoring.....	8
Control activities	8
Control management	8
Getting control under control.....	9
Assessing technology options	10
– Should you retain existing processes?	10
– Can existing processes be optimized?	10
– Can existing systems be simplified?	10
Making choices	10
Comprehensive business and compliance functionality	10
Works with your current document management solutions.....	10
Control processes through automated workflows.....	10
Reporting and monitoring	11
Facilitating collaboration	11
Tight integration	11
Flexible, open architecture.....	11
Single source of employee data	11
Digital dashboards.....	11
Drill-down capabilities	11
System security	11
Change notifications	11
Manager and employee self-service	11
Management by exception	11
Automated, on-demand reports	11
Customized data feeds to vendors	11
Benefits beyond compliance.....	12
About the author	12

Introduction

With the passage of the Sarbanes-Oxley Act in 2002, publicly traded companies in the U.S. must exercise higher levels of oversight over corporate information and the processes used to link this information to financial accounting statements.

New rules promulgated by the European Union, drafted in response to corporate accounting fraud similar to the scandals that roiled the U.S. economy, compound the challenge for multinational businesses.

Virtually all publicly traded companies are affected by one or more of these regulations. The suddenness with which many of these new regulations were enacted has left many businesses scrambling to understand their impact on internal processes. In the United States, most affected businesses have focused on the most striking — and loosely drawn — provisions of the SOX Act, which are briefly described below.

Section 404

Section 404 requires management to establish, maintain, and report on internal financial control components in financial reports and other public documents.

As part of the provision, external auditors are required to perform an independent assessment of management's performance in this area. This independent assessment also has to be disclosed publicly.

The provision itself is very broad and does not mandate specific mechanisms for compliance. Subsequent guidance from

the SEC, however, directed publicly traded companies to follow an established internal control framework for meeting the broad requirements of Section 404. The overwhelming majority of companies subject to SOX have adopted what is referred to as the COSO framework, which was developed by the five main U.S. professional accounting associations in 1992 in response to the meltdown of the U.S. savings and loan industry in the 1980s.

COSO, which stands for the Committee of Sponsoring Organizations of the Treadway Commission, attempts to provide a common definition of internal controls, standards, and criteria against which companies and organizations can assess their financial control systems. It defines internal control as a process, affected by an entity's board of directors, management and other personnel, designed to provide the reasonable assurance of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

The COSO Framework has the five key elements shown below.

Control environment: This refers to the integrity, ethical values, management operating style, human resource policies, and delegation of authority systems that hold people accountable not only for financial results, but for attaining those results in appropriate ways.

Risk assessment: This includes the identification of a company's strategic and tactical goals and objectives coupled with the identification and analysis of barriers to achieving those goals and objectives. Included are the relevant risks to accurate and compliant financial reporting.

Control activities: These include the policies and procedures that help ensure management and board directives are carried out. Control activities occur throughout the organization, at all levels and in all functions, and may number in the thousands. Companies have control activities to ensure the accomplishment of operational objectives and ensure compliance with applicable laws and regulations, including those mandated by SOX Section 404.

Internal controls over financial reporting include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, asset security, and segregation of duties. The latter area is an important part of SOX and refers to ensuring that no single employee is authorized or has the ability to carry out all necessary steps of a financial process alone.

Monitoring: The process assesses the quality of the internal control system over time, and ensures that management and board members know that people in the organization are doing things the right way. Monitoring takes place both on an on-going basis and through separate evaluations.

Introduction, continued

Information and communication:

Basically, a company's system of gathering and communicating information constitutes the glue that holds internal control systems together by ensuring that appropriate information is communicated across, and up and down, the organization and with external parties, such as customers, suppliers, regulators and shareholders. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own roles in the internal control system, as well as how individual activities relate to the work of others.

In 2004, COSO, largely in response to the new compliance demands of SOX and other legislation, amended the framework and suggested that companies should add controls and formalize reporting processes in three additional areas — internal controls objective setting, event identification, and risk response.

Section 302

Section 302 requires CEO's and CFO's to personally certify that they are responsible for disclosure controls and procedures, and that they have performed an evaluation of the controls and have notified their audit committees and independent auditors of any deficiencies. Basically, Section 302 mandates that companies insure that all relevant information that requires disclosure to the public under SEC regulations are evaluated and disclosed in quarterly and annual financial reports.

