

BasWare

Sarbanes Oxley and The Procure-to-Pay Process

For US and Non-US based Companies

Stout Causey Consulting

White Paper

Copyright

Copyright © 2006 BasWare Corporation. All rights reserved. BasWare is a registered trademark of BasWare Corporation. Other product names mentioned may be trademarks of BasWare or the property of their respective owners.

Comments

All comments to this document can be addressed to BasWare Product Marketing mailbox@basware.com.

BasWare Corporation

Address: Linnoitustie 2, Cello Building, FIN-Espoo, Finland

Postal address: P.O. Box 97, FIN-02601 Espoo, Finland

Tel. +358 9 8791 71

Fax: +358 9 8791 7297

www.basware.com

About Stout Causey

Stout Causey is an internationally acclaimed CPA and management consulting firm, with service lines specializing in financial and internal control consulting (including Sarbanes-Oxley and IT audit services), Unclaimed Property Services, procure-to-pay consulting, mergers and acquisitions, technology implementations, and tax consulting. We offer practical and cost-effective business and software tools that streamline business processes offering immediate cost savings. Our staff of former “Big Four” auditors, CPAs, CISAs, former chief auditors, and tax experts will respond to your company’s needs swiftly and without the “Big Four” price tag. Our professionals document and test controls, remediate internal control deficiencies, and implement controls to minimize financial leakage. Stout Causey serves a large client base ranging from emerging businesses to the largest Fortune 500 companies.

www.stoutcausey.com

Tel. 410-403-1600

Table of Contents

1	Summary	4
2	Sarbanes Oxley – A General Overview.....	5
3	Sarbanes Oxley and Non-US Companies	6
4	Procure-to-pay and Sarbanes Oxley	8
	4.1 Risk Assessment.....	8
	4.2 Segregation of Duties.....	9
	4.3 Duplicate Payments	11
	4.4 Payment Coding and Timing.....	11
	4.5 Fraud.....	12
5	Cost of Compliance	12
6	Cost of Non-Compliance.....	13
7	Controlling the Cost of Compliance	13
	7.1 Compliance Strategy.....	14
	7.2 Software Solutions	14
8	References	15

1 Summary

This paper provides a brief introduction to the Sarbanes Oxley (SOX) Act of 2002 and its impact on the procure-to-pay process of both US and non-US-based companies. The Sarbanes Oxley Act of 2002 was enacted by the US congress as a result of situations that emerged from bookkeeping and business scandals at the time. The intent of the SOX act is to strengthen corporate governance, make senior level executives personally responsible for ensuring accurate financial reporting by their companies, and restore investor confidence related to the accuracy and full disclosure of companies' financial statements. While all US-based corporations that submit Securities and Exchange Commission (SEC) filings are required to adhere to the regulations prescribed by the Sarbanes Oxley Act (requiring new auditing, monitoring and risk management practices), non-US based companies that submit filings to the SEC are also subject to the provisions of the Sarbanes Oxley Act of 2002. Additionally, many non-US based companies with no official ties to the SEC may be required to conform to certain segments of the Sarbanes Oxley Act as requested by their clients or by the capital markets.

2 Sarbanes Oxley – A General Overview

In December of 2001 a fraudulent Enron Corporation filed for bankruptcy, causing investors to lose as much as \$25 billion. In June of 2002, owing to fraud, Adelphia Communications filed for bankruptcy, causing investors to lose as much as \$60 billion. In July of 2002 WorldCom, Inc. filed the largest bankruptcy protection petition in United States history; as a result investors lost as much as \$200 billion. In response to heavy political pressures and declining investor confidence the Sarbanes-Oxley Act (the “Act”) of 2002 was signed into law by President Bush on July 30, 2002. The Act applies to any securities issuer, including non-US based companies, and contains specific provisions and public policy changes designed to protect investors by improving the accuracy and reliability of corporate disclosure. Additionally, the Act gives the Securities and Exchange Commission (the “SEC”) the authority to regulate and enforce the Act. Simply put, the Sarbanes Oxley Act was designed to clean up corporate governance in any company that is required to file reports with the SEC, regardless of size or country of incorporation.

