

IT implications of Sarbanes-Oxley:

# challenge or opportunity?



in association with

Sarbanes-Oxley revealed companies that had:

- 2 million orphaned user access IDs
- 150,000 spreadsheets
- 100,000 control objectives
- 88,000 key controls
- 1,000 systems
- 29,000 controls tested
- 4,000 people involved in the programme

## The origins of this paper Business

Application Software Developers Association (BASDA) has formed a working party to specify the business application requirements for the introduction of the Sarbanes-Oxley Act. The working party has supported the BASDA Sarbanes-Oxley White Paper as a means of communicating the impact of the Sarbanes-Oxley Act to its members and their customers.

**Acknowledgements** Our thanks go to Peter Jones of Lawson Software, the Chairman of the working party, Richard Morley of Epicor, Sheila Brisland of Sage (UK) Ltd, Shelley Howard of SSA Global, Richard Anning of Systems Union, Del Attah of Zeraxis, Anton Ruddenklau and Andrew Broadhead of PricewaterhouseCoopers LLP who all contributed so much to this initiative.

The working party member organisations that took part in formulating this White Paper are: Epicor, Lawson, Sage (UK) Ltd, SSA Global, Systems Union, Zeraxis.

**Disclaimer** This White Paper is published without responsibility on the part of BASDA or the various contributors, sponsors or members of the BASDA Sarbanes-Oxley Working Party for any loss occasioned to any person acting or refraining from action as a result of any view expressed herein. BASDA cannot accept any responsibility and shall not be liable in contract, tort or otherwise, for the accuracy, completeness or otherwise, of this document, the extent to which it has been implemented by packaged software vendors, or any consequences or losses arising from the failure of software to meet Sarbanes-Oxley requirements. You are advised to take appropriate advice in order to determine the full implications of the introduction of Sarbanes-Oxley for your business.

**© Copyright BASDA 2005** All rights reserved. No part of this publication may be reproduced, stored in any retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of BASDA.

Additional copies of this document may be obtained from BASDA on +44 1494 677 699 at a price of GBP £50 per copy (£25.00 per copy to BASDA Members) - postage extra outside the UK.

Published by BASDA Ltd.,  
The Business Application Software Developers' Association Ltd.,  
Templestowe, Longbottom Lane, Seer Green, Beaconsfield,  
Buckinghamshire. HP9 2UL, United Kingdom.

[www.basda.org](http://www.basda.org)

## Contacts

**David Webb**  
(Public Sector)  
[david.a.webb@uk.pwc.com](mailto:david.a.webb@uk.pwc.com)  
020 7213 4395  
07834 519 012

**Sam Samaratunga**  
(Financial Services)  
[sam.samaratunga@uk.pwc.com](mailto:sam.samaratunga@uk.pwc.com)  
020 7804 3432  
07710 058 286

**Marc Bena**  
(Consumer Industrial Product Services)  
[marc.bena@uk.pwc.com](mailto:marc.bena@uk.pwc.com)  
020 7804 1125  
07713 162 721

**Andrew Broadhead**  
(Technology, InfoComms, Entertainment and Energy)  
[andrew.j.broadhead@uk.pwc.com](mailto:andrew.j.broadhead@uk.pwc.com)  
020 7212 4979  
07841 783 039

**Anton Ruddenklau**  
(Technology, InfoComms, Entertainment and Energy)  
[anton.ruddenklau@uk.pwc.com](mailto:anton.ruddenklau@uk.pwc.com)  
020 7213 1194  
07834 251 943

**Kersty Beaumont**  
(Wales and West)  
[kersty.beaumont@uk.pwc.com](mailto:kersty.beaumont@uk.pwc.com)  
0117 928 1282  
0780 1038 075

**Marco Amitrano**  
(South East)  
[marco.amitrano@uk.pwc.com](mailto:marco.amitrano@uk.pwc.com)  
01895 52 2386  
07739 449 214

**Elwyn Roberts**  
(Midlands)  
[elwyn.roberts@uk.pwc.com](mailto:elwyn.roberts@uk.pwc.com)  
0121 265 5069  
07710 397 783

**Andrew Winters**  
(Leeds / North East)  
[andrew.winters@uk.pwc.com](mailto:andrew.winters@uk.pwc.com)  
0113 288 2311  
0780 1038 084

**Marie Marland**  
(North West)  
[marie.t.marland@uk.pwc.com](mailto:marie.t.marland@uk.pwc.com)  
0161 245 2183  
07713 793 615

**Stephanie Bruce |**  
(Scotland)  
[stephanie.bruce@uk.pwc.com](mailto:stephanie.bruce@uk.pwc.com)  
0131 524 2376  
07711 685 137

“Sarbanes-Oxley has forever  
changed the relationship between  
the software user and their provider”

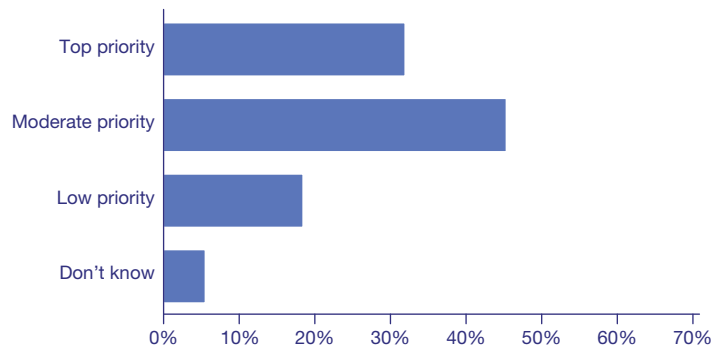
Richard Morley, Senior Manager, Product Marketing, Epicor

# Contents

Executive summary	7
What is Sarbanes-Oxley?	9
The Sarbanes-Oxley Implementation Challenge	11
Sarbanes-Oxley and IT	13
What have we learned from the Sarbanes-Oxley experience to date?	21
Choose a governance framework to work from	25
Integrate IT with Sarbanes-Oxley and the broader internal control agenda	27
Take an inventory of IT assets	29
Assess the impact on applications architecture	31
Address end-user computing	35
Understand how outsourcing is controlled	37
Appendices	39

**Figure 1: Senior finance executives say that automating compliance and control will be a high priority in the next year**

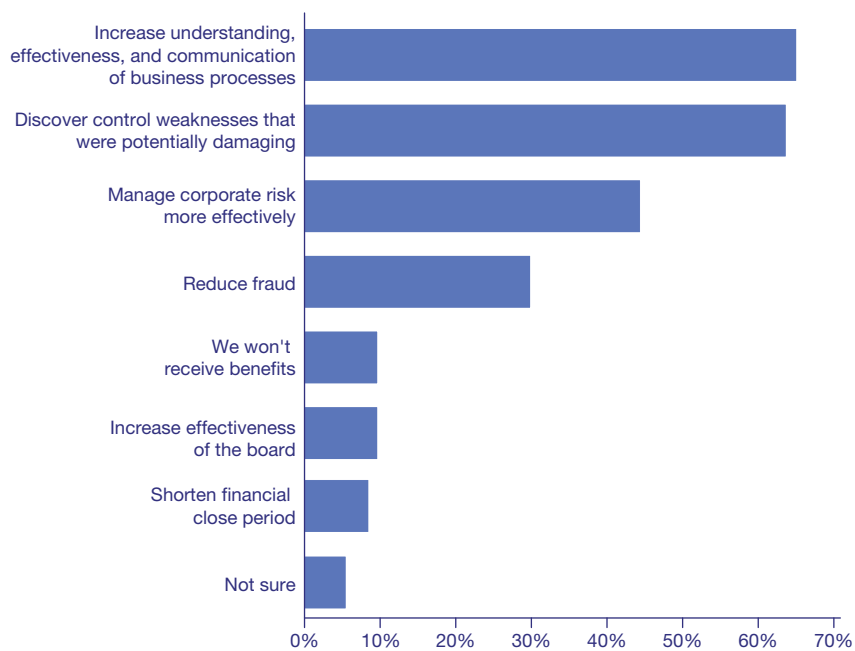
How high a priority will automating your compliance and control environment be in the next 12 months?



Source: PricewaterhouseCoopers, Virsa Systems, CFO Publishing survey, August 2005 Survey of 180 business executives

**Figure 2: Finance executives say operating benefits grow out of Sarbanes-Oxley compliance**

Which of the following benefits do you expect your company will receive as a result of complying with Sarbanes-Oxley?



Source: PricewaterhouseCoopers, Virsa Systems, CFO Publishing survey, August 2005 Survey of 180 business executives

# Executive Summary

The Sarbanes-Oxley Act of 2002, the US Congress's sweeping reaction to a series of corporate scandals, is having a profound effect on companies. Companies have been placed under the microscope like never before and this has provided an unparalleled insight into the quality of processes, controls and organisation in modern corporate business. Importantly valuable lessons have and are being learned that have implications for all companies, whether required to comply or not. The EU have not missed these outcomes either and are planning their own Audit Directive on Corporate Governance.

The US experience of Sarbanes-Oxley highlights a number of issues, risks and opportunities that are increasingly pressing for UK-based enterprises and application software developers. These issues are relevant not only to SEC (Securities and Exchange Commission) registrants, but to all companies – partly because many non-SEC registrants are choosing to adopt Sarbanes-Oxley-style processes because of the operating benefits they deliver in terms of process controls and management information (see Figure 2). Non-US companies with a US listing must now comply with the act for fiscal years ending after 15 July 2006.

Key trends that have emerged in the US and now UK include:

- Companies are becoming far more informed about the effectiveness of their business processes and controls and are starting to act on this information. Aiming for mere compliance effectively means much of the investment is wasted – it should also be used to improve management information, process effectiveness and control to enhance decision making
- The IT element of Sarbanes-Oxley compliance programmes has proved contentious and especially challenging. Many companies have uncovered overly complex, duplicative and fragmented systems and spreadsheet processes running in various parts of their organisation. Also, since the legislation does not differentiate between manual and automated controls, it has often been difficult for companies to decide exactly where to draw the line between the two. All too often, the result has been the creation of complex, overlapping layers of automated and manual control processes and reconciliations.
- The interrelation between Sarbanes-Oxley and IT has put the CIO at centre stage as never before. The transparency that this regulation has generated has created an environment for greater accountability and huge pressure to deliver greater RoI on IT spend. The appetite for the centralisation and standardisation of system infrastructures and the automation of processes and controls is growing as a consequence. See Figure 1.
- Finance Directors and Chief Executive Officers are looking for substantial reductions in the cost of compliance whilst minimising the risk of non-compliance at the same time. Sarbanes-Oxley is not a one-off, but an ongoing requirement and senior management are looking at how to sustain cost effective compliance not just with Sarbanes-Oxley but all forms of regulatory compliance.
- The problem can be summed up by quoting a common question from customers to application developers: 'Is this application Sarbanes-Oxley compliant?' There is no such thing as Sarbanes-Oxley complaint software, only compliant companies. The rules of the game have changed, and both customers and application providers need to adapt accordingly.