Section 409

Section 409 mandates "real-time" disclosure of financial and operational material events that could affect business operations and potentially stock prices. Section 409 is even shorter than Section 404, and originally its provisions seemed quite severe. These included a 48-hour deadline for filing and a much broader definition of material events than

businesses were accustomed to.

Subsequent guidance from the SEC extended the deadline to a minimum of four business days and rejected some of the proposed events necessitating a filing. Still, Section 409 represents a major departure from previous standards.

Compliance and auditing concerns

As noted, Section 404 of Sarbanes-Oxley has commanded the most attention from companies and their auditors, since it has the most wide-reaching implications for the establishment of key internal financial controls. These key controls will need to meet five general characteristics:

- They are documented and repeatable formal processes.
- They provide clear ownership, with demonstrated accountability, of processes and functions.
- They are both high level and address specific compliance requirements.
- They are based on well-defined segregation of duties.
- They provide supporting reports, data feeds, and documentation of approvals.

Achieving this level of financial control is dependent to a great extent on the control characteristics of the underlying computer and other IT systems that support financial reporting systems. In order to successfully meet SOX financial reporting mandates, these IT systems generally require controls such as:

- Access control — or who can access applications and what they are authorized or able to do.
- Change control — when there are changes made to an application or database, has it gone through an appropriate level of review and testing before being introduced into a production environment?
- Backup and recovery — SOX and other regulations have increased the amount of time businesses are required to save transaction and financial data. Auditors are currently required to save data for

seven years, and many are pushing their clients to do the same. Auditors will want to know if data is being backed up securely and adequately and what provisions have been made for recovery. Therefore, maintaining data in spreadsheets and other desktop applications will probably no longer suffice for many business units. Instead, these units will be required to adopt data backup strategies that automatically capture and retain data in centralized applications.

- General IT controls on how well applications and databases are managed and maintained and whether IT has the appropriate skills sets.

Manual versus automated system controls

SOX says little about the use of technology when it comes to establishing and reporting on key controls. A business can, for example, rely on completely manual procedures for monitoring the effectiveness of key controls. This will be an ongoing effort that requires the periodic review and testing of possibly thousands of key controls and vigilant attention paid to spreadsheets and voluminous paper reports. Both the internal costs of maintaining and reviewing, and the external auditing costs of such an effort, can be onerous. For example, testing the integrity of individual key controls may involve testing 60 or more events or transactions.

The alternative is to embed key controls whenever possible in applications through workflow automation, proactive notifications, and other types of business process management automation. With

systems-embedded controls, financial control activity is triggered by workflow tasks. Since workflows are predefined and automatically enforced, consistency in terms of how key controls are handled is guaranteed. And the workflow application itself provides an audit trail of transactions.

The initial expense of embedding key controls into application systems will be higher than taking a manual approach, but the value of such controls will probably be greater over the long run. In fact, auditors may ask two questions of any control in evaluating its effectiveness: Is it manual or automated? Is it preventative or detective (in other words, does it allow you to uncover a lapse in financial compliance only after it happens)? To auditors, the controls with the least value in terms of their effectiveness versus the level of effort required to monitor them are generally controls that are manual and detective. The highest value controls are those that are both automated and preventative.

Lessons learned

By mid 2005, accelerated SOX 404 filers (businesses with a market cap of more than \$75 million) had completed “year 1” of Section 404 by assessing their internal controls over financial reporting. The majority had placed a high reliance on manual controls to support their assertion of adequate controls.

The cost and effort involved has not been trivial. A survey by the International Data Corporation put the average cost of effort at \$2 million to \$8 million for companies with less than \$5 billion in revenues. For companies of all sizes, the process took between 12 and 18 months. Much of the cost was consumed by outside consulting and auditing fees, which rose by 51 percent to 82 percent for companies included in the survey. After this assessment, the ongoing costs of monitoring and controlling SOX compliance requirements were projected to equal 0.15% per billion dollars of revenue, with mid-market companies paying a higher ratio of expense to revenue. This presumed that companies continued to use the same largely manual processes of internal control.

