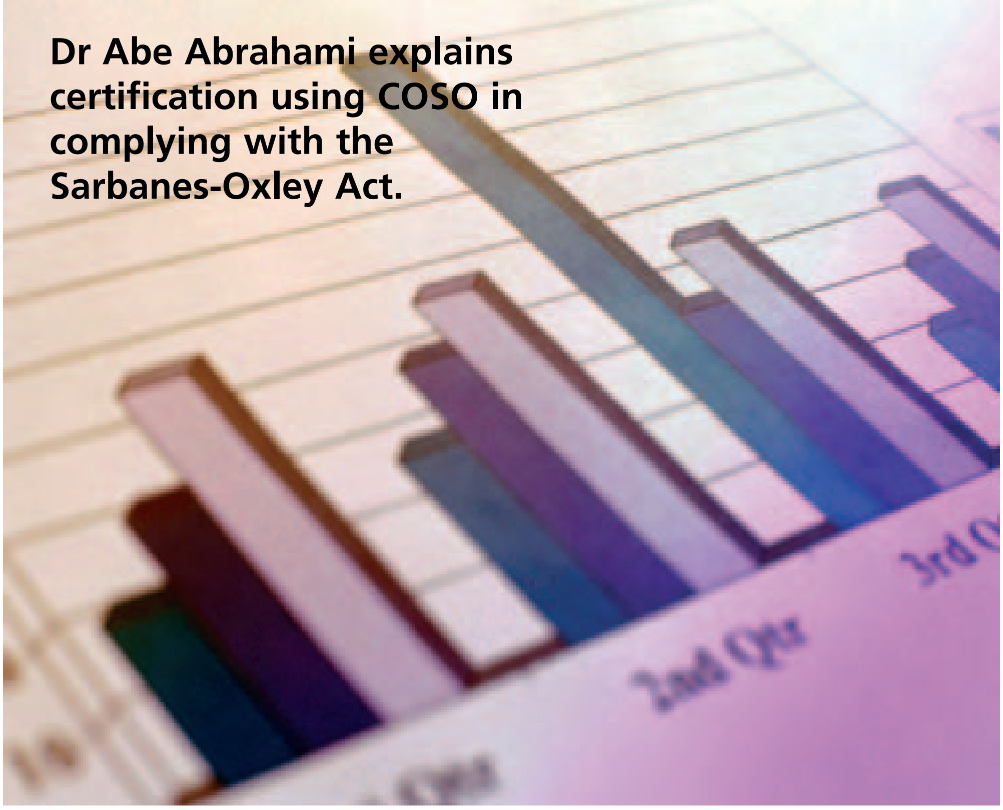
Business governance:
Sarbanes-Oxley Act (SOA) Compliance



Dr Abe Abrahami explains certification using COSO in complying with the Sarbanes-Oxley Act.

According to International Journal of Business Governance and Ethics:

"Issues of governance, responsibility and accountability are becoming increasingly important as the world, simultaneously, becomes dominated by corporations, interconnected via forces of globalisation, and transparent through heightened media attention and the rise in Internet-led democracy. Companies, and in particular leaders of business, can no longer hide from their responsibilities to a wider stakeholder community by claims of ignorance of corporate malpractices and of failure."

Company directors and executive officers are being made increasingly responsible for the successes and failures of their companies, as well as their own conduct. Actions of business have become a concern not just for shareholders, but also to the wider community at large, affecting individuals' investments and savings.

Business and financial governance is no longer just about running the company as efficiently as possible in narrow cost and profit terms, but about managing the wider responsibilities, compliance, ethics, honesty, integrity and transparency.

Sarbanes-Oxley Act (SOA) compliance is one of these critical instruments that force large international and local companies to enhance and extend their accountability, integrity, transparency and honesty in business conduct and financial reporting.

Implications

As a result of corporate scandals such as Enron, Arthur Andersen, and others, SOA was signed into law on 30 July 2002, largely in response to accounting frauds, the effects of which are still being felt throughout the US economy and the lives of many people who have been affected by these events.