## The interrelation between Sarbanes-Oxley and IT has put the CIO at centre stage as never before

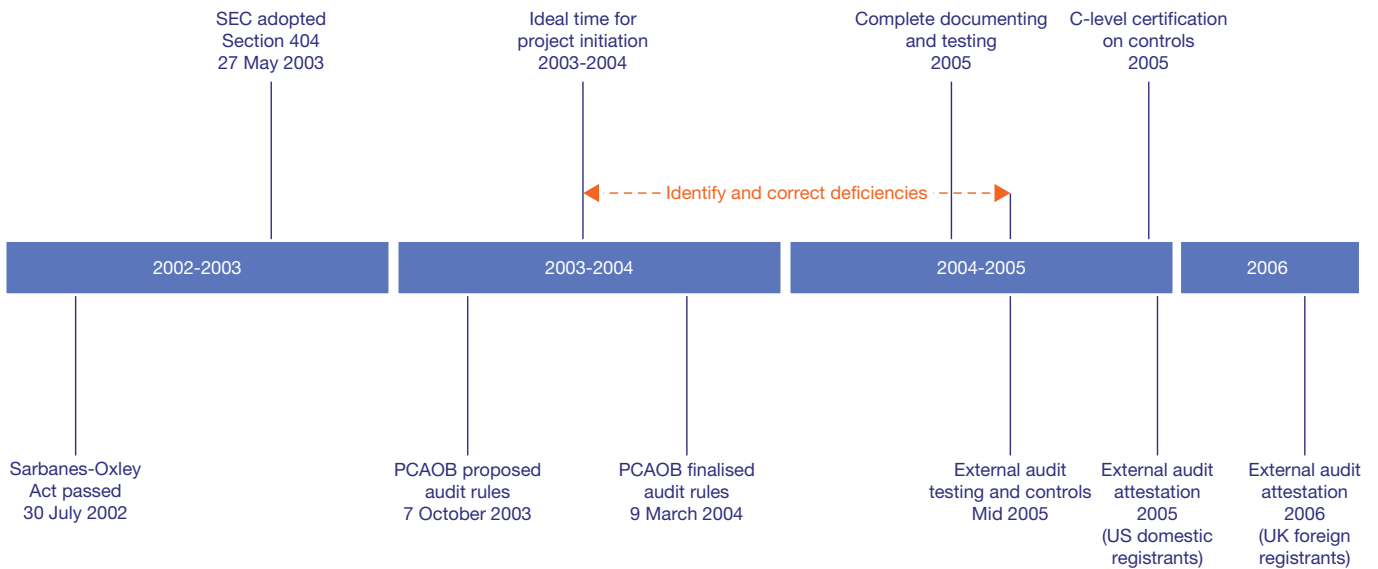
### Key messages for CIOs and Application Developers

At the end of each section of this report, we will list what we regard as some of the relevant key messages from that section for CIOs and for the sales directors of application software developers. These will help:

- CIOs to understand the implications of Sarbanes-Oxley for the role of IT in their business, distil the issues and provide a focus for responses.
- Application software developers to understand the implications of their customers' increased demand for centralisation and automation.

The experience of SEC registrants has highlighted a number of issues, risks and opportunities that are increasingly pressing for UK-based enterprises and application software developers.

Figure 3: Historical and future milestones



# What is Sarbanes-Oxley?

The Sarbanes-Oxley Act of 2002, which applies to all SEC-registered companies, was introduced by the US Congress as a response to the wave of scandals that rocked the USA's corporate landscape. Its primary purpose was to overhaul corporate transparency. The three-year timeline for compliance (shown in the diagram below), overseen by the newly-created Public Company Accounting Oversight Board (PCAOB), appeared to provide SEC-registered companies with adequate time to address the issues at first sight.

However, as companies got to grips with compliance it became obvious that the scale of the challenge had been underestimated. With Year One compliance in the US completed, it is clear that companies have been forced to scrutinise and, in many instances, substantially (or temporarily) upgrade their internal systems and controls. SOX 404, which places new obligations on companies to assess and report on the effectiveness of their internal controls has proved to be by far the most significant aspect of the Act where companies' IT systems are concerned. There are, however, other sections of the Act that are also applicable, and these are summarised below:

## SOX 302

### Corporate Responsibility for Financial Reports

Quarterly and annual filings must contain a certification that the CEO and CFO have performed an evaluation of the design and effectiveness of the disclosure controls. Certifying executives must state that they have disclosed to their audit committee and independent auditor any significant control deficiencies, material weaknesses or acts of fraud, and significant changes in financial reporting internal controls.

## SOX 404

### Management Assessment of Internal Controls

Companies must perform an annual evaluation of internal controls over financial reporting and a quarterly evaluation of any material change in the company's internal controls over financial reporting that occurred during the fiscal quarter. Annual filings must contain a report of management on their assessment of the effectiveness of internal controls over financial reporting.

## SOX 409

### Real-Time Disclosure

Companies must disclose information on material changes in the financial condition or operations of the Company on a rapid and current basis. The enforcement of 409 lies directly with the SEC, which has added a number of events to the existing list that would necessitate an 8-K filing now due within 4, instead of 14, business days. These events include entry into, amendment, or termination of a material definitive agreement outside the ordinary course of business; costs associated with the exit or disposal of long-lived assets or employee reductions; and material impairment charges to assets.

### Key terms: a primer

The profound impact of Sarbanes-Oxley has altered the definitions of certain key terms, as well as spawning some new ones. Following are some useful definitions:

- **Internal control over financial reporting** – focuses on policies and procedures that pertain to reliable financial reporting. This is obviously narrower in scope than the term 'internal control' on its own which would also encompass things such as the effectiveness and efficiency of operations and compliance with laws and regulations. The dilemma for companies is to judge which controls can impact the reliability of financial reporting.
- **Frameworks for assessment** – both management and the auditor are required to base their assessments on a suitable recognised control framework such as the framework developed by the Committee of Sponsoring Organisations (COSO) of the Treadway Commission.
- **Types of deficiencies** – if any deficiencies are identified, both management and the auditor are required to determine if they are a 'significant deficiency' or, more serious, a 'material weakness'.
- **Significant deficiency** – a control deficiency that adversely affects the company's ability to initiate, authorise, record, process or report external financial data reliably in accordance with GAAP. It could result in "more than a remote likelihood that a more than inconsequential misstatement of the annual or interim financial statements will not be prevented or detected." This type of deficiency does not have to be publicly reported, but it is reported to the audit committee.
- **Material weakness** – where there is a "more than remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected." This type of deficiency has to be publicly reported.
- **Aggregation of deficiencies** – s404 also includes a concept where companies must look at individual deficiencies to see how they might interact with each other. A combination of deficiencies might individually not be significant, but together they might rise to the level of a material weakness.

Figure 4. Diagram of key elements in Sarbanes-Oxley project management and implementation planning

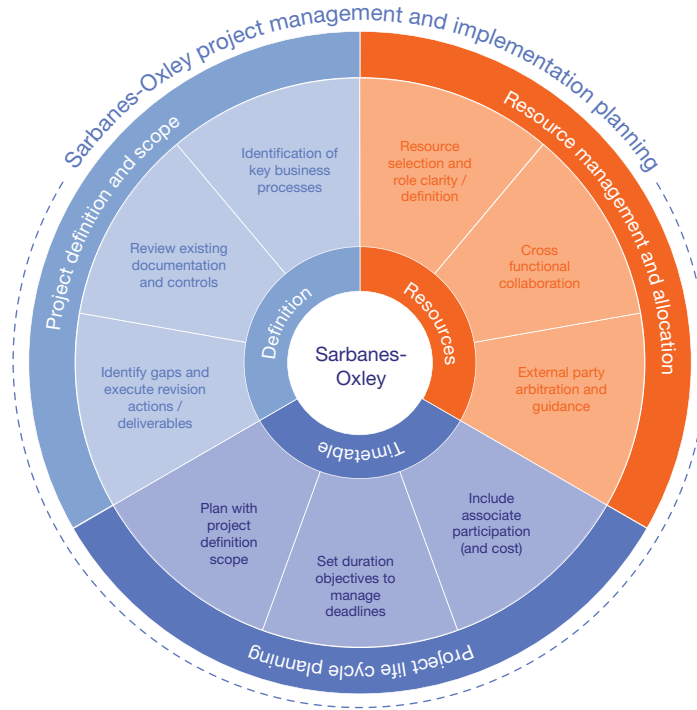


Figure 5. Example project scope by geography

Operating region	North America				LatAm		EMEA			APJ	
Operating entities	New York	Chicago	LA	Montreal	Buenos Aries	Sao Paulo	London	Paris	Joburg	Sydney	Osaka
<b>Business process</b>											
Revenue recognition					Under evaluation						
Property, plant and equipment					Under evaluation						
Treasury management					Under evaluation	Under evaluation			Under evaluation		
Taxation			Out of scope		Under evaluation				Out of scope		Out of scope
Legal					Under evaluation						
HR and payroll					Under evaluation						
Management information systems					Under evaluation						
Mergers and acquisitions		Out of scope	Out of scope	Out of scope	Out of scope	Out of scope		Out of scope	Out of scope	Out of scope	Out of scope
Procurement to payment					Under evaluation						

Legend / Key

In scope	
Out of scope	Out of scope
Under evaluation	Under evaluation

# The Sarbanes-Oxley Implementation Challenge

One of the biggest concerns for US companies has been the high the cost of compliance with Sarbanes-Oxley – the resources needed to determine what is required to achieve compliance and the resources needed to get it done.

Some examples of specific challenges arising in the IT arena are:

- Security and reliability – essential requirements in today’s e-commerce marketplace and a prominent feature in any implementation.
- Complexities surrounding web-based, collaborative business applications – create issues that lie beyond the boundaries of traditional corporate infrastructures.
- Third party systems integration – companies may be forced to go outside of their local operating borders to include external third party software providers whose systems are integrated with their own applications.

It should also be remembered that even post Year One, US companies continue to battle with the challenge of implementing the rules already set in place by the SEC. New amendments and new rules relating to existing sections of the act continue to be issued. It is abundantly clear that the commercial and personal risk of non-compliance is very real. The challenge of implementation is still therefore very pertinent.

Figure 4 opposite illustrates the implementation challenge in terms of the relationship between project definition, resource allocation and timetable.

## Some Implementation Project Success Factors

Companies considering or faced with the prospect of a Sarbanes-like implementation now or in the future, can take some comfort from the fact that general project management principals and experience can equip them to tackle some of the common challenges.

An effective project team, often comprising of internal and external resources, is essential to the success of any implementation project. Corporate personnel, from ‘C level’ executives to key end-users have a stake in the outcome and should be represented within the project.

Thorough evaluation of project scope and risk is critical in terms of defining what is going to be the final deliverable. Care should be taken to ensure that scoping activity covers all business processes that have a potential impact on materiality. Documenting the structure of the company by operating geography will help to identify and determine which business processes should be included in the project.

It is essential that weak business controls within each functional area are identified as early as possible to maximise the opportunity for remediation. Since core business processes (and their sub business processes) are the focal points for compliance, each should be reviewed to determine where lack of control or weak procedures are evident.

In certain localities there may be instances where specific processes are not required, for example, they are managed at a corporate level. In this instance a corporate repository of entity specific information will help to minimise risk and possible non compliance.

Figure 5 opposite illustrates a typical output from the documentation and controls evaluation stage. The list shown is not exhaustive but is sufficient for reference purposes.

Overall, the life cycle of the project should not be constrained and any apparent shortcuts should be thoroughly reviewed from a number of view points before committing to action.

## Key Roles and Responsibilities

All employees, from top level management to key business system users, have responsibilities under Sarbanes-Oxley and are required to collaborate in an implementation project (this also includes external associates):

- Board of Directors, including C-level Executives: Sign-off and agreement the companies’ internal controls are sufficiently effective to minimise risk and fraudulent activities.
- Management from all business disciplines: Ensure internal controls and procedures are in place and adhered to at geographic locations, aligned to business reporting and information collection.
- Internal Auditors (or equivalent): Attest accuracy of management’s assessment.
- Steering Committee and project team: Overseer and management entity for the internal SOX implementation project. Acts as a feedback channel to the Board of Directors.
- Process, Control and Key Areas Managers, End-users: Owner and expeditors of policy and adherence.
- External parties (Auditors): Provide guidance to ensure consistency between project deliverables and audit expectations. More important to attest management’s assessment of internal control and prepare testing scripts for use by process and key area managers.
- IT Managers: should also be available to manage the expectation, input and delivery of any infrastructure requirements and systems improvements that have been documented. IT should not be omitted from the project.

“Look for robust reporting from the security administration system protecting access to your IT applications. That’s where auditors will start - can you show who has security to do each task and when it was granted, and by whom? An audit trail of what actually happened maybe too late in the process if you can’t show how your systems allowed it.”