The Act is divided into a number of sections that outline the newly created responsibilities of companies. The sections that have relevance to the Procure-to-Pay process are:

- Section 409. This section requires that public companies disclose in “plain English” additional information concerning material changes in their financial condition or operations on a “real time” basis.
- Section 305. This section states that, if a company is required to restate its financial statements owing to noncompliance with securities laws, CEOs and CFOs must reimburse the company for any bonus or incentive or equity based compensation as well as for any profits realized from the sale of securities.
- Section 404. This section requires the inclusion of an internal control reports assessment. This report is designed to assess the effectiveness of the internal control structure and procedures for financial reporting. Internal controls development, documentation and testing include such areas as Accounts Payable and Information Technology. It is important to note that this section is a preventative section and while it is the most costly and time consuming section, if properly performed it will reduce the likelihood of noncompliance.
- Section 203. This portion of the Act mandates rotation every five years of both the lead audit partner working for the audit client and the audit partner responsible for reviewing the audit. Additionally, both lead and concurring audit partners shall abide by a five year time-

out period after rotation. Also, Title II of the Act requests rotation after 7 years with a two year time-out for all other audit partners who have significant decision making responsibilities.

- Section 302: This section requires CEO's and CFO's to personally certify company SEC periodic reports, with possible criminal and civil penalties for false statements. Additionally, sections of the Sarbanes Oxley Act outline the penalties for executive officers, which may lead up to 25 years in prison and penalties of up to \$25 million.

Additionally, as a part of the Sarbanes Oxley Act of 2002, the SEC has received an additional \$98 million to hire at least 200 employees to provide enhanced oversight for auditors and audit services. The US government's renewed focus on corporate compliance should not be taken lightly. This broad reaching Act affects not only US domestic companies but all companies that have any relation with the SEC as well as companies that act as major suppliers to US corporations.

3 Sarbanes Oxley and Non-US Companies

The Act has far reaching implications, not only for US companies but for foreign companies as well. There are three distinct types of non-US based companies that are affected by the Act. The first are companies that have securities or debt filings with the SEC. These non-US based companies are required to include in their annual reporting, beginning with year-ends on or after July 15, 2006, an internal control report from management which includes:

- A statement acknowledging management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting;
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over financial

reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting; and

- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting.

Additionally, as with US-based companies, management of foreign companies with SEC filings must personally certify statements.

The second type of non-US-based company that may be subject to Sarbanes Oxley compliance is organizations that are looking for financing from venture capitalists. Venture capitalists are increasingly using SOX compliance as part of their due diligence tool kit. With an ultimate goal of filing for a public offering, venture capitalists are looking to reduce issues at IPO time.

The third type of non-US-based company that may be subject to Sarbanes Oxley compliance is any non-US-based company doing business in the United States. Increasingly, many US companies are fully leveraging the practices prescribed by the Act and are implementing many of these same practices across their entire organization, and are forcing their non-US-based suppliers to do the same.

From a risks and liabilities perspective, SOX legislation forces US companies to have their external suppliers and, in many instances, customers comply with the legislation. From a pure risk management perspective, this is pushing companies to adopt a bottom-up way of thinking when it comes to compliance. Understandably, this is also having a significant impact on the purchase to pay process.

The Act has largely ignored differences in practices and corporate governance policies between the United States and other countries. As a result, non-US based companies face many of the same challenges US companies face in addition to their own country's governance regulations. For example European based companies with SEC filings will now have to coordinate multiple financial control standards including the International Financial Reporting Standards ("IFRS"), Sarbanes Oxley, and any other national financial controls regulations. Additionally, non-US based companies have the added complexity of assessing internal controls in multiple geographical locations, and the monitoring of controls in complex, multiple location environments.