Currently, all US listed companies fall under the Act, which may be extended to private companies. It impacts, among other things, information storage and retrieval of the companies' electronic records and documents, together with the recording and reporting of its finances.

SOA has a direct and severe impact on information storage, data warehousing, business intelligence, document and records management, financial process and knowledge management.

The Act, which has resulted in major changes to compliance practices at nearly 85 per cent of large US multinational companies, requires executives, boards of directors and auditors to take precise measures to bring about greater corporate accountability and transparency.

But what sort of impact is SOA having on European companies that do business in the US? Are those companies liable in the same way as their US counterparts? Does the Act apply to any non-US company registered on US exchanges under either the Securities Act or the Exchange Act? Does a company's country of incorporation or corporate domicile make any difference?

HSBC revealed that it is spending over $400m (£215m) a year on complying with regulations. The Shell scandal concerning over booked reserves has sent a shiver through the spine of European companies.

"Post Sarbanes-Oxley, the ante has been upped," said Larry Vranka, a corporate partner at City law firm Linklaters. "Companies are seriously looking at delisting and deregistering from the US."

The regulatory burden is about to get worse, he added. Non-US companies will need a report from their auditors verifying that the group's internal controls are up to scratch. This is causing concern not just to companies but also to their advisors. "This could be the straw that breaks the camel's back," said Mr Vranka. "It will mean that the accountants are doing effectively two audits and could add 50 to 100 per cent onto the cost of the audit."

According to Daniel Dooley, a PricewaterhouseCoopers partner and leader of its US securities litigation consultancy practice: "European corporations, their directors and officers and their independent and legal advisors would be wise to understand and prepare for the new world of Sarbanes-Oxley."

A pivotal part of the Act is to ensure auditor's complete independence and removal of conflict of interests between a fee-charging consultant role, and an independent critique reviewer of the company's financial and business affairs.

In Washington, DC, on 22 January 2003: "The Securities and Exchange Commission voted to adopt rules to fulfil the mandate of Title II of the Sarbanes-Oxley Act of 2002, strengthen auditor independence and require additional disclosures to investors about the services provided to issuers by the independent accountant.

The Commission approved measures that will revise the rules related to the non-audit services that, if provided to an audit client, would impair an accounting firm's independence:

- Require that certain partners on the audit engagement team rotate after no more than five or seven consecutive years, depending on the partner's involvement in the audit, except that certain small accounting firms may be exempt from this requirement;
- Establish rules that an accounting firm would not be independent if certain members of management of that issuer had been members of the accounting firm's audit engagement team within the one-year period preceding the commencement of audit procedures;
- Establish rules that an accountant would not be independent from an audit client if any 'audit partner' received compensation based on the partner procuring engagements with that client for services other than audit, review and attest services;
- Require the auditor to report certain matters to the issuer's audit committee, including 'critical' accounting policies used by the issuer;
- Require the issuer's audit committee to pre-approve all audit and non-audit services provided to the issuer by the auditor; and
- Require disclosures to investors of information related to audit and non-audit services provided by, and fees paid to, the auditor."

But how do you interpret these rules and filter through what concerns your specific business? Is it the accountant's job? Is it the managing director's job? Is it the auditor's job? Is it the IT director's job? In truth, it is a joint responsibility of all these people.

The author has discovered that some large accounting firms are selling their compliance 'expertise', while they themselves are not yet compliant.

To make matters worse, some of the people in charge of SOA compliance lack the multi-disciplinary experience and inter-disciplinary approach to SOA compliance, that it is far more than balancing the figures, having an audit trail and producing operation control procedures.

Without a solid IT and business process re-engineering background, an SOA compliance officer is doomed to fail.

Without an understanding and experience of content management system, data storage, management and security, information retrieval and linkage between records, documents and objects, one cannot succeed with SOA compliance.

> **'Not many people understand the Act and how to deal with it effectively'**

It's like building a beautiful racing car without the engine inside or without the gearbox connected to it.

Culture change is another issue – you will simply be unable to get away with things you were able to. It will not wash away, and it's a different ball-game, but do not despair, help is available.

Education is the key and despite the fact that SOA has been around since July 2002, not many people truly understand the Act and how to deal with it effectively.