Peter Jones, Product Manager, Lawson Software

# Sarbanes-Oxley and IT

To comply with SOX 404, management needs to assess the design and operating effectiveness of internal controls over financial reporting. The relationship with IT has three characteristics:

- the key controls can be manual, automated or a combination of both
- the PCAOB's Accounting Standard 2 does not differentiate between manual or automated controls
- all key controls for all relevant assertions relating to significant accounts and disclosure need to be assessed and an inventory of these controls created.

The SEC considers a control to be 'key' if the organisation relies on it to ensure that there are no material misstatements in the financial accounts. Management are required to demonstrate that all key controls are operating effectively. This means that management must 'test' their controls on a yearly basis in order to satisfy this stipulation. Although IT controls are deemed to be pervasive under the Act, an organisation may choose to employ a layer of mitigating manual controls that effectively eliminate the reliance on automated technology-based controls.

Automated controls are considered to be repeatable under the Act and therefore only need to be tested on one transaction to prove effectiveness, as opposed to substantively (many transactions) for manual or semi-automated controls. Some organisations are attempting to lobby the SEC on the basis that an automated control should not need to be re-tested on a yearly basis, provided it can be demonstrated that no changes have been made. In practice, it is in all likelihood, as difficult to demonstrate that nothing

has changed as it is to test the control, however the Act may well be amended to reflect this point of view.

Although the SEC does not differentiate between manual and automated controls, there is clearly a case for arguing that automated controls will be more efficient in many circumstances. Of course, the reality for most companies is that their key controls will consist of an amalgam of automated, semi-automated and manual controls. Whatever form this combination takes, the underlying technology/ infrastructure needs to be operating effectively for a company's key controls to be deemed effective.

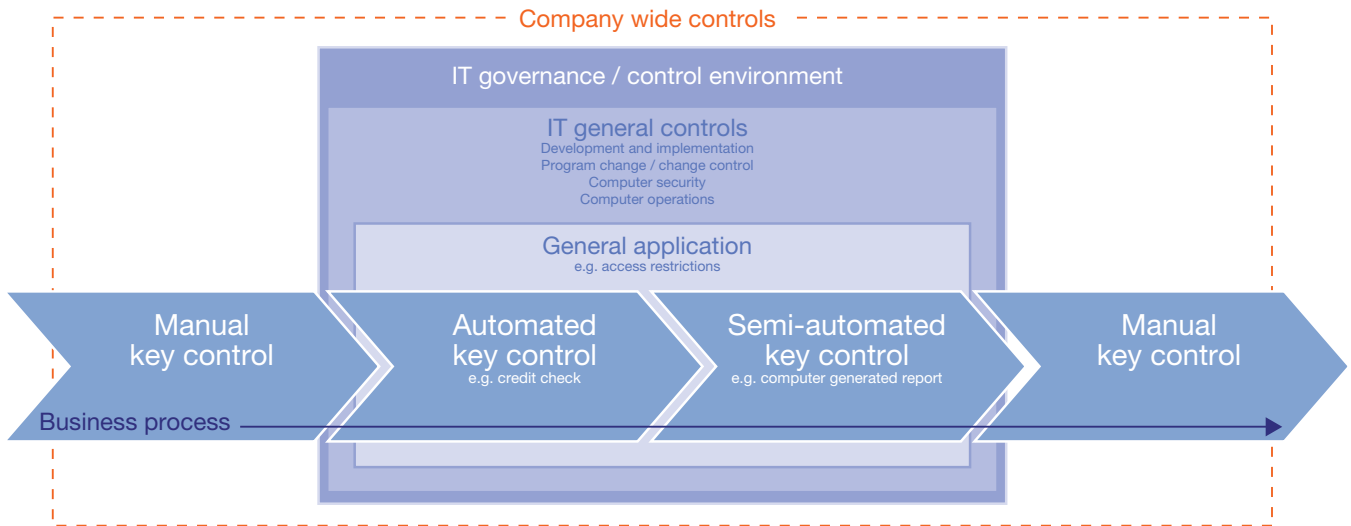
Brief definitions follow:

<b>Automated Controls</b>	By definition, automated controls are preventative controls in IT terms. Due to the flexible and complex nature of most modern finance systems, care should be taken in the choices made during setup and implementation. These choices may invalidate or make impossible the desired automated controls.
<b>Semi-automated Controls</b>	These controls combine a system and human element in the same control. Care should be taken with the design of the system element of the control to reduce the burden of human intervention by, say, filtering and targeting the reporting to only certain areas of the business or transactions at risk. If this is done, it will be necessary to be able to prove that, though only certain transactions are reported, say, all transactions were inspected.
<b>Manual Controls</b>	IT systems can play only a limited part in manual controls. However they can be used to document that the control exists, who is responsible for it, and whether it has been performed.

## IT General Controls (ITGC)

The SEC considers IT General Controls (ITGC) to be pervasive in nature; that is to say, any deficiencies arising in any of these controls will undermine the validity of automated controls, meaning that they can no longer be relied upon in financial reporting.

**Figure 6: The following diagram illustrates the Sarbanes-Oxley view of ITGC.**



For all companies, ITGC divide into four domains (discussed in the following pages). These are:

- Development and Implementation;
- Program Change or Change Control;
- Computer Security; and
- Computer Operations.

Appendix 2 on page 43 provides a checklist of key questions to ask relating to general computer controls.

## Development and Implementation

Software development may take place in a number of scenarios. It might occur as part of the development or enhancement of a generic software package, as local customisation of a package during its implementation for an individual business, or as one-off in-house development for a specific business, whether performed by an external software house or by an internal IT department. Whatever the scenario, the same control regime is required – although the mechanism for monitoring them will vary.

Where local development affecting systems that impact on financial reporting processes has occurred within a particular reporting period, the controls that govern system development and implementation must be tested.

Where development is outsourced, an external audit report – such as a SAS 70 report – may be an appropriate mechanism to allow the service organisation to disclose their control activities and processes to their users and their users' auditors in a uniform reporting format. SAS 70 is a globally recognised reporting standard used by a number of UK organisations (also see section on outsourcing for a more detailed description of a SAS 70 report, page 37).

The implementation phase must support the use of the relevant security and control features in the software – and in cases where this is not sufficient or appropriate, manual processes will have to be used to ensure effective control. For some smaller installations, manual controls may be more appropriate, rather than imposing unnecessarily complex automated procedures.

These requirements bring a number of best practice recommendations for software developers – including the use of a clear and demonstrable development methodology, and giving due consideration to application and data controls, as well as to security features. Similarly, implementers should ensure that the set-up and implementation of the system infrastructure does not jeopardise the security of the data and programs stored on the system, and that sufficient resource are available to fully implement the relevant application controls and security features. Crucially, the end-user company's IT management must understand the implications of the software controls requirement for Sarbanes-Oxley.

### Key messages for CIOs and Application Developers

#### CIOs:

- Ensure IT management understands the implications of the software controls requirement for Sarbanes-Oxley.
- Ensure setup and implementation of system infrastructure does not jeopardise the security of the data and programs stored on the system.
- Ensure sufficient resources are available to fully implement the relevant application controls and security features.

#### Application developers:

- Use a clear development methodology, and be prepared to evidence this. Typically this would be confirmed by regular audits leading to certifications such as ISO9001.
- Where appropriate, gain validation of the software by external bodies leading to certification.
- Give due consideration to application and data controls and to security features.

## Program Change or Change Control

Changes to an established system – whether due to a planned upgrade or to an emergency update – will require verification that the controls already in place are not adversely impacted by the change. Updates to packaged software and changes to locally developed software must follow the same cycle as initial development, including review of the changes, documentation and test of changed procedures and updates to documentation, as well as a review of the data security and control aspects.

When an upgrade of a commercial package takes place, the software provider should supply the user with documentation to enable them to assess the potential changes to procedures required.

### Key messages for CIOs and Application Developers

#### CIOs:

- Institute formal change control process for all updates, including emergency changes, systems conversions and enhancements.
- Ensure changes to data structures are assessed for impact on financial reporting processes.
- Implement a testing strategy that ensures that all significant changes in technology results in deployed systems that operate as intended.

#### Application developers:

- Where end-users request changes, the control implications of the requested change must be considered.
- Provide sufficient documentation to allow assessment of risk, level of testing required and identification of business processes affected by any changes.
- Make available a clear audit trail of system changes – audit file at installation, version numbering, and so on.

## Computer Security

The operation and administration of the security function of IT systems needs to be a key area of focus in a Sarbanes-Oxley compliance programme. The security system forms the first line of defence against inappropriate access.

With this in mind, the security system should have a number of automated characteristics to mitigate risk. For example, when new users are added to the system the default should be to grant them limited or no access, with any access having to be positively granted by an administrator. Periodic checks should be performed across all systems to report on and retire users that have been dormant. Only appropriate levels within an organisation should have access to duties that should otherwise be separated. And the security administration system should itself be controlled, capable of restricting access to certain functions, and reporting on who granted (and/or removed) access rights to a particular employee, and when.

These baseline requirements clearly feed into a number of best practice points for CIOs and developers alike. For example, CIOs should ensure that procedures are defined and followed to ensure that infrastructure systems, including network devices and software, are installed and maintained in a manner that support the controls and security required, for instance by forcing regular password changes. And developers need to ensure they provide features to control access to application software functions and data based on the individual's demonstrated need to view, add, change, or delete data.

Where appropriate, controls should be included to ensure transactions cannot be denied by either party and provide non-repudiation of origin or receipt, proof of submission and receipt of transactions. This is particularly important for transactions received electronically, but might also be relevant to the recording of proof-of-delivery documentation.

## Computer Operations

The day-to-day running of systems is an essential part of business continuity planning. This should include monitoring of attempted or actual security breaches, capacity and availability monitoring, as well as ensuring security back-ups.

In defining the business continuity plan in the Sarbanes-Oxley era, it is important to identify the critical application programs, third party services, operating systems, personnel and supplies, data files, and time frames needed for recovery. In addition to the more obvious concerns around continued availability services, businesses may wish to consider a number of more specific items. For example, escrow agreements can provide security in the event the software provider can no longer continue support, failsafe and/or fall-over systems may provide added security, and source documents must be retained or be reproducible for an adequate amount of time, with suitable backup procedures in cases where these are stored electronically.

Where services are outsourced, service levels must be clearly defined and monitored on an ongoing basis to ensure that financial reporting is accurate and available when required.

In all cases, regular review of procedures and monitoring of effectiveness is critical. Again, these requirements give rise to a number of best practice recommendations. For example, CIOs should ensure the organisation maintains and regularly tests a remote backup, while application developers should provide documentation to allow users to understand the system structure sufficiently to implement secure login control, security backups and recovery processes.

### Key messages for CIOs and Application Developers

#### CIOs:

- Identify your segregation of duties risks, address them, and automate your processes.
- Reduce reliance on user-developed reports and avoiding re-keying of data through automated reporting.
- Institute formal change control process for all updates, including emergency.

#### Application developers:

- Provide features to control access to application software functions and data, based on the individual's demonstrated need to view, add, change, or delete data.
- These features may include initial login control, an 'opt-in' approach to security for new users, and an ability to report that the separation of duties requirements are met by the security administration system.
- Embed the capability to provide an audit trail of data changes to allow chronological reconstruction of events.

### Key messages for CIOs and Application Developers

#### CIOs:

- Maintain and regularly test a remote backup, as well as implementing day-to-day security backups for both data and systems and periodically assess offsite storage and recovery facilities
- Regularly monitor and log security activity for both network and application software
- Regularly test the business continuity plan and monitor capacity to ensure continued availability of software and hardware

#### Application developers:

- Provide documentation to allow users to understand the system structure sufficiently to implement secure login control, security backups and recovery processes
- Put processes in place to ensure that, in the unlikely event of major disaster or company failure, the software can continue to be maintained and customers supported.