Two things were common among companies that completed the projects: costs were underestimated and projects took far longer than anticipated.¹ The unexpectedly high costs and time required to do initial SOX assessments stemmed from what many businesses discovered about their financial reporting and controls — they touched on thousands of points of contact within the organization and were often documented inconsistently in non-standardized spreadsheets and other documents.

One CFO summed up the experience by saying “A post-mortem of [our] Sarbanes-Oxley compliance efforts, looking at what worked and didn’t work, found inconsistent documentation of financial controls, as well as ones that should have been automated. Among the lessons learned is that standardization of processes minimizes the risk of misstatements on financial reports.”²

Recent trends in IT also contributed to the challenge. During the 1990s, many businesses centralized enterprise applications into monolithic ERP systems. These served as central repositories for

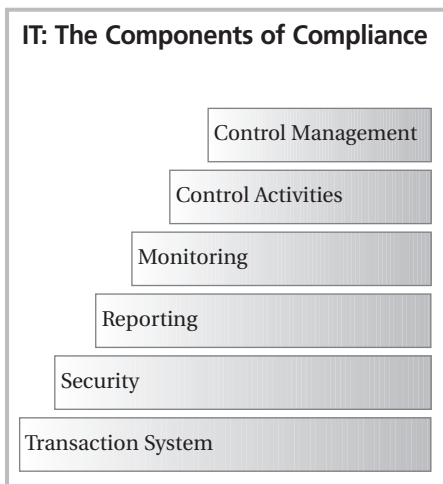
transaction and financial data. This rapidly gave way in recent years to a much more decentralized approach in which individual business units adopted their own “best of breed” solutions, thanks to the ability of web services and other new technologies to integrate disparate applications and systems into enterprise IT infrastructures. Most businesses have reaped huge benefits from the trend, but one unforeseen result is that during Section 404 audits, many businesses discovered that material transaction and financial data resided in a plethora of applications, some of which corporate offices didn’t even know existed. Rolling up all this data into the single enterprise-wide views needed to document controls proved one of the most time-consuming aspects of SOX projects.

¹Donald Nicolaisen, Chief Account, SEC, November 12, 2004, BNA Daily Report for Executives

²Chris McWilton, CFO, MasterCard, Information Week, March 21, 2005.

IT: The Components of Compliance

COSO provides a framework in which to build general financial control systems and ensure their compliance with SOX provisions. The following section looks at the six IT processes and application systems contained within such a general financial framework and suggests how they interact with each other and fit together. It is based on the model shown below. Following the model are descriptions of the compliance-control characteristics required by each of these IT processes and application systems.



Transactions

The bedrock of compliance systems are core accounting applications that manage the transactions that flow through the enterprise. There are often multiple transaction systems in use in the enterprise, especially if IT decision-making has been decentralized. The compliance requirements for transaction systems are unambiguous:

- Accuracy of financial entries
- A documented, testable and ultimately auditable connection between figures reported in financial reports and their original sources in transaction systems.

Security

This level refers to controls to secure transaction systems against fraud and abuse. These controls govern who has access to transaction systems to initiate, process, edit, or view transactions and also is authorized to grant access to other employees to enter, review or edit financial data. Most businesses have identified thousands of these controls and many are working to whittle these down to a smaller set of key controls that have a direct and material impact on financial reporting. In many businesses these controls are manual or at best semi-automated.

One important aspect of key controls for transaction security systems involves ensuring appropriate segregation of duties. Segregation of duties is intended to ensure that no single employee is authorized or has the ability to carry out all necessary steps of a process alone. This is most effectively accomplished by system security settings that limit any employee from handling too many steps in the processing of a single transaction. To use a simple example, proper segregation of duties would prevent the same employee from setting up fictitious vendors or accounts, creating purchase orders, and then authorizing and issuing payment of invoices.

Enforcing segregation of duties is harder in smaller companies, where employees may be required to wear several hats. For example, in a small accounts payable department, there simply may not be enough resources to separate check authorization and check issuance between different employees. For this reason lawmakers and regulators have extended

the deadlines for SOX reporting several times, but all affected companies, regardless of size, will be required as part of the public filing process to issue management reports and independently audited reports in 2006 detailing separation of duties provisions.