Therefore, suitable training is essential and desperately needed.

Sections of the Act and compliance tools

The Act's most relevant and important sections are:

- 302: Corporate responsibility (honesty, integrity, transparency, accountability);
- 404: Management assertion of internal controls (robust procedures, audit independence versus consulting engagement of advisors, conflict of interests etc);
- 802: Reliance on information retention policies (audit trail, document links etc.);
- 1001: Corporate tax returns (consistent/transportable electronic file formats exchanged between companies, tax authorities and advisors).

There are several methods and standards, including software applications that help companies comply with SOA.

COBIT (Control Objectives for Information and related Technology) is a process model developed to assist enterprises with the management of IT resources. The process model focuses on developing suitable controls for each of the 34 IT processes, raising the level of process maturity in information technology and satisfying the business expectations of IT.

The adoption of COBIT can be largely attributed to increased attention being given to corporate governance and to the need for enterprises to be able to do more with less when economic conditions are tough.

ITIL (Information Technology Infrastructure Library) is a set of best practice standards for IT service management. The UK's Central Computer and Telecommunications Agency created ITIL in response to the growing dependence on IT to meet business needs and goals. ITIL provides businesses with a customisable framework of best practice to achieve quality service and overcome difficulties associated with the growth of IT systems.

ISO 17799 is a widely recognised security standard. It is comprehensive in its coverage of security issues and contains a substantial number of control requirements, some extremely complex. It is a detailed security standard, organised into 10 major sections, each covering a different topic or area.

QCR (Quality Compliance Cost Reduction) 3000 methodology embraces corporate health checks, IT governance, due diligence, audit, information management and business re-engineering elements, as well as integration with web service applications. QCR3000 embraces generic, re-usable and modular components, which are very similar to the tools described on the next page.

QCR3000 incorporates the most critical aspects of ITIL, COBIT and ISO 17799. Its major strength is the data-gathering questionnaire, information analysis and consolidation to discover and highlight deficiencies or conflicts that arise. In particular, QCR3000 helps to analyse, classify and concentrate on the issues and challenges for resolution in three common categories: red, amber, and green. It addresses common re-usable web-based system components, such as those produced by IBM and other leading IT suppliers.

According to Brenda Cammarano, IBM Rational Market Manager, Enterprise Modernisation Solution, and Forrester Research, only about 10-15 per cent of organisations effectively roll up the sub-processes into higher-level consolidated processes to enable better strategic decision-making, more effective portfolio management and comply with SOA requirements.

As a result, many organisations are likely to be wasting about five to 10 per cent of their IT budgets due to duplicated, misaligned and ineffective spending. For example, an organisation with £50 million per year IT budget, translates directly into £2.5 million to £5 million per year of wasted money.

Faced with a portfolio of disparate systems, limited resources, reduced budgets, and tighter business deadlines, companies can no longer tear away and replace legacy applications.

The answer lies in IT-SOI

For many organisations, the answer lies in the latest evolution of the distributed computing and common component-based development paradigm: web-based, IT service-oriented-infrastructure (IT-SOI).