## The IT implication of SOX 409

When SOX 409 was initially proposed in 2002 it included a 48 hour deadline for filing and a much broader definition of 'material events'. This led to an interpretation by software developers that the 'real time' nature of the requirements would require major infrastructure changes, particularly to implementations with a heavy dependency on batch processing. 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. From a value to the business perspective, there is a valid argument for companies to have more effective, timely, reporting systems. From a regulatory perspective, there is little in SOX 409 to enforce this.

For software developers, reduced reliance on batch processing and the provision of, or interface with, some variety of 'business intelligence' tool are all good practices. For example, loading or refreshing a data warehouse (repository of data collated from one or more systems) on a more frequent basis can facilitate the creation of management reports outside of the normal monthly cycle. Messaging or notification systems can also be used to proactively deliver reports containing only relevant information that is targeted to specific individual users. An integrated system, with all departments viewing the same data is critical, since an event initiated by one area of the business may have an impact across the whole enterprise.

## The Challenges of Real-Time Reporting

A survey commissioned by Zeraxis and conducted at the Cass Business School explains what some companies are doing to achieve compliance.

Many experts believe that Sarbanes-Oxley 409 is a call for real-time reporting and leading companies are already starting to implement a Business Performance Management (BPM) framework to support strategy-driven real-time analytics and decision-making.

When asked how quickly companies could obtain the results of operations

- 50% said within 5 days
- 10 % said 6 – 10 days
- 30% said 11 to 30 days
- 10% said 31 to 60 days

For large organisations, in the financial services sector in particular, obtaining an integrated overview of an organisation's data is a task of monumental proportions. This is partly because many of them tend to have inherited numerous legacy systems based on different standards and platforms. In many cases various divisions and departments of the same organisation hold their own information which is not fully integrated into the main corporate operating system. This is particularly so, where the organisation may have subsidiaries in different geographical locations or countries.

Only 4 out of 10 respondents said that they have fully integrated systems.

In many cases, companies are working with a vast number of different systems, some of which are not equipped for the speed and complexity of today's business environment. Merging information from all these various systems into a single auditable and transparent system is an enormous challenge for most companies.

A disproportionate amount of time is also being spent on compiling the reporting pack rather than analysing and interpreting what the information means to the business. A surprising number (about 13%) spent 80% of the time compiling the information and very little time interpreting what that information means to their business.

### Key messages for CIOs and Application Developers

CIOs:

- Ensure all areas of the business are viewing information drawn from the same data set.
- Consider implementing pro-active reporting technologies for better targeted key information delivery.
- Consider moving the implementation of a data warehouse, typically not seen as a priority requirement, to the initial stages of a system deployment project.

Application Developers:

- Reduce the reliance on batch processing.
- Support more frequent loading of data warehouses to support the 'business intelligence' concept.
- Support the pro-active reporting technologies described above.

“Controls need to be well-designed and to operate effectively. This requires diligent staff who understand why the controls are important and implement them reliably. It is important to bear in mind that what’s appropriate for the head office finance department with a large headcount may not be practicable, or necessary, in a small subsidiary.”

Sheila Brisland, Product Manager, Sage (UK) Ltd.

## Application Controls

As can be seen from the diagram (figure 6) at the start of this section, automated controls are commonly embedded in an application. Application controls may be part of the basic operation of a system, such as numbering during posting – or post-event, such as a data integrity check. Controls, checks and tests need to ensure that assertions of completeness, timeliness and so on can safely be made for all stages in the transaction lifecycle. Failure at any one point means failure at the end point.

Where data is passed from one module or one system to another, data integrity controls are required at each interface to ensure that no values are omitted, changed or double-counted. So the system needs to be checked not just for its internal functioning, but for its external interfaces to other systems, both upstream and downstream. In an outsourced environment, application controls need to start from the information's point of entry to the organisation.

Controls and tests may be inherent to a system, may be set up specifically to comply with Sarbanes-Oxley or may be applied as part of the wider audit. Crucially, the more controls are inherent in the software, the less surrounding tests are required, except for proving the integrity of data transition between systems. Therefore a system which provides adequate or more than adequate internal controls can significantly reduce an organisation's compliance burden.

It is important to define clearly where the checks and tests occur, when they occur, who is responsible for ensuring they complete successfully, what particular assertion they help to support, what remedial action is required in case of failure, and which area of the transaction lifecycle they cover. It is also important that those responsible for ensuring checks complete successfully understand what is meant by "successful" – both in the spirit and the letter.

In designing the testing of automated application controls, factors that need to be taken into account include: whatever financial statement assertions are relevant to the automated application control under test; the nature of the key controls to be tested; and the location and source of inputs.

### Key messages for CIOs and Application Developers

#### CIOs:

- Define where, when and why the checks and tests occur in your applications.
- Define who is responsible for monitoring these controls and ensure they understand what level of control is required by the business.
- Define how these controls contribute to financial reporting, how they rely on other systems and what remedial action can be taken in case of failure.

#### Application developers:

- Ensure your product offers adequate documentation identifying the processes, risks and corresponding controls options.
- Your product should document the data flow, reliance and interfaces with other systems.

## IT Governance/Control Environment

This notion of ITGC also includes the 'tone at the top', in other words IT governance or the IT environment as it is termed by the SEC. The PCAOB has indicated that an ineffective control environment should be regarded as at least a significant deficiency and as a strong indicator that a material weakness in internal control over financial reporting exists.

From a wider perspective, executive management set business objectives, establish policies, and make decisions as to how the resources of the organisation should be deployed and managed. IT is obviously a fundamental resource of the organisation, and therefore it is anticipated that IT policies and other enterprise wide guidelines are set and communicated throughout the organisation. The IT governance process therefore includes the information systems strategic plan, the IT risk management process, compliance and regulatory management, IT policies, procedures and standards.

Monitoring and reporting are expected to ensure that IT is aligned with business requirements. The IT governance structure should be designed to help ensure that IT adds value to the business and that IT risks are mitigated. This also includes an IT organisation structure that supports adequate segregation of duties and promotes the achievement of the organisation's objectives. In terms of implementing a suitable IT control environment, it is important to demonstrate how the IT controls support the COSO framework. Five essential components of effective internal control are defined in COSO. They are:

- Control environment – Encompasses the tone at the top of an organisation, including risk appetite, integrity and ethical values.
- Risk assessment – The identification and analysis of relevant risks to achieving the entity's objectives, forming the basis of determining control activities.
- Control activities – Policies and procedures that ensure management directives are carried out including approvals, authorisations, verifications, recommendations, reviews, security and segregation of duties.
- Information and communication – Flow of information that allows for successful control actions.
- Monitoring – Assessment of a control system's performance over time, including management and supervisory actions and internal audit.

### Key messages for CIOs and Application Developers

#### CIOs:

- Ensure your staff understand risk and controls both at company and technology levels.

#### Application developers:

- Align your IT activities to your company's governance and risk policies.
- Think about some of the "soft" issues that wrap around your product - governance, controls understanding or "consciousness" and the ability to provide various levels of control dependent on your clients risk appetite.

“As organisations continue to move from manual to automated processes and business tools, to support their compliance challenges it is clear that technology has an equally critical role to play in achieving compliance. The objectives are clear. The end-game is sustainable compliance, controlling the costs of compliance and getting a return on compliance.”

Shelley Howard, Solutions Manager, SSA Global

# What have we learned from the Sarbanes-Oxley experience to date?

In this second half of the document we detail key learnings from the Sarbanes-Oxley experience to date, being:

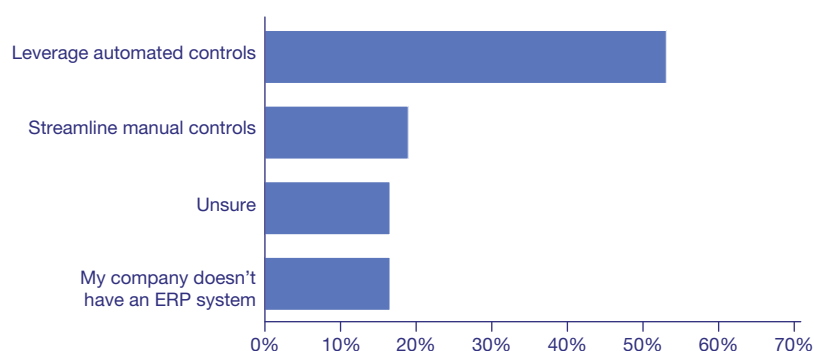
- Choose a governance framework to work from
- Integrate IT with Sarbanes-Oxley and the broader internal control agenda
- Take an inventory of your IT assets
- Assess the impact of your applications
- Address end-user computing
- Understand how outsourcing is controlled

## The impact of automation

While most companies are anxious for business unit managers to assume accountability for Sarbanes-Oxley compliance, they also realise that the biggest pain points in the compliance process – and the biggest opportunities for achieving savings and greater efficiency – lie beyond the scramble for better documentation, in fundamental areas of financial reporting such as testing, monitoring, and remediation or mitigation. This is where automation comes in – a message underlined by recent survey findings (see Figure 7) that senior executives with an ERP system would rather focus on leveraging automated controls within it than on streamlining manual controls.

### Figure 7. Automation of controls within ERP systems prevails over manual controls, say survey respondents

Do you feel you would rather streamline your manual controls or leverage automated controls within your ERP system?

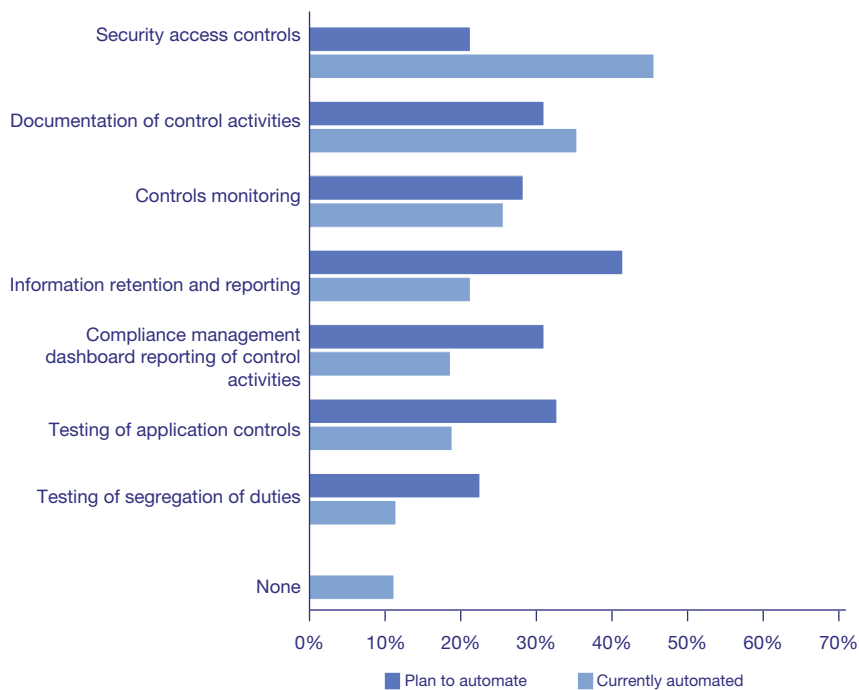


Source: PricewaterhouseCoopers, Virsa Systems, CFO Publishing survey, August 2005 Survey of 180 business executives

Going forward, automation will be essential to establishing a sustainable Sarbanes compliance framework. However, companies have different expectations for what they believe will be the most important uses of their new automated systems (see Figure 8), although there is widespread agreement on the importance of areas such as security.

**Figure 8. Companies have invested most aggressively in technology for security and controls documentation**

Which of the following areas of compliance have you automated or plan to automate in the future?



Source: PricewaterhouseCoopers, Virsa Systems, CFO Publishing survey, August 2005 Survey of 180 business executives

Most companies emphasise the importance of automation in achieving the greater command and control over data that successful Sarbanes-Oxley compliance provides. Some companies now have an explicit policy of replacing manual with automated controls and reporting at every available opportunity.