Reporting

So far, this white paper has discussed requirements to secure base financial numbers in transaction systems and implement controls that limit access to those systems. The reporting layer refers to how financial position and results are reported to managers, executives, and auditors. The reporting layer should be designed to ensure that the financial reporting information all parties see is directly derived from the same accurate and secure transactional data.

This is more of a challenge than it at first appears, especially in decentralized businesses that rely on loading transaction data into manually created and non-standardized spreadsheets to create financial reports. It is very easy, for example, for two business units, each using spreadsheets containing different macros and data factors, to come up with different reporting results based on the same transaction data. Reconciling and centralizing this sometimes contradictory data is another reason why initial reviews of key controls proved such an onerous and expensive process for so many companies.

IT: The Components of Compliance, continued

Monitoring

The ideal situation for most businesses would be a monitoring process that is a dynamic and largely automated effort that identifies situations in the business that put compliance at risk or trigger compliance conflicts, alerts the appropriate personnel, and allows remedial action to be taken. Not all, but a significant number of the processes identified in Section 404 and 409 reviews, will need to be monitored in such a fashion. Identifying and reducing to optimal levels the processes that need to be monitored proved to be a substantial challenge during initial SOX assessments. Mid-market and larger companies often came up with tens of thousands of potential control points, only a fraction of which auditors considered as true key controls that require monitoring.

Control activities

Given the scope of the compliance challenge facing many businesses, reporting and monitoring processes will seldom be enough to create a complete compliance solution. Instead, businesses need to implement a layer that sits on top of transaction, security, reporting and monitoring systems, and which allows them to *control* control activities.

As with most of the controls built into the lower layers, this layer of control management will be software controlled. Most of these software-controlled activities will focus on security, process and auditing requirements in workflow applications that govern business processes that contain pre-set limits, thresholds, and sequences of events.

Control management

The final layer sits on top of all other activities. Compliance is a complex, enterprise-wide, and ongoing project, and as such it needs a project management software layer that brings together all the components discussed above.

Control management is not about enforcing compliance (unlike previous components). Rather, compliance management is a tool that centralizes the information you need to manage compliance documentation, testing and reporting. In 2002 and 2003, a number of software vendors developed “compliance management” solutions that few companies actually purchased, since during the period the true implications of SOX compliance weren’t completely understood, and these solutions often failed to adequately integrate with the layers discussed above. Most utilize

a web portal and some sort of graphical dashboard that collects, categorizes and summarizes control activities from the layers discussed above, and allows internal and external auditors to see how compliance processes are documented, when and how to test those processes, and take action when needed.

A good control management solution will focus on four areas:

Documentation. With a central repository of all compliance-related information that is accessible to auditors and compliance managers, and is updated in as close to real time as possible.

Testing. With a running centralized tally of testing efforts, showing what was tested and by whom, testing results, and remedial actions taken when testing failed.

User interface. That promotes all key information regarding the control environment to everyone within the organization through a completely self-evident, secured, and user-defined portal.

Monitoring. That enables organizations to monitor key events/transactions within financial and ERP applications and immediately present any significant or material events to the appropriate audience.

Getting control under control

In creating and managing a compliance system that encompasses the six layers described above, businesses have several choices. They can rely on manual processes and controls that require constant communication among employees. They can combine manual processes and controls with automation — for example, an event that happens in one application may automatically trigger an e-mail to a manager, but subsequent action depends on the initiative of the manager. Or they can automate virtually all key controls of compliance by putting them under software control.

The third option isn't as complicated as it sounds. The keys are electronic workflow automation and proactive notifications.

Electronic workflow automation is based on the concept of graphical workflow mapping through the use of process control engines built into financial accounting and/or ERP software

applications. In the Sarbanes-Oxley environment, workflow products can play a major role in helping to both document and control business processes. A properly configured workflow tool not only provides documentation — which by definition must be accurate — but also enables many controls to be linked together in a defined sequence. How, when, and who completed a process can be tracked and reported. Most important, unlike manual or semi-automated procedures, employees can't "work around" electronic workflow applications that are set up and configured to authorize or block employee actions based on pre-defined employee roles and role responsibility.