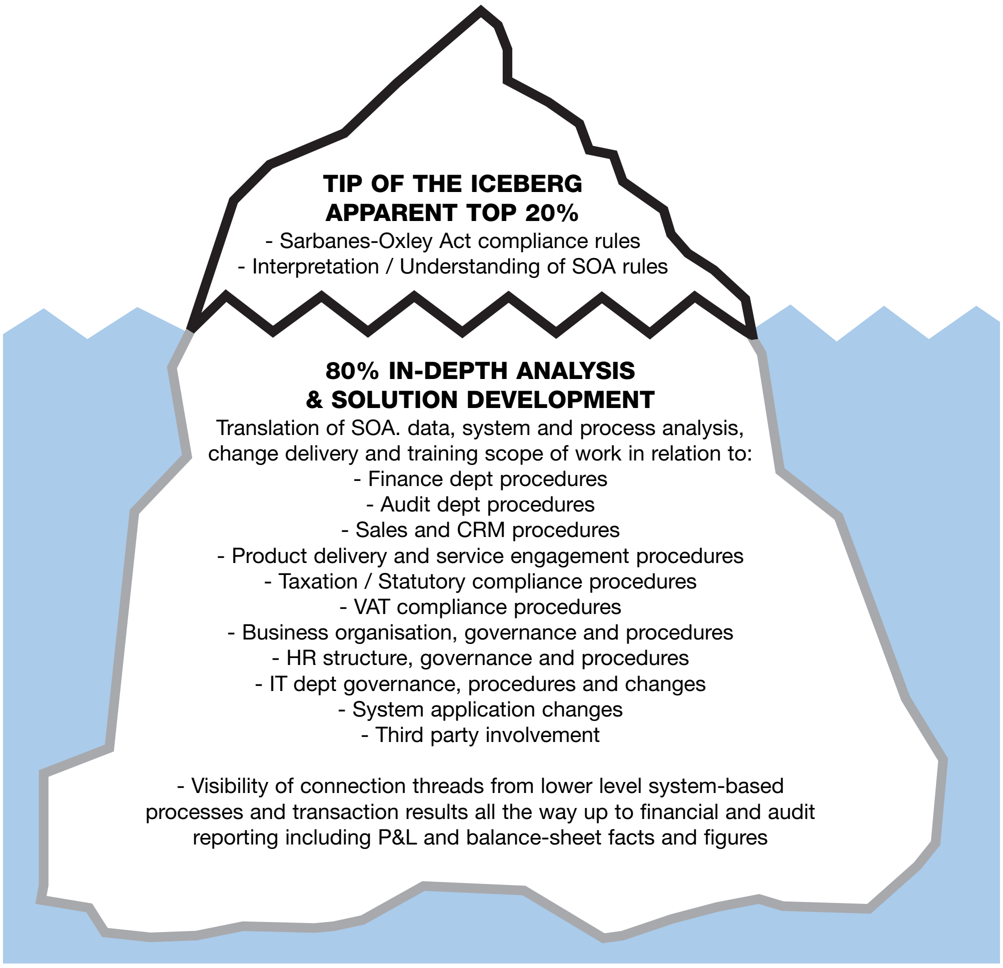
Based on web services, an IT-SOI gives an IT organisation the ability to standardise common functions used among many applications as reusable components or services.

This enables developers to focus their efforts on creating unique processes within an application, because they can leverage common process functionality across systems simply by calling a web service.

Government bodies as well as major banks and utilities have gone the IT-SOI route and increasingly, this is a preferred solution that also helps with SOA compliance.

Forrester Research conducted a survey of 75 IT executives at large North American companies to find out what they are doing with web services.

Internal deployment of web service capabilities were at the top of the project list with 83 per cent of firms planning to use web service inside their firewalls.


TIP OF THE ICEBERG
APPARENT TOP 20%
- Sarbanes-Oxley Act compliance rules
- Interpretation / Understanding of SOA rules
80% IN-DEPTH ANALYSIS
& SOLUTION DEVELOPMENT
Translation of SOA. data, system and process analysis, change delivery and training scope of work in relation to:
- Finance dept procedures
- Audit dept procedures
- Sales and CRM procedures
- Product delivery and service engagement procedures
- Taxation / Statutory compliance procedures
- VAT compliance procedures
- Business organisation, governance and procedures
- HR structure, governance and procedures
- IT dept governance, procedures and changes
- System application changes
- Third party involvement
- Visibility of connection threads from lower level system-based processes and transaction results all the way up to financial and audit reporting including P&L and balance-sheet facts and figures

The 80/20 empirical rule as it relates to SOA.

QCR3000 greatly helps and encourages companies to focus on a highly effective and efficient analysis and implementation of SOA compliance combined together with IT-SOI to cut or eliminate waste whilst becoming compliant.

QCR3000 exploits and employs the best of IT-SOI solutions and related controls and procedures, interacting as the fit-gap ‘glue’ between the business operational and financial processes, IT infrastructure, and common re-usable components, applications and generic-modular system engines.

Such re-useable modular engines include workflow, electronic document and record management, client relationship management, e-business and related applications.