This illustrates a key trend. As forward-thinking companies shift from their year one project-based to a sustainable approach to Sarbanes-Oxley compliance – effectively making it an integral part of ‘business as usual’ – they are embracing automation to drive sustainable, cost-effective compliance across the enterprise. This not only means optimising underlying business processes, but also leveraging automation to facilitate more effective collaboration between business owners, auditors, and IT administrators, and to enable a shift from detective to preventive capabilities. The overarching goal is to achieve a state of pervasive compliance in which rationalised controls, embedded in optimised business processes, operate in real time to prevent compliance issues before they arise.

## Five Common Compliance Challenges

As CIOs and their enterprises undertake this shift from tactical, project-based compliance to pervasive, process-based compliance, there are five common challenges that often emerge. There are:

### 1. Inadequate use of automated controls resident in IT systems.

Companies' IT systems contain many automated control capabilities that are underused or completely overlooked. Automating the monitoring and enforcement of these controls can dramatically accelerate time to compliance and reduce cost.

### 2. Segregation of duties violations.

One of the most common compliance issues facing companies today is a proliferation of segregation of duties (SoD) violations in their IT systems. Companies are seeking to identify these SoD risks rapidly, address them, and then maintain their systems free of SoD violations through automated solutions.

### 3. Too many roles.

Having far more roles defined in a system than necessary is a major contributor to SoD violations. Companies are moving to automated role management to prevent authorisation conflicts.

### 4. Manual user provisioning.

Inefficient user provisioning is a further contributor to control issues. Automated, workflow-driven solutions that incorporate risk analysis can achieve dramatically more efficient user provisioning and prevent potential audit issues.

### 5. Excessive time spent on assessing the control environment.

A major driver of Sarbanes-Oxley related costs has been excessive time spent detecting and then remediating and/or mitigating control deficiencies. Solutions that combine efficient remediation and mitigation with preventive risk analysis and automated reporting can significantly reduce the cost and time spent on compliance.

“Through automation, the sites themselves are able to be more efficient operationally, and also the corporate office gains greater understanding of what’s going on.” – CFO, real-estate firm.

#### Key messages for CIOs and Application Developers

##### CIOs:

- Internal control processes based on manual procedures or tactical workarounds may have helped companies “get by” the first time, but are inefficient, costly and unsustainable components of a long-term compliance programme.
- Automation of controls and reporting delivers efficiency and effectiveness benefits not just in compliance but in operational terms.
- The goal is a state of pervasive compliance in which rationalised controls, embedded in optimised business processes, operate in real time to prevent compliance issues before they arise.

##### Application developers:

- Applications developers should develop their products to provide the progressive advance in automation of controls and reporting that companies require.
- To be fully effective, these capabilities need to be embedded within and across the product, and capable of integration with other applications.
- If application developers do not meet this need for greater automation, then they may find other ERP vendors or niche middleware developers moving into their customer base to provide this.

“Effective compliance requires integration of the applications supporting context and collaboration to ensure up-to-date information and timely reporting.”

Del Attah, Director, Zeraxis

# Choose a governance framework to work from

Various IT governance frameworks can be used to underpin compliance and, whichever they choose, organisations are expected to employ the entire framework (or to demonstrate why the entire framework is not required). Companies should therefore take time to ensure that they select the one that is best aligned with their particular business. Valuable lessons can be learned from the experience of those companies which have adopted a framework, only to find that it proves to be unsuitable for their needs.

When it comes to selecting the right governance framework, there are several options to choose from – including COSO, COBIT and ISO17799. Each framework has its own pros and cons, although both COBIT and ISO17799 tend to be more prescriptive and can be more complex to implement.

Here is a summary of the key features of each of the main frameworks.

## COSO

This is less prescriptive from an IT point of view, but can provide greater flexibility than the alternatives.

COSO is underpinned by four key concepts. Firstly, internal control is a process. It is a means to an end, not an end in itself. Secondly, internal control is effected by people – it is not merely about policy manuals and forms, but about people at every level of an organisation. Thirdly, internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board. And finally, internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

## COBIT

For companies needing detailed signposting, the granularity provided by COBIT's control objectives can prove helpful. However, for other companies, it may prove to be too specific and cumbersome in operation.

COBIT – Control Objectives for Information and related Technology – was originally released as an IT process and control framework to link IT to business requirements. It was initially used mainly by the assurance community in conjunction with business and IT process owners. Since the addition of Management Guidelines in 1998, COBIT is now used increasingly as a framework for IT governance, providing management tools such as metrics and maturity models to complement the control framework.

## ISO17799

Unlike COBIT, which specifies actual controls required for different areas, ISO17799 flags key domains, without being prescriptive. Although it is less granular than COBIT, it can still be challenging for some organisations.

ISO/IEC 17799:2000 - The Code of Practice for Information Security Management is an international standard, based on BS 7799-1. It is presented as best practice for implementing information security management.

- There is more detail on these frameworks in Appendix 1 on page 39.

### Key messages for CIOs and Application Developers

#### CIOs:

- Each framework carries its own characteristics and pros and cons.
- While the choice is for each company to make, the preference shown by industry peers and enterprises of a similar size and nature may help to shape the decision.
- Consult with other risk and control stakeholders in your business to ensure consistency of approach

#### Application developers:

- Knowing and understanding the risk framework employed by the customer is a key element of getting to know its business.
- The chosen risk framework may influence the optimal product and support offering to the particular client.

“Integrating computer controls and business processes has gone fairly well for us. It has led to greater convergence of business and IT process.”

Chief Finance Officer, US Energy Corporate

# Integrate IT with Sarbanes-Oxley and the broader Internal Control agenda

We have already pointed out how the advent of Sarbanes-Oxley has brought the CIO new accountabilities and an unprecedented central positioning in shaping the corporate agenda. Crucially, all IT actions launched and sanctioned by the CIO must be integrated and coordinated with the broader range of Sarbanes-Oxley related initiatives. This in turn means consulting and liaising much more closely with a broader array of stakeholders, ranging from risk management to internal financial control personnel.

In a number of organisations, IT has historically been viewed as a utility, rather than an integral part of the business. IT professionals have therefore been marginalised from core management functions as a result. Now that the challenge of Year One compliance has been met, CIOs are starting to take advantage of the opportunity they have been given to integrate IT into all aspects of the business process, instead of being a standalone, service department.

As companies get to grips with year one compliance, many are starting to realise that the benefits they have started to realise in the financial reporting environment can be similarly taken across the operational and strategic parts of their business – areas where greater commercial and competitive risk to the organisation lies.

Many internal audit functions are now starting to work with operational management in the areas of production, R&D / innovation, customer service functions, call centres, fulfilment and distribution and sales / marketing. Whilst companies only have the organisational capacity for a certain amount of change at any one time, IT should be positioned at the forefront of these initiatives to enable desired business benefits to be realised over time.

## Key messages for CIOs and Application Developers

### CIOs:

- Do not just approach Sarbanes-Oxley as a compliance requirement, but as an opportunity to enhance controls, management information and decision-making, creating real and measurable RoI.
- Ensure full understanding, backing and buy-in for the programme both at board level and in operational divisions.

### Application developers:

- To capitalise fully on opportunities in this type of programme, application developers should try to build as deep an understanding as possible of the customer's issues and requirements, both in terms of compliance and operations.
- These issues – and the resulting application offering – may need to differ in various parts of the business.
- Embedded automated control and reporting capabilities will give an application an edge during software selection for the programme. This especially applies to applications equipped with an embedded ability to test and reconfigure themselves where necessary, reducing the workload for the company.

## Making Business Performance Management (BPM) a reality

With the process and control improvements obtained through their SOX 404 work, the greater visibility of end-to-end business processes and the implications of SOX 409, many companies are now looking to improve their BPM activities. Helping companies to manage and improve their processes on a continual basis, aiding decision making in the areas of resource allocation, controls improvement and organisational design, BPM relies on accurate and timely reporting.

With this in mind a heavy emphasis has been placed on developing 'dashboards', high level compliance and process performance reports, that provide the CEO and CFO with confirmation that key business controls are operating effectively. Of obvious value to a BPM initiative and SOX 409, these reports are, however, highly dependent on the accuracy of back office feeder systems. Unless the challenges of system integration have been tackled successfully, companies need to take a measured view when it comes to relying on dashboard style reports. It should also be remembered, that for real time reporting to work, an organisation's control framework must be sufficiently embedded and mature. There is a very real risk of falling foul of the garbage in/ garbage out syndrome.

Many companies are focusing on "non-financial" data such as the operation of internal business process controls. This can mean gathering and reporting information on processes such as

receivables, customer acquisition or purchase to pay for example. For the internal audit or financial control departments, this may mean monitoring the performance of a group of controls, using a dashboard spanning various entities, to provide them with the ability to identify problems arising at an early stage, preventing them from becoming major issues, e.g. fraud, process "looping", system failure or capacity limitations.

CIOs and their departments have a key role to play in terms of making BPM a reality. The drive to overcome the integration issues, so that accurate and timely dashboards or real time reports can be made available for executive management, has put this high on the CIOs agenda. CIOs need to take on board these new key stakeholder requirements and provide guidance as to how IT can take the business beyond compliance to real performance management.

Application developers are also presented with an opportunity to lead the way. By proactively talking to clients and finding out what they need to improve the speed and effectiveness of decision making, application developers can add immense value to a BPM initiative.

Additionally, developers should consider their software in the wider context of their client's business. Viewing their software as stand alone is likely to result in a solution that does not meet the client's needs.

“We have a lot of silos in this unit. People do not always know when there are reports already in place and instead go out and recreate things. So there’s duplication of effort everywhere, just because people are not talking.”

Unit Executive, Manufacturing Company

# Take an inventory of your IT assets

From an IT standpoint, one of the first steps towards compliance with Sarbanes-Oxley – and also towards realising the resulting operational benefits – is to establish a firm grasp of the current IT assets, in terms of both systems and applications across the organisation. This means creating a comprehensive IT inventory, which must include not only systems owned and run in-house, but any third-party systems used under outsourcing or hosting arrangements.

**Before starting to take any action around the IT assets, it is imperative to establish first exactly what those assets are.**

Compliance middleware software products are available to ease this task. Some provide links to the individual controls themselves and document their status, history and when last performed. Consideration should be given to how such middleware is integrated into the core finance systems. Using an extra application just to manage the management of controls does not improve the efficiency or effectiveness of the controls themselves.

The logic for creating this inventory is clear. Before starting to take any action around the IT assets, it is imperative to establish first exactly what those assets are. Crucially, the process of creating this inventory will reveal instances where spreadsheets are being used for processes and applications in the business – often on a more widespread basis than previously thought – and where non-standard systems and applications have been bought in at a business unit or divisional level for specific tactical purposes, and either used stand-alone or bolted onto the group system.

## Strengths and weaknesses

Establishing the precise status of third-party systems may clearly present particular issues. The scope of the Sarbanes-Oxley provisions includes external suppliers who provide services around a business's processes, whatever the commercial basis on which they are supplied. Examples might include a data warehousing supplier providing services to a bank, and therefore holding data remotely about the bank's customers. The internal control environment in that outsourced services provider has to be attested in exactly the same way as the bank's own controls. See section on outsourcing on page 37.

Once completed, this inventory then creates the basis for a considered analysis of the strengths and weaknesses both of the overall IT assets and of each component, enabling decisions to be made over whether to retain, optimise or remove each one. The considerations taken into account will include how each component is used, and how closely integrated it is both with the specific process and the corporate system. As well as bringing fragmentation and dis-integration issues to light, this process may also reveal isolated pockets of best practice that can be rolled out more widely.

## Breaking down silos

Having developed a better understanding of their systems and processes, companies are then in a position to consider a move towards common and/or centralised systems and processes, as well as instituting less complex end-to-end processes. This standardisation and simplification process will take substantial cost out of the business whilst improving the company's agility and competitiveness.