4 Procure-to-pay and Sarbanes Oxley

The procure-to-pay process has traditionally been seen as a cost center. Not only do companies have to pay for goods and services received, but they have to pay for the payment of those same goods and services. Despite the inherent risks and increasing costs associated with processing check payments the creation, enforcement, and monitoring of internal controls for the procure-to-pay process have largely been ignored. With the introduction of the Sarbanes Oxley Act (the "Act"), the federal government has ensured that the procure-to-pay process will no longer be disregarded. Within the procure-to-pay process, the areas at greatest risk for control deficiencies are the segregation of duties, duplicate payments, coding error, and fraud. Of course, before companies can address these or any other risks, a complete risk assessment must be completed.

4.1 Risk Assessment

Performing a risk assessment is one of the first steps in creating a culture of transparency. Ultimately, the goal is to create, monitor, and enforce internal controls designed to mitigate risks to critical assets. Any implementation of internal controls without first identifying the critical assets exposed to risk may result in a loss of focus when creating internal controls. For a complete and accurate risk assessment, it is important for non-US based companies to ensure that Sarbanes Oxley regulations are not overlooked. Without taking Sarbanes Oxley regulations into consideration, many Accounts Payable organizations may realize they face substantial risks in a number of processes they previously thought of as secure.

For example, many organizations are performing three-way matching on invoices and believe, because they are doing so, they are safe in terms of compliance. Unfortunately, in reality, many invoices are missing key data (often as many as 30% to 50 %) and thus, the matching rate is actually closer to 0%. In order to reduce the significant risks related to material deficiencies, monetary losses, fraud attempts, etc., companies should implement a five-way matching process where invoices go through an automated five-step-test (Invoice to Purchase Order to goods received to delivery confirmation acceptance (quality inspection) to Approval audit trail/Posting) before automatically being routed to the correct place. Another area which may constitute a deficiency, as pointed out by the Act, is the lack of monthly account reconciliation of all significant accounts. This not only applies to significant customer accounts but significant vendor accounts as well. The only practical, cost-effective way to accomplish the above requirements is with an automated solution.

It should be noted that there are number of factors which impact the deficiency levels identified in any risk assessment. Such factors include causes and frequency of exceptions as well as any future consequences as a result of those exceptions. For example, a low degree of confidence in

determining certain figures, such as unrecorded liabilities, carries a significant level of risk and should be mitigated as quickly as possible.

We have all heard that you can not manage or control, what you can not measure. The only way to provide accurate, timely risk assessment reporting, (i.e. cash pipeline/accrual, quantify unrecorded liabilities, accurately forecast cash flow requirements) is with a good automated solution with robust reporting. This will enable your organization to raise awareness of current performance, allowing decision makers to be proactive. In addition, improved transparency will also provide many additional value-added benefits to your organization.

4.2 Segregation of Duties

For many companies the segregation of duties in and around functions related to the procure-to-pay process is an area of high risk. Though the IFRS considers the segregation of duties an essential part of internal controls, it does not go far enough. The European Commission's Central Financial Service, Document 3, titled "Financial Procedures and Control Systems (December 2000) states: "The operational and financial aspects of each transaction shall be checked by two people who are independent of each other [i.e. not subordinate to each other]. The functions of initiation and verification of each transaction shall be kept separate". Sarbanes Oxley goes even further, requiring that duties be segregated not only along operational and financial lines, but across data access controls as well. Additionally, Sarbanes Oxley ensures that the controls and processes to enforce proper segregation of duties are applied consistently, successfully, and reviewed and approved by an external auditor. Finally, even though the IFRS mandates segregation of duties, a recent survey shows that only 38% of European Union based corporations believe they have effectively separated duties at risk.

Another area of focus is vendor management. Many companies combine the functions of vendor negotiation, management/maintenance, and accounts payable. However, in order to ensure Sarbanes Oxley compliance, segregation of supplier maintenance and contract management functions is essential. Additionally, persons who are authorized to negotiate supplier contracts should not be the same individuals that are responsible for supplier maintenance or monitoring. Lastly, it is important that employees responsible for posting invoices not be the same employees responsible for vendor maintenance/set-up functionality. More important than vendor management is the separation of purchase order, order receiving, invoice entry, invoice approval, cash disbursement, invoice administration and data administration functions. These functions are strictly controlled and there must be a clear and logical separation of duties in order for organizations to comply with Sarbanes Oxley guidelines. For example, a typical exception identified during an audit is when employees who approve invoices for payment also have the ability to setup and maintain vendors. Another common exception is to combine the functions of order receiving and invoice

entry. Initially it seems logical that invoices delivered with goods or services should be entered by the individual receiving the goods – thereby streamlining the process. This scenario, however, creates opportunities for fraudulent activities. An individual with control over both goods receipt and invoice entry functions could easily enter invoices without actually receiving goods.