A relatively new software technology, proactive (or "smart") notification streamlines the process of identifying and responding to compliance risks and material events. It is based on the concept of building triggers into workflow

automation processes that monitor data sources and automatically notify others in the enterprise when potentially material events or other compliance risks occur. This notification is typically linked to employee e-mail in-baskets or personal digital devices (PDAs). As part of the notification process, employees are told not only what happened, but also why, and are provided the relevant course of actions.

Assessing technology options

By now, most businesses affected by SOX and other financial regulations have completed their initial assessments of internal controls and processes or are well on their way. Among other things, these audits probably revealed:

- Where spreadsheets have become key to your financial processes. As previously suggested, spreadsheets can be a significant challenge to ensuring an effective compliance solution.
- Where systems not implemented by the central IT function have become key concerns in the compliance challenge.
- Critical third party systems — i.e., where you have outsourced part of your transaction and financials processes to another company. If these processes are material to the business, auditors will require companies to ensure that equivalent levels of controls are applied to the processes of these third party suppliers as if they were handled in-house.

What about the weak spots you've found in your financial controls? Three considerations will apply:

Should you retain existing processes?

In many cases, the answer will be yes, but additional controls will be needed. Software-based automatic controls implemented through electronic workflow are preferable, since they provide the consistent application of other system-based controls, are easier to implement, are preventative, and are less expensive to maintain in the long run.

Can existing processes be optimized?

Again the answer is probably yes. The focus should be on replacing manual steps by automated workflows to improve compliance and streamline monitoring.

Can existing systems be simplified?

Simple systems fail less often, so the fewer key controls you identify the better. This requires a process of first identifying a broad array of potential control points in your financial systems — initially there could be thousands — and whittling them down to only those that actually materially impact financial and compliance reporting and auditing requirements.

Making choices

SOX is forcing many companies to change the way they do business. This virtually always involves changing existing IT solutions to eliminate manual processes, automate compliance-related workflow, and develop new reporting and auditing systems required by regulators and auditors.

Some businesses may be evaluating entirely new compliance management solutions, but most are seeking a middle ground by combining new technology with existing systems. Regardless of your strategy, both new applications and modified or upgraded existing applications should include:

Comprehensive business and compliance functionality

Key features to look for in these applications as they pertain to compliance requirements include whistle blower functionality, single sign-on, and integration with your current security solution

Works with your current document management solutions

Whatever choices you make about compliance management solutions, it is important to determine if new technology will easily plug into your current document management solutions, since this plays such a central role in the compliance process. SOX technology should simplify the document management challenge, not compound it. Some SOX compliance management solutions rely on proprietary components of the supplier's technology stack, which in the end may prove to be more trouble than it's worth.

Control processes through automated workflows

Your existing workflows may be manual, semi-automated or automated, but many of them will inevitably change as a result of the compliance requirements you've identified during your initial SOX assessment. As noted, automated workflows are generally the best way to streamline and control compliance processes in businesses that have hundreds or thousands of key control points. Processes that are 'workflowed' are self-documenting and provide clear documentation for auditing. They can also make use of proactive notifications. Maybe more important, they can build in automated provisions to enforce segregation of duties.

Assessing technology options, continued

Automated workflows can also serve as a cornerstone of good corporate governance. They formalize and automate “best practices” across a broad spectrum of activities, from spending limits to security measures, and strengthen fiscal and operational accountability.

Questions to ask include whether existing automated workflows can be set up and configured, using concepts such as role- and rule-based security, to meet new compliance requirements, or if a new workflow system has to be superimposed on top of existing workflows. The latter option may prove to be an expensive and disruptive proposition.

Reporting and monitoring

Any new application has to fit under your current reporting strategy — your users want the same tool and the same location for all reports.

Facilitating collaboration

How easy is it to e-mail URLs to other users? To link other people to monitoring systems or test results? To communicate across application boundaries?

Tight integration

When business applications connect multiple functional areas, such as HR, payroll, finance, and procurement, you get not only more accurate and complete data, but better control through the ability to keep processes within corporate compliance parameters.

Flexible, open architecture

Compliance management solutions should enable easy customization, especially important in building workflows and key controls, and interface readily with legacy or best-of-breed systems.