A further operational and cost benefit of the inventory is that it will help the CIO to root out not only financial reporting control gaps, but also duplication and redundancies across different areas of the business. This in turn will support the organisation in its efforts to make data and other resources available on a consistent basis to more people within and across business units.

## Key messages for CIOs and Application Developers

CIOs:

- The inventory to form the basis of the Sarbanes-Oxley programme must be comprehensive in terms of its coverage (including the level of risk) of systems, hardware and software assets, of all parts of the business, and of external suppliers.
- Middleware products are available for this – but beware of adding another layer of complexity and cost.
- The process of compiling an inventory of third-party assets may create opportunities to gain service and cost improvements from contractors.

Application developers:

- Application developers have an opportunity to add real value to their clients' businesses, and to their client relationships, by helping them to compile inventories of their IT assets. In its simplest form, this means making licence and user details at both a subsidiary and group level available to the CIO.
- As a minimum, a procedure could be introduced under which new licence sales are logged centrally with the

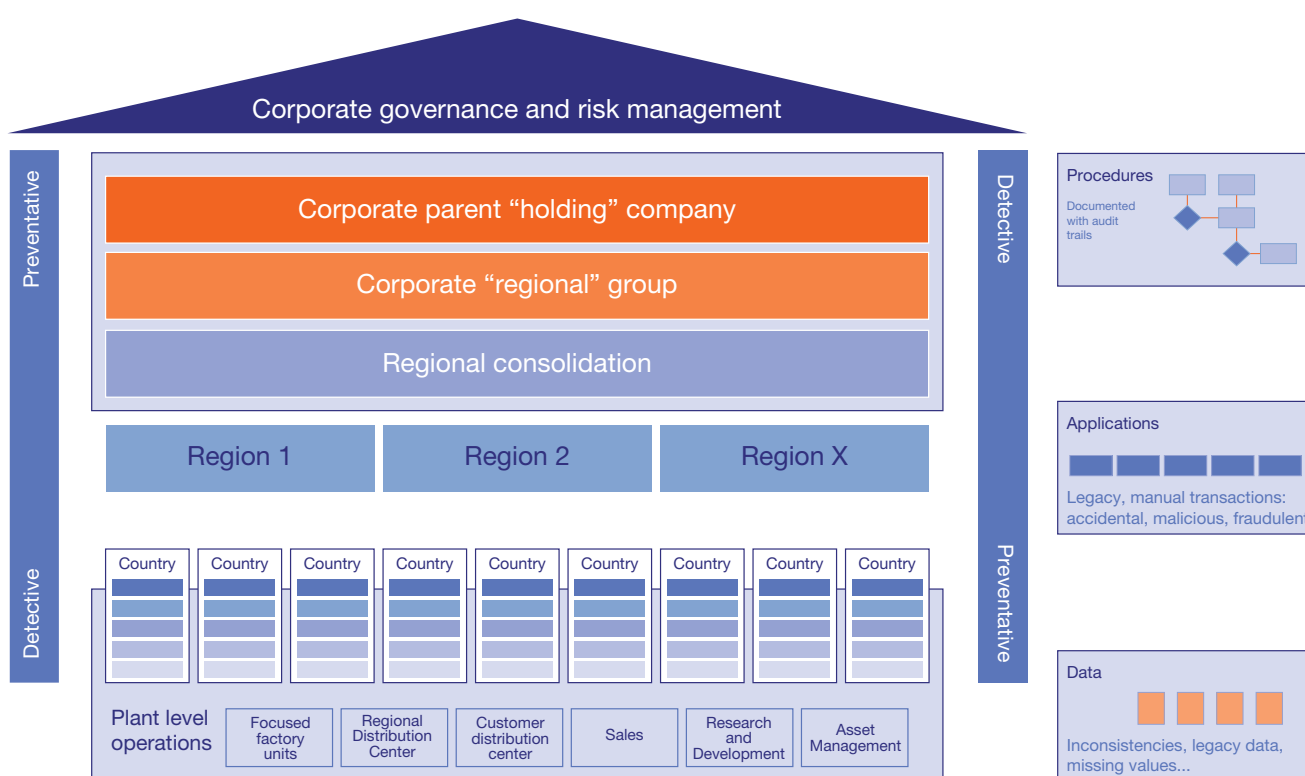
“We have always been a well-controlled company, so we started from a better position than many companies. Even so, we had issues to address. Now with this suite of documentation, we are well-primed to move into 2005 and streamline things.”

Director of Internal Audit and Compliance, US Corporate

# Assess the impact on your applications architecture

Within large organisations, roles and responsibilities should be consistent, even if applications (both core and legacy) differ from location to location. Since SOX demands controls, consistency and clarity, the relationship between resources and IT is critical for sustained compliance. This is graphically illustrated in the diagram below.

Figure 8. Company structure mapped against applications architecture



The most important issue arising from Sarbanes-Oxley for IT is that Year One compliance made most companies realise that the systems underlying their controls and processes were fragmented and often inefficient. For example, in many companies, individual business units had been pursuing their own agendas in response to market developments, bolting on new applications as needed.

In the rush to meet the deadline for Year One compliance, most companies lacked the time to either streamline their processes or test their automated controls. As a result, they created manual checks and balances to get them through the compliance process. The net result was that additional and unsustainable layers of complexity were added to their already over-complex systems. Many also turned to external consultants to help with the documentation of processes

and testing of controls. For most organisations the process proved to be costly with little of the cultural change required actually taking root in the organisation.

Realising this, companies are now driving forward to centralise and consolidate their systems, so as to generate organisation-wide efficiencies and reduce the cost of compliance. As a consequence, the move to Enterprise Resource Planning (ERP) systems, with a single dataset and audit trail, will possibly accelerate to the detriment of stand-alone best of breed systems with discrete datasets and audit trails.

The IT function is a crucial enabler in this process and CIOs are finding themselves with a lead role to play in shaping this change.

“The implications for IT systems following the introduction of Sarbanes Oxley will be far reaching. The overriding need to control processes will affect the ways business systems are designed and implemented. The move to integrated, with workflow, a single dataset and audit trail, will provide a simplified systems architecture that will be far easier to maintain and control.”

Dennis Keeling, Chief Executive, BASDA

As we have already pointed out, the SEC does not distinguish between manual, automated or semi-automated controls. The value that IT systems can bring is in automating as many controls as possible. Even within semi-automated controls, those with a human review element, IT systems can target that review, and deliver only the information that is relevant to the person performing it.

The move towards graphical ‘workflow’ mapping was first seen in the 1990s. In recent years more and more financial systems have included process control engines in their products. In the Sarbanes-Oxley environment, workflow products can play a major role in both helping to 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.

Using technology to assist with the management of the compliance process can also enable improvements in the quality of information, speed of delivery, assurance that compliance steps (such as testing) are performed in accordance with the programme design, and accountability in the management and reporting of events through a “closed loop” environment. This can lessen the effort required to comply with Sarbanes-Oxley, speed the identification of problems and reduce the amount of reworking needed. Many have turned to Sarbanes-Oxley middleware products to provide this functionality and have gained some of the benefits described above, however such tools are not likely to be the answer in the longer term.

If an organisation has multi-company operations deploying both core/ legacy applications, the CIO needs to ask a number of hard questions. Are appropriate controls and procedures in place to manage operations under the new guidelines? More importantly, can the board rely on the integrity of the data within the transactional layers to produce accurate and fair value financial statements? If not, the business has a problem.

## A Consolidated Technology Architecture

By developing a technology architecture that pulls together data from disparate systems and uses appropriate functionality to enforce accountability, improve data quality and identify incidents, companies can bring compliance to life. There is clearly an opportunity for application developers to seize the high ground by building their offerings to utilise this kind of consolidated approach.

To determine whether upgrading or replacement are viable and cost effective options, the key question is whether the applications can address all of the challenges raised by Sarbanes-Oxley. Upgrading may be a cheaper option, if there is an embedded capability that has not been utilised. On the other hand, a full system replacement may increase implementation costs, but this should be weighed against the potential penalties for non-compliance.

The long-term solution for most organisations is likely to be the replacement of disparate systems with a fully integrated system using a single database, possibly from one vendor.

Automatically documenting and controlling their processes, delivering the composite audit trails required, this approach is undeniably attractive. The time horizon for organisations to re-engineer their systems architecture is however likely to be long. A gradual move to a single integrated system incorporating financials, consolidation and final accounts preparation is probably inevitable.

For CIOs contemplating a project of this nature, their priorities are, in order:

- To get the IT department to proactively identify opportunities to leverage existing technology in the control environment as well as in the compliance process.
- To define the technology architecture.
- To identify components to be acquired
- To lay down a phased approach to implementation.

These steps enable existing functionality to be repurposed and new capabilities to be acquired selectively, thereby supporting a Sarbanes-Oxley programme that is sustainable and realistic to implement.

In many companies, the process of scrutinising existing application architectures forces them to question whether and to what extent end-user computing needs to be retained and, if it does, how it needs to be controlled from a security perspective. The following section addresses this in greater detail.

### Key messages for CIOs and Application Developers

#### CIOs:

- Companies are driving towards the centralisation and consolidation of their systems. IT is a crucial enabler in this process and CIOs have a key role to play.
- Ultimately IT systems add value by automating as many controls as possible.
- CIOs need to ask a number of hard questions in circumstances where multi-country operations or a mixture of core/legacy applications are encountered.
- Maintaining the balance between compliance and opportunities to leverage efficiency improvements is an important priority.

#### Application developers:

- There is an opportunity for application software developers who can provide offerings with the capability to implement a consolidated approach
- Application developers should be sensitive to the problems of their customers administering frequent upgrades.

“Management should evaluate whether it is possible to implement adequate controls over significant spreadsheets to mitigate this risk or if these should be mitigated to an application system with a more formalised information technology control environment.”

PricewaterhouseCoopers

# Address end-user computing

Over time, companies have built up an increasing number of quick-fix documents such as spreadsheets, databases and other manual documents to supplement their main systems – typically called ‘end-user computing’. The process of s404 compliance has brought into focus the inherent problems posed by end-user computing. The key is that it should be addressed both as thoroughly and as early as possible, before it undermines the company’s compliance effort.

There are three main issues around end-user computing:

- It poses a high level of risk to financial reporting, due to these documents generally existing outside companies’ central control framework
- There is a high level of error in end-user computing compared to automated procedures due to human error, poor quality assurance and inadequate training.
- There is a significant hidden cost in time and resources for set-up, maintenance, use and audit – on average more than nine times the cost of automated processes. If you multiply that by 2,100 manual processes that a typical corporate runs, there is clearly huge scope for cost reduction.

The CIO’s first step towards addressing end-user computing is to ensure that all instances of it across the organisation are fully identified and documented, as part of the process of identifying key business controls. The key question to ask at that point is whether there are controls in place over all end-user computing. If they are not in place, they should be applied – or the instance of end-user computing terminated forthwith.

## Applying controls

The relevant controls might include standardised policies and procedures on system development, maintenance and operations, testing of end-user computing, and testing of manual controls over end-user computing. Alternatively the instance of end-user computing might be treated as an application, with validation checks applied to the inputs used in the formulae/macros and to the formulae/macros themselves.

The results from end-user computing should be tested against the expected results to validate the output. In general, testing of end-user computing as an application will be similar to GACC, but the granularity of controls will depend on complexity of the end-user application. Areas to cover and gain assurance on include development and implementation, change controls, access controls and computer operations.

With Sarbanes-Oxley inspired information on the level and types of end-user computing to hand, many companies are currently investigating the cost savings they can make by building greater functionality into their IT systems, and removing the incentive for staff to go it alone in this way.

### Key messages for CIOs and Application Developers

CIOs:

- Beware end-user computing – it carries additional risks and costs and can undermine a company’s Sarbanes-Oxley compliance programme.
- End-user computing should be reduced and subjected to controls as quickly as possible.
- The trends and causes of end-user computing can help to guide ‘official’ functionality upgrades in the corporate IT systems.