Many organizations have a very informal culture which may lead to material deficiencies in the invoice approval process. For example, organizations that do not have a formal structure in place to segregate and approve invoices in a hierarchical manner may be exposing deficiencies. In order to ensure Sarbanes Oxley compliance there should be multiple levels of approval across the company with maximum dollar amounts in place and an effective system to ensure such compliance. This is more commonly known as an approval matrix. The matrix should have sufficient detail to ensure that a conflict of interest is not inherent. The matrix should include such things as: who is responsible for issuing and approving purchase orders; who is authorized to enter and approve invoices, and who is responsible for preparing, signing, and mailing checks. For your benefit a sample invoice approval matrix is included in the appendix.

In addition to the development of an approval matrix, a system that reduces the likelihood of a conflict of interest must be in place to ensure the approval matrix is strictly observed. Such a system can be thought of as a workflow. The idea of a workflow system typically conjures up thoughts of an expensive, complex, and convoluted process. In fact, a workflow is simply the management of a series of steps in a business process. It can be as simple as ensuring that all invoices received are first approved by the head of the placing department, then by Accounts Payable. Or, it can be as complex as passing a purchase order through multiple pre-approval steps before committing to a final approval. The key, though, is that an effective workflow system should be flexible, easy to maintain, and enforceable.

Beyond the development of controls and processes to define the segregation of duties, a method of enforcement must be in place. Many companies utilize manual controls and procedures to enforce company policy. This is a highly ineffective approach as manual controls are difficult to enforce and monitor. Consequently, companies who have significant Accounts Payable spending may encounter significant deficiencies or even material weakness if their manual processes are not appropriately enforced and monitored. Alternatively, organizations that are able to effectively monitor and enforce their manual controls require staff and resources that are above and beyond what they should be spending. In order to mitigate these deficiencies many organizations have turned to automated solutions.

The requirements related to segregation of duties are certainly challenging but ways exist to facilitate their implementation. One such way is an automated solution, especially the so-called

packaged, or out-of-the-box, solutions. The most advanced packaged applications already contain many of the required best practices for the segregation of duties described previously.. Solutions related to vendor management, approval hierarchies and workflow, and controlling and monitoring access to financial data already exist and thus, can be of great assistance, when tackling compliance challenges.

4.3 Duplicate Payments

On average, the error rates for vendor payments are approximately 1.6 percent, of which almost 30% can be attributed to duplicate payments. For many Accounts Payable departments duplicate payments are typically processed due to rush or late payments. Others create duplicate payments by paying on invoice copies or statements. This problem is particularly prevalent in manufacturing, industrial, and advertising companies. As such, it is generally considered good practice not to process payment based on vendor statements or photocopies of invoices.

While duplicate payments are not specifically addressed in the Sarbanes Oxley Act, the Act requires controls to be in place to identify losses and to reflect those losses in financial reports.

4.4 Payment Coding and Timing

Many companies allow invoice approvals and the resultant account coding to be completed by the business units rather than the Accounts Payable department. As a result, opportunities for intentional, as well as accidental miscoding exist. For example, a common exception uncovered by an auditor may be that approval managers are transposing accounts numbers. While this seems like an innocent mistake, this scenario may lead to improperly categorizing inventory purchases as expense accounts. Another common problem which may affect companies relates to the timing of invoice entry. Since many European and US companies operate in multiple countries, it is possible that invoices are not submitted for processing in a timely manner. Consequently, expenses may not be categorized in the appropriate period, leading to potential material misstatement of accrued liabilities.