Single source of employee data

This improves data accuracy through a single database; changes are made in one location, and the system feeds the changes to other applications.

Digital dashboards

These support efforts to stay on top of emerging material situations through “on-demand,” highly graphical data viewing systems.

Drill-down capabilities

These help uncover detailed information — a more complete story — behind transactions and data.

System security

Compliance may depend on your ability to set up applications to prevent unauthorized access through role-based access to systems and facilities. This access should be based on position, not the individual. Other important characteristics include single sign-on to multiple applications; automated sign-off at predetermined levels of inactivity; and the granting and removal of access privileges triggered by hires, terminations, and leaves of absence.

Change notifications

These automatically alert appropriate parties (employees, managers, payroll, finance, IT, building security, etc.) upon completion of certain employee lifecycle events, such as hiring, terminations, and leaves of absence, while generating documentation of these events.

Manager and employee self-service

These provide a mechanism for launching automated, documented workflows, such as purchase order issuance and invoice payment

Management by exception

This notifies staff as material issues arise, supporting proactive intervention and timely reporting.

Automated, on-demand reports

These should cover such critical areas as credit limits, accounts payable, vendor payments, compensation, payroll, and stock options.

Customized data feeds to vendors

These should address the integrity of data connections (e.g. accurate information going to the right vendor or outsourcer at the right time) and the security of data itself.

Benefits beyond compliance

SOX 404 and 409 require businesses to apply the process controls discipline they've longed used in manufacturing, supply chain management and other areas to financial statements.³ The benefits of taking this approach extend far beyond merely improving the reliability of financial reporting or meeting mandated compliance requirements. As businesses deconstruct their financial controls, analyze the risks and weaknesses of these controls, streamline and simplify when redundancies and overlaps are revealed, and put their controls back together in a more documentable, testable and repeatable fashion, many have noted that the inevitable fallout includes:

- Greater understanding and insight into business process and transaction flows. This new awareness shouldn't be wasted. Instead, businesses can use SOX as a springboard for improving process efficiencies throughout the enterprise. The key driver of success in these efforts will be technology that allows processes to be documented and managed through automated and centrally controlled workflows.
- A window into performance metrics. With SOX compliance, performance metrics are bound to improve, since businesses will have far more extensive, real-time and consistent ways to measure their performance. The same transaction and financial data that goes into SOX controls can also be applied to key performance indicators and business intelligence applications.
- Uncovering and rolling out pockets of best practices. SOX requires the kind of self-examination that few if any businesses have undertaken in the past. As part of this journey of discovery, businesses may unearth pockets of process excellence that previously were little noticed beyond the confines of particular departments or units. Since a key component of SOX compliance efforts is the documentation and testing of processes, outstanding processes that appear to have enterprise-wide benefits are virtually ready-made for rolling out to other parts of the business.

About the Author

Mr. Ostler joined Lawson in 2003, bringing 20 years of finance and operations experience with leading companies including Ecolab and Koch Industries, where he held a variety of leadership roles. Mr. Ostler lead Lawson's SOX 404 "Year 1" compliance program and current efforts to drive value through optimized internal controls. He holds a BA in Accounting from Weber State University, and is a Certified Public Accountant.

³Jeffery Immelt, GE CEO, GE 2004 Annual Report, 2/11/05.

For information on how Lawson® Financial solutions can support regulatory compliance and operational excellence, please visit www.lawson.com.

Corporate Headquarters
380 Saint Peter Street
Saint Paul, MN 55102
United States
651-767-7000



www.lawson.com

International Headquarters
Box 596 (Vendevägen 89)
SE-182 15 Danderyd
Stockholm, Sweden
+46 (0)8 5552 5000

Notice: The content of this white paper is based on information reasonably available to Lawson, and may include the opinions of Lawson or other persons. This white paper does not create or amend any contractual obligations or warranties. Information contained herein is subject to change without notice.

Lawson, Lawson Software, and the Lawson logo are trademarks of Lawson Software, Inc. Other product or services names mentioned may be trademarks of Lawson or the respective owners of those trademarks.

Copyright ©2006 Lawson Software, Inc. All rights reserved. EEO/AA SFIN-WP1000 0406