Application developers:

- Software developers should try to incorporate the missing features in their applications which force their customers to use add-ons.
- Application developers can support customers’ efforts to control end-user computing by cooperating proactively with their central IT control and compliance programmes.
- Helping customers to address end-user computing issues in their business will deliver added value to clients, build customer loyalty and open up new sales opportunities.

“The project has increased our audit efficiency, as well as enabling Technology and the business to work together on identifying and exploiting opportunities for efficiency.”

UK FTSE50 Finance Director

# Understand how outsourcing is controlled

We have already highlighted the requirements under s404 for companies to gain comfort over the state of internal control within third parties – outsourced services, key suppliers and so on. As a result, such service providers are increasingly being asked by their customers to provide evidence that the internal control environment used within the service provider’s organisation meets standards acceptable to the user organisation.

In some situations, outsource providers have failed to provide companies with assurance that their own systems of internal controls meet Sarbanes-Oxley requirements (in payroll, for example). Faced with this, companies have had to implement additional controls to compensate for the shortfall. As a consequence, efficiencies that could otherwise have been delivered may have been eroded.

On a positive note, this trend has resulted in improved service, strengthened reputation management and improved customer satisfaction. This is because one effect of these provisions has been that key third-party providers have had to gain a better understanding of the end-to-end processes or cycles that they provide or participate in, thereby improving process performance. This has reduced errors, wastage and ‘looping’ in the process, and delivered greater visibility over performance and other opportunities for performance improvement.

Examples of the type of service provider that may be included under the Act’s provisions include computer service bureaux, record-keeping providers, payroll bureaux, transaction processing services, and other hosted ERP services. Companies using services of these kinds have to document and demonstrate to regulators that control exists over operational activities conducted by third party administrators.

## The role of SAS 70

An increasingly common solution is a SAS 70 report – Statements on Auditing Standards No. 70, Service Organisations (as amended – April 2002). This report provides a uniform framework in which a service organisation can disclose its control activities and processes to its users.

There are two types of SAS 70 report. Type I reports on the design of controls at a particular point in time, including a description of the processes and controls. Type II reports on the effectiveness of these controls over time, and extends on the Type I report by including a description of the testing done and the results.

The SAS 70 report addresses the system of internal control used within the service organisation. This includes the technical components of the service, including hardware, software and network infrastructure; operational activities of the service centre staff; and information on any suppliers that the service organisation may rely on.

The auditor preparing the SAS 70 report will seek to establish whether the description of the controls provided by the service centre is materially correct, whether those controls are appropriate, and the effectiveness of those controls. The controls should be sufficiently effective to provide reasonable assurance that the control objectives were achieved.

For a company that uses third-party services, obtaining a SAS 70 report will provide a number of benefits and safeguards. These include assurance that the outsourced activities are properly managed, an independent assessment of controls and operating effectiveness, and an ability to satisfy the regulatory requirements under both the Sarbanes-Oxley Act and the IPSB (Integrated Prudential Sourcebook) from the Financial Services Authority in the UK.

### Key messages for CIOs and Application Developers

#### CIOs:

- The regulatory need to establish that third-party services and processes are effectively controlled brings a number of associated benefits and opportunities, which should be pursued.
- Companies should – as a matter of course – investigate the SAS 70 as a convenient and standardised way of meeting the requirements.
- CIOs of service providers should also consider initiating their own SAS 70, as it will reduce disruption with only a single audit, provide evidence that service levels are being achieved, and reduce the perception of risk that users may have.

#### Application developers:

- If you are considered a “key supplier” to an organisation providing outsourced services, you may find yourself subject to scrutiny in a Type II SAS 70 report.
- If this is the case, the auditor preparing the Type II SAS 70 report may seek to measure the completeness, accuracy and timeliness of the deliveries you make to the service provider.

“Sarbanes-Oxley has been hard, but it has been a valuable catalyst, ensuring that important and beneficial improvements have been made to the business. Overall, it has proved to be a positive catalyst, a Trojan horse for change.”

EMEA Finance Director, Global Technology Company

# Appendix 1

## Risk Management Frameworks

\* extracts from IT Governance Institute: COBIT Mapping.

### 1. COSO

COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. This was an independent private-sector initiative set up to study the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

<b>Document taxonomy</b>	'COSO Internal Control—Integrated Framework' is a report that consists of four volumes. It is dedicated to improving the quality of financial reporting and ethics through effective internal control.					
<b>Issuer</b>	The report was issued by Committee of Sponsoring Organisations of the Treadway Commission (COSO), which is a voluntary private sector organisation. The committee was formed in 1985 to sponsor an initiative of the US National Commission on Fraudulent Financial Reporting to study causal factors that can lead to fraud. Sponsoring organisations are: American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Institute, Institute of Internal Auditors and Institute of Management Accountants.					
<b>Goal(s) of the standard or guidance publication</b>	<p>The goal is to improve the ways of controlling enterprises by defining an integrated control system. It enables senior executives to put internal controls in place to assure the achievement of the mission and profitability goals and to manage risks. It is the most comprehensive study on internal control.</p> <table border="0"> <tr> <td>Business Drivers for Implementing the Guidance</td> <td>Related Risks of Non-compliance</td> </tr> <tr> <td> <ul style="list-style-type: none"> <li>• The need for a structured approach when defining a control system</li> <li>• Improvement of the efficiency of internal controls</li> <li>• Assessment and evaluation of the internal controls</li> <li>• Need to structure the internal controls</li> <li>• Guideline for reporting to external parties</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>• Non-systematic approach for controls</li> <li>• Incomplete controls</li> <li>• Weak control environment</li> <li>• Inefficient controls</li> <li>• Inadequate processes due to a lack of controls</li> </ul> </td> </tr> </table>		Business Drivers for Implementing the Guidance	Related Risks of Non-compliance	<ul style="list-style-type: none"> <li>• The need for a structured approach when defining a control system</li> <li>• Improvement of the efficiency of internal controls</li> <li>• Assessment and evaluation of the internal controls</li> <li>• Need to structure the internal controls</li> <li>• Guideline for reporting to external parties</li> </ul>	<ul style="list-style-type: none"> <li>• Non-systematic approach for controls</li> <li>• Incomplete controls</li> <li>• Weak control environment</li> <li>• Inefficient controls</li> <li>• Inadequate processes due to a lack of controls</li> </ul>
Business Drivers for Implementing the Guidance	Related Risks of Non-compliance					
<ul style="list-style-type: none"> <li>• The need for a structured approach when defining a control system</li> <li>• Improvement of the efficiency of internal controls</li> <li>• Assessment and evaluation of the internal controls</li> <li>• Need to structure the internal controls</li> <li>• Guideline for reporting to external parties</li> </ul>	<ul style="list-style-type: none"> <li>• Non-systematic approach for controls</li> <li>• Incomplete controls</li> <li>• Weak control environment</li> <li>• Inefficient controls</li> <li>• Inadequate processes due to a lack of controls</li> </ul>					
<b>Target audience</b>	The responsible parties for internal control are addressed by the guidance. They range from senior management, board of directors and internal auditors, to every individual in the organisation.					
<b>Timeliness</b>	COSO published Internal Control—Integrated Framework in 1992. At the time of this publication, a new version was out for exposure.					
<b>Certification opportunities</b>	There is no opportunity for a certification.					
<b>Circulation</b>	The report is referenced to as the international baseline for internal control systems. However, it is available in English only.					
<b>Completeness</b>	The report covers the topic of controls in a comprehensive manner. As it is focused on a management and control framework point of view, it may be seen as an additional reference for a framework for IT governance efforts. It is on a very high level and does not address IT requirements in a comprehensive manner, but its key concepts and definitions may be applied to control and management of diversified IT issues.					
<b>Availability</b>	The report can be purchased online from AICPA, <a href="http://www.cpa2biz.com">www.cpa2biz.com</a> .					

## 2. COBIT

The first guidance publication explained is COBIT. COBIT is an abbreviation of Control Objectives for Information and related Technology.

<b>Document taxonomy</b>	COBIT represents a collection of documents which can be classified as generally accepted best practice for IT governance, control and assurance.
<b>Issuer</b>	The first edition of COBIT was issued by the Information Systems Audit and Control Foundation (ISACF) in 1996. In 1998 the second edition was published with additional control objectives and the Implementation Tool Set. The third edition currently available was issued by the IT Governance Institute in 2000, and added the Management Guidelines, as well as several other detailed control objectives.
<b>Goal(s) of the standard or guidance publication</b>	<p>“The COBIT Mission: To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.”</p> <p>Business Drivers for Implementing the Guidance, Including Typical Situations</p> <p>COBIT is usually implemented subject to the following business cases:</p> <ul style="list-style-type: none"> <li>• There is a need for IT governance.</li> <li>• Services delivered by IT are to be aligned with business goals.</li> <li>• IT processes are to be standardised/automated.</li> <li>• A framework for overall IT processes is needed.</li> <li>• Processes are to be unified.</li> <li>• There is a need of a framework for a quality management system.</li> <li>• A structured audit approach is to be defined.</li> <li>• Mergers and acquisitions are occurring.</li> <li>• IT cost-control initiatives are desired.</li> <li>• Part or all of the IT function is to be outsourced.</li> <li>• Compliance with external (e.g., regulators, organisations or third-party) requirements is of concern.</li> </ul> <p>Related Risks of Non-compliance</p> <ul style="list-style-type: none"> <li>• Misaligned IT services, divergence.</li> <li>• Weak support of business goals due to misalignment.</li> <li>• Wasted opportunities due to misalignment.</li> <li>• Persistence of the perception of IT as a black-box.</li> <li>• Shortfall between management’s measurements and management’s expectations.</li> <li>• Know-how tied to key individuals, not to the organisation.</li> <li>• Excessive IT cost and overheads.</li> <li>• Erroneous investment decisions and projections.</li> </ul>
<b>Target audience</b>	Various organisations, public and private companies and external assurance professionals form the relevant target group. Within organisations, three levels are addressed: management, IT users and professionals and assurance professionals.
<b>Timeliness</b>	Although the latest version was issued in 2000, it is still up to date. The latest enhancements to COBIT at the time of this publication include: COBIT Quick-start, COBIT Online, IT Governance Implementation Guide and IT Control Practices
<b>Certification opportunities</b>	<p>COBIT’s audit guidelines contain information for auditing and self-assessment against the control objectives, however there is no certificate available for any part of COBIT. Furthermore, the COBIT framework is used frequently by certified public accountants (CPAs) and chartered accountants (CAs), for instance, when performing an SAS 70 review.</p> <p>Non-COBIT certification is available through ISACA, the originator of COBIT, in the form of the Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager™ (CISM™) certifications.</p>
<b>Circulation</b>	COBIT is used worldwide. In addition to the English version of the publications, it has been translated into Spanish, German, French, as well as several other languages.
<b>Completeness</b>	<p>As mentioned, COBIT addresses a broad spectrum of duties in IT management. COBIT includes all significant parts of IT management, including those covered by other standards. Although no technical details have been included, the necessary tasks for complying with the control objectives are self-explanatory.</p> <p>Therefore, it is classified as relatively high-level, aiming to be generically complete but not specific.</p>
<b>Availability</b>	<p>COBIT Online can be purchased by going to, <a href="http://www.isaca.org/cobitonline">www.isaca.org/cobitonline</a>. COBIT Online allows users to customise a version of COBIT just right for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys and benchmarking. Most parts of COBIT are open and readily accessible for complimentary electronic download on the ITGI or ISACA web sites, <a href="http://www.itgi.org">www.itgi.org</a> or <a href="http://www.isaca.org">www.isaca.org</a>. The audit guidelines are posted for complimentary download for ISACA members.</p> <p>Alternatively, a printed set and fully searchable CD-ROM can be purchased from the ISACA bookstore, <a href="mailto:bookstore@isaca.org">bookstore@isaca.org</a>.</p>