While the potential for improper payment coding and issues with payment timing exist, non-US based companies, and in particular, European companies, are particularly susceptible to deficiencies due to their geographical diversity.

The risks related to payment coding and timing, i.e. misstatement of accrued liabilities, are greatly reduced with more efficient and automated processes. Additionally, these automated processes

also enable month- or year-end closing (an indirect requirement of “full, fair, accurate and timely reporting” in Section 406) to be completed faster and more accurately.

4.5 Fraud

The Association of Certified Fraud Examiners reports that the typical organization loses 6% of its revenues to fraud. While everyone would like to believe that their organization is exempt from fraud, the fact of the matter is that the majority of fraud is perpetrated by internal employees. Unfortunately, for non-US based companies similar statistics apply. Indeed, non-US based companies face many of the same types of fraudulent activities as US based companies. Some of these include ‘phantom supplier’ fraud where fake vendors are created and paid and ‘timing difference’ fraud where expenses are not reported in the period in which they occur.

It is important to note that non-US based companies face greater challenges when attempting to prevent and detect fraud. IFRS gives organizations the flexibility to adopt controls and procedures relevant to their specific situations or environments. However, the Sarbanes Oxley Act attempts to standardize fraud detection and prevention activities. And, since the Sarbanes Oxley Act does not give specific exemptions to non-US based companies, they must find ways to normalize national, European Union, and Sarbanes Oxley methods of fraud detection and prevention.

One method of normalization is to automate, to the extent possible, controls and processes. In fact, in some cases, automation is all but required. For example, due to cultural differences, many non-US based companies will find that segregation of duties controls become very difficult to enforce without automated controls. Non-US based companies should understand that the central goal of the Sarbanes Oxley Act is the prevention and detection of fraud. Good intentions and a clean history are not enough to be Sarbanes Oxley compliant. Companies must invest the time and effort into performing a comprehensive risk assessment, identifying deficient controls, and developing a strategy to mitigate those deficiencies.

5 Cost of Compliance

The cost of Sarbanes Oxley compliance is significant. A recent study by Korn/Ferry International estimated that US based companies spend, on average, \$5 million for Sarbanes Oxley certification. Owing to, among other things, competing international financial standards, a Parson Consulting survey estimates that, on average, non-US based companies may have to spend even more, upwards of \$12 million, to achieve Sarbanes Oxley certification.

In terms of man hours, a recent study suggests that US based companies will spend at least 12,000 man hours to complete Sarbanes Oxley compliance. Extrapolating that number, non-US based companies can expect to spend upwards to 25,000 man hours for complete Sarbanes Oxley compliance.

6 Cost of Non-Compliance

The cost of non-compliance has extended well beyond the fuzzy boundaries of market conditions and perceptions. The financial consequences of payment errors, duplicate payments, and vendor and employee fraud can run into millions of dollars of losses per year. The consequences of non-compliance with increased regulatory requirements can be even more severe – with penalties such as harsh fines, negative publicity, and damage to investor and consumer confidence. The SEC has developed very strict guidelines for both US and non-US based companies with respect to penalties. The SEC allows for not only corporate fines but personal fines and punishments. CFOs and CEOs are personally liable for their company's SEC periodic reports and face criminal and civil penalties for filing false statements. And, of course, non-US filers and their managers are not exempt from the long reach of the US law. With respect to penalties, the Act does not contain any express exemptions for foreign issuers. As a result, the fines imposed on US corporations and their managers are the same fines imposed on non-US companies and their managers.

While the SEC imposes defined fines, the penalties for non-compliance can go beyond government sanctions. As corporations increasingly ask their vendors to become Sarbanes Oxley compliant, either in part or in whole, non-compliance may lead to a strategic disadvantage. Additionally, it is important to note that the market may impose penalties on non-compliant companies. For example, companies, US and non-US, that are considering merger activity will now have to perform additional due diligence to ensure target companies are Sarbanes Oxley compliant. Organization, documentation and above all, Sarbanes Oxley certification, will decrease due diligence costs and make for a more attractive target.