### 3. ISO / IEC 17799:2000

<b>Document taxonomy</b>	ISO/IEC 17799:2000 is an international standard.					
<b>Issuer</b>	<p>The international standard was published by ISO (International Organisation for Standardisation) and IEC (International Electro-technical Commission), which have established a joint technical committee, ISO/IEC JTC 1, addressing the components of BS7799-1 only. Essential parts of the international standards labelled as Information Technology—Code of Practice For Information Security Management were developed and published by the British Standards Institution, labelled as BS 7799-1:1999. The original British Standard was issued in two parts:</p> <ul style="list-style-type: none"> <li>• BS 7799 Part 1: Information Technology—Code of Practice for Information Security Management</li> <li>• BS 7799 Part 2: Information Security Management Systems—Specification with Guidance for Use</li> </ul>					
<b>Goal(s) of the standard or guidance publication</b>	<p>ISO/IEC 17799:2000 provides information to parties responsible for implementing information security within an organisation. It can be seen as a basis for developing security standards and management practices within an organisation to improve reliability on information security in inter-organisational relationships.</p> <table border="0"> <thead> <tr> <th>Business Drivers for Implementing the Guidance</th> <th>Related Risks of Non-compliance</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>• Definition of an information security management system, applying best practice in security management based on a systematic approach</li> <li>• Identification of critical assets via the business risk assessment</li> <li>• Enhancement of the knowledge and importance of security-related issues at the management level</li> <li>• Definition of responsibility and organisational structures for information security</li> <li>• Need for a basis for certification of the information security management system</li> <li>• Need for contractual relationships</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>• Risk of information disclosure, including related risks such as loss of confidence and trust</li> <li>• Incomplete risk assessment, thus inadequate level of risk management</li> <li>• Inadequate business continuity management</li> <li>• Lack of security awareness within the organisation</li> <li>• Inadequate security requirements when interacting with third-party organisations</li> <li>• Inadequate level of physical and logical security</li> <li>• Flawed procedures due to the lack of incident management</li> </ul> </td> </tr> </tbody> </table>		Business Drivers for Implementing the Guidance	Related Risks of Non-compliance	<ul style="list-style-type: none"> <li>• Definition of an information security management system, applying best practice in security management based on a systematic approach</li> <li>• Identification of critical assets via the business risk assessment</li> <li>• Enhancement of the knowledge and importance of security-related issues at the management level</li> <li>• Definition of responsibility and organisational structures for information security</li> <li>• Need for a basis for certification of the information security management system</li> <li>• Need for contractual relationships</li> </ul>	<ul style="list-style-type: none"> <li>• Risk of information disclosure, including related risks such as loss of confidence and trust</li> <li>• Incomplete risk assessment, thus inadequate level of risk management</li> <li>• Inadequate business continuity management</li> <li>• Lack of security awareness within the organisation</li> <li>• Inadequate security requirements when interacting with third-party organisations</li> <li>• Inadequate level of physical and logical security</li> <li>• Flawed procedures due to the lack of incident management</li> </ul>
Business Drivers for Implementing the Guidance	Related Risks of Non-compliance					
<ul style="list-style-type: none"> <li>• Definition of an information security management system, applying best practice in security management based on a systematic approach</li> <li>• Identification of critical assets via the business risk assessment</li> <li>• Enhancement of the knowledge and importance of security-related issues at the management level</li> <li>• Definition of responsibility and organisational structures for information security</li> <li>• Need for a basis for certification of the information security management system</li> <li>• Need for contractual relationships</li> </ul>	<ul style="list-style-type: none"> <li>• Risk of information disclosure, including related risks such as loss of confidence and trust</li> <li>• Incomplete risk assessment, thus inadequate level of risk management</li> <li>• Inadequate business continuity management</li> <li>• Lack of security awareness within the organisation</li> <li>• Inadequate security requirements when interacting with third-party organisations</li> <li>• Inadequate level of physical and logical security</li> <li>• Flawed procedures due to the lack of incident management</li> </ul>					
<b>Target audience</b>	The document targets people responsible for information security within various organisations willing to initiate, implement or maintain information security.					
<b>Timeliness</b>	The standard was published in 2000 in its first edition, which still is valid, and it is updated at infrequent intervals. Since this is an official ISO standard it will automatically be revised and updated when required every three to five years. It can be classified as current best practice in the subject area of information security management systems. The originating BS 7799 was revised and reissued in September 2002.					
<b>Certification opportunities</b>	A certification of ISO/IEC 17799:2000 is not available. However, a certificate on compliance with the British Standard 7799 Part 2 can be obtained, as BS7799 Part 2 contains binding specifications for a certification of an information security management system, as well as normative controls.					
<b>Circulation</b>	The standard is used worldwide and several countries have published local versions.					
<b>Completeness</b>	<p>Generic measures for information security management are provided, as well as the imperative of compliance with laws and regulations.</p> <p>Being focused on security issues, it does not cover the full scope of IT management duties, while the level of detail is comparable to COBIT. Phase two of this research will provide a detailed mapping of ISO 17799 to COBIT.</p>					
<b>Availability</b>	The standard can be purchased from ISO.					

“We had an archaic pricing system. We we went to document it under Sarbanes-Oxley, we decided we could make it better.”

Chief Executive Officer, Global Security Corporate

# Appendix 2

## Checklists

### General Computer Controls

This checklist has been prepared as a useful reference to help application providers better understand the environment that their product will need to fit into, and to act as a primer for dialogue with clients when assessing their control needs. It does not constitute advice or guidance and should be used with this caution.

Questions	Response	
	Yes	No
<b>Strategic planning</b>		
Has management prepared plans that align IT with business strategy and objectives?		
Does IT management solicit feedback from users and end to end process owners regarding the usefulness, effectiveness and efficiency of IT plans?		
Are IT strategies and operations formally governed by senior management and communicated to process owners and other key management stakeholders?		
Does IT management communicate its activities, risks and issues to the CEO, CFO and board on a planned and regular basis?		
Does IT monitor its progress against its objectives in a sustained and objective manner?		
<b>Organisation</b>		
Are IT management sufficiently knowledgeable, experienced and authorised to undertake their responsibilities?		
Is the IT department organisation properly constituted, with roles, responsibilities and reporting requirements defined and accepted?		
Have key systems and data been recorded and ownership of these communicated with the business?		
Is there the appropriate segregation of duties within the IT function?		
Are IT staff evaluated by competency and role definition on a regular and planned basis to ensure they align to the IT strategy and business needs?		
Are contract staff properly controlled and compliant with the company's procedures and policies?		
Are significant IT events, failures and control breakdowns reported to senior management or the board?		
<b>Human resources</b>		
Are job changes and terminations properly controlled so that internal control and security is not breached?		
Does the IT function have an ongoing training and development plan that is aligned to the IT strategy and business need?		
Does the IT function comply with the company's behavioural policies including codes of ethics/ conduct, values/ integrity statements and human resource policies?		
<b>Information architecture</b>		
Has IT management defined its information capture, processing and reporting controls to support financial reporting requirements?		
Has IT management defined, implemented and maintained security standards and subsequent levels for the classification of data? Are they reviewed on a planned and regular basis?		
<b>Communication</b>		
Has IT management developed, communicated and reviewed its policies, procedures and standards regarding the IT function activities. Is this reviewed on a planned and regular basis?		
Does IT management have processes in place to investigate, assess and remediate compliance with these policies, procedures and standards?		
Does IT management understand its roles and responsibilities related to Sarbanes-Oxley and other regulation?		

Questions	Response	
	Yes	No
<b>Assessment of risks</b>		
Does the IT function assess the likelihood and impact of risk (both at a functional and business wide level)?		
Does the IT function have in place appropriate management responses to mitigate these risks including but not limited to internal controls?		
Has a security assessment been performed on systems based on their critical importance to the organisation?		
Has a business continuity plan been formed by the IT function – one that aligns itself with the wider business interruption plan? Is it regularly reviewed and updated based on business requirements and environmental factors?		
Are data centre facilities equipped with adequate environmental controls to maintain systems and data?		
Is access to the data centre restricted?		
<b>Quality and performance management</b>		
Is documentation created and maintained to company standards for all significant IT processes, controls and activities?		
Does a quality plan exist for significant IT functions and does it prescribe an approach to address quality assurance activities on both an ongoing and project specific basis?		
Does IT management monitor performance and capacity levels of systems and respond where necessary in a timely manner?		
Is performance and capacity planning included in system design and implementation activities?		
Are key performance indicators in place for IT and are these monitored and acted upon as part of key management activities?		
<b>Assurance, compliance and control</b>		
Does IT management monitor the effectiveness of the internal control environment using quantitative, qualitative and supervisory methods?		
Does IT management use independent parties to review systems prior to implementation?		
Does the organisation monitor changes in external requirements – legal, regulatory, voluntary codes of practice with regards to IT practice and control?		
Are effective controls in place to ensure compliance with external requirements?		
Does IT management obtain assurance over the quality of internal control over third party providers?		
Does internal audit review IT activities and controls?		
Is the internal audit plan based on business risk assessment that incorporates all aspects of IT?		

## Application Controls

The following checklist provides a high level guide to the requirements of Sarbanes-Oxley s404 requirements for software developers. It does not constitute advice and should be used as a reference only.

Questions	Response	
	Yes	No
My product has the ability to meet the security, availability and processing integrity requirements of the target company (including controls to support complete, accurate, authorised and valid transaction processing).		
During the selection process my product documentation satisfies all control related questions of my client – controls both within my application and acknowledgement of controls within the wider business processes my application participates in.		
I have controls savvy staff who provide post implementation reviews of my product to verify that controls are operating effectively either within my products processes or as part of an interface of a larger business process.		
My product offering includes documentation identifying the processes, risks and corresponding controls options with my application and the interfaces with other business processes and systems.		
My product offers defined and documented interfaces around the transmission of data to help customers build their internal controls around my application.		
My product will continuously monitor customer defined business rules/ controls and self test with the ability to define alerts.		
We offer a standardised approach to change management. This includes defined and agreed documentation, approval processes and maintenance procedures.		
My product offers security control features that support generally accepted security standards – e.g. password length, change, etc.		
My product offers features to restrict access to authorised personnel according to my customer's policies and procedures.		
My product has the ability to build role based access profiles to restrict access to activities required to perform jobs and segregating incompatible access at both an activity and organisational level.		
My product offers real time checking of segregation of duties conflicts and sensitive access according to customer defined rules.		
My product has the ability to log activities and facilitates customised reporting and alerts using log data.		

“Sarbanes-Oxley has been hard, but it has been a valuable catalyst, ensuring that important and beneficial improvements have been made to the business. Overall, it has proved to be a positive catalyst, a Trojan horse for change”

EMEA Finance Director, Global Technology Company

# Appendix 3

## Glossary of terms used

<b>Abbreviation</b>	<b>Description</b>
AS 2	PCAOB Auditing Standard No 2.
COSO	COSO Internal Control - Integrated Framework is a report that was issued by the Committee of Sponsoring Organisations of the Treadway Commission (COSO).
COBIT	Control Objectives for Information and related Technology was issued by the Information Systems Audit and Control Association (ISACA) in 1996.
GACC	General Application Corporate Controls
ISACA	Information Systems Audit and Control Association
IPSB	Integrated Prudential Source Book
ISO / IEC 17799:2000	ISO / IEC 17799:2000 is an international standard that was published by ISO (International Organisation for Standardisation) and IEC (International Electro-technical Commission), which have established a joint technical committee, ISO / IEC JTC 1, addressing the components of BS7799-1 only.
OECD	Organisation of Economic Co-operation and Development.
PCAOB	Public Company Accounting Oversight Board - PCAOB is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002.
SAS 70	Statement of Auditing Standards No.70, Service organisations (as amended - April 2002)
SEC	Securities and Exchange Commission
SOX 302	Sarbanes-Oxley: Corporate Responsibility for Financial Reports.
SOX 404	Sarbanes-Oxley: Management Assessment of Internal Controls.
SOX 409	Sarbanes-Oxley: Real Time Disclosure.