7 Controlling the Cost of Compliance

With staggering costs and great consequences for non-compliance, many companies are looking for ways to lower the cost of compliance. Non-US based companies can take advantage of the ideas and processes generated by their US counterparts to reduce Sarbanes Oxley compliance costs. The two most valuable ideas are the development of a compliance strategy and the implementation of software solutions.

7.1 Compliance Strategy

Developing a comprehensive compliance strategy prior to initiating a Sarbanes Oxley project is the proper approach. Since compliance for non-US companies is not set to begin until mid 2006, non-US companies can reduce their costs by developing their own compliance strategy based on the work of US companies. While it would be ill-advised to simply 'copy' the compliance strategy of a US company, non-US companies can be assured that reliable strategies have some commonality. Among those are: insisting that auditors be involved from the beginning of the process, developing a comprehensive risk assessment plan, ensuring that only auditable controls are tested and documented, remediation of deficient controls and processes as documentation progresses, and finally, making sure that compliance is approached as a process and not a one time project.

While developing ways to become compliant with SOX legislation, i.e. reporting, companies can also benefit from improvements in their overall business performance, as a result of achieving compliance. Similarly, when companies improve their processes and perform more efficiently, they become more compliant. While not the intent of the legislation, a case could be made that implementing compliance measures can help improve the overall business performance of an organization.

7.2 Software Solutions

Software solutions provide an ascertainable way of lowering the cost of compliance. Typically, the largest expense in developing Sarbanes Oxley compliance is the documentation and testing of internal controls. Automation of controls and processes streamlines documentation procedures and allows auditors to quickly and efficiently collect documentation. Additionally, the automation of controls and processes greatly reduces the number of controls an auditor must perform. On average, manual controls in a centralized environment require at least 8 hours per control to test. Automated controls require approximately 4 hours testing. The table below briefly describes potential time savings due to automated controls.

Description	Minimum Number of Items to Test
Manual control, performed many times per day	At least 25
Manual control, performed daily	At least 25
Manual control, performed weekly	At least 5
Manual control, performed monthly	At least 2
Manual control, performed quarterly	At least 2
Manual control, performed annually	Test Annually
Programmed control	Test 1 or 2 applications of each programmed control for each type of transaction.

The chart above indicates that a single manual control requires at least 200 (25 * 8) hours of testing where an automated control requires approximately 8 (4 * 2) hours of testing. When developing Sarbanes Oxley cost models and attempting to lower the cost of compliance it is

important to include return on investment calculations for automating controls and processes. For example, an automated invoice processing solution would not only help to reduce the time required for documentation and testing controls but would also help to reduce duplicate payments, lower the cost per transaction of a processed invoice, and increase invoice processing throughput.

Software solutions help to automate the most resource intensive parts of compliance requirements. The benefits derived from software solutions come from, amongst other things, the fact that SOX requires repeated testing and audits and it's difficult, if not impossible, to make these more efficient using manual procedures. Whether you are a US- or non-US-based public company required to comply with Sarbanes Oxley regulations or simply a non-US based company looking to implement Sarbanes Oxley in order to please your US-based customers, one of the most effective ways to reduce the cost of compliance encompasses process automation utilizing software solutions.

8 References

<http://images.jw.com/com/publications/220.pdf>

http://www.aicpa.org/info/sarbanes_oxley_summary.htm

http://www.deloitte.com/dtt/cda/doc/content/us_so_FPI%283%29.pdf

<http://www.fleetcapital.com/resources/capeyes/a01-03-139.html>

<http://www.charityvillage.com/cv/research/rlegal17.html>

<http://www.utoronto.ca/ams/news/103/html/103-7.htm>

<http://www.cfenet.com/home.asp>

http://www.dorsey.com/files/tbl_s21Publications%5CPDFUpload141%5C94%5C109%20Foreign%20Private%20Issuers-Sarbanes-Oxley%20Act%20020802.pdf

http://www.businessweek.com/bwdaily/dnflash/dec2004/nf20041215_9306_db016.htm?chan=adsections&sub=credit_management&campaign_id=knw_atradius

http://www.thelenreid.com/articles/article/art_135_idx.htm