Tip of the iceberg

The 80-20 empirical rule as it relates to SOA is shown above.

The numerous issues at the bottom part of the iceberg indicate how deep and wide SOA compliance reaches, and why it should be used as an opportunity to better the business as a whole, and not simply just comply with a set of rules.

COSO framework

According to Dennis Applegate and Ted Wills, in *Internal Auditor*, (December 1999) published by The Institute of Internal Auditors:

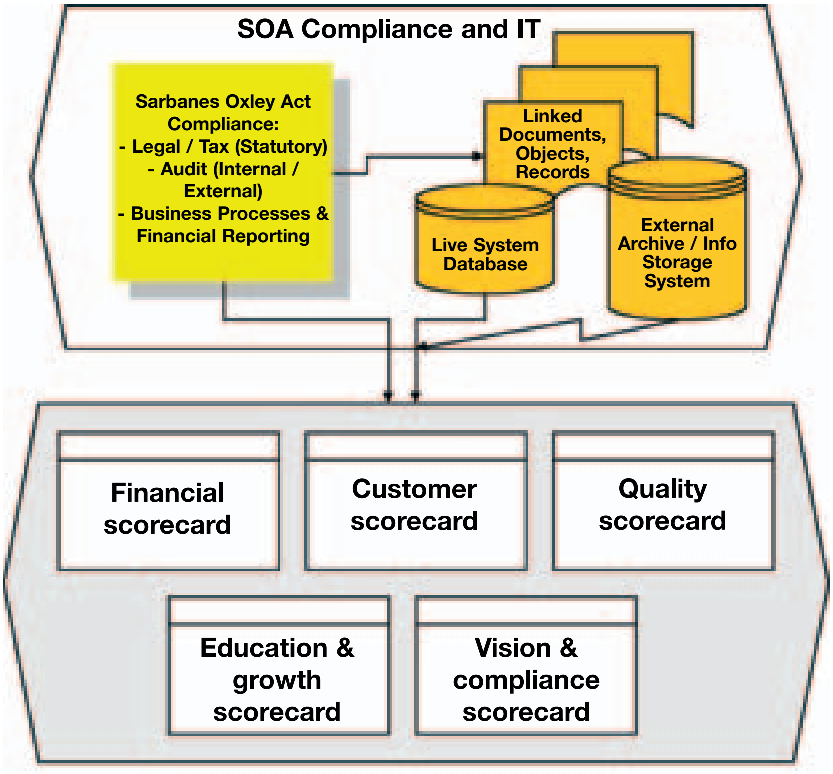
“In 1992, the committee of sponsoring organisations of the Treadway Commission (COSO) issued a landmark report on internal control.

Internal Control – Integrated Framework, which is often referred to as COSO provides a sound basis for establishing internal control systems and determining their effectiveness.

Following the report’s publication, The Boeing Company adopted the COSO principles partly as the basis for its internal control policies and procedures. As a result, our internal audit department began to rate the quality of internal controls covered in each audit.”

Boeing soon discovered that incorporating these standards into actual practice proved challenging. To achieve a higher quality result, Boeing re-engineered its existing audit methodology – from inception, through fieldwork, to final reporting – to fit the COSO framework.

The effort was a success and no longer incidental to business processes. COSO now provides the foundation for all Boeing's audit work.


SOA Compliance and IT
Sarbanes Oxley Act Compliance:
- Legal / Tax (Statutory)
- Audit (Internal / External)
- Business Processes & Financial Reporting
Linked Documents, Objects, Records
Live System Database
External Archive / Info Storage System
Financial scorecard
Customer scorecard
Quality scorecard
Education & growth scorecard
Vision & compliance scorecard

Business balance score card and benchmarking.

COSO is very much alive today, as it paved the way to SOA, which has enhanced and enforced what COSO initiated a few years ago, and as legislated by the Securities and Exchange Committee. The two entities, although independent, are inseparable.

Internal controls are pivotal to SOA compliance and must be understood.

The Security and Exchange Commission (SEC) rule-making body for Sarbanes-Oxley Section 404 mandated that a company's internal control over financial reporting should be based upon a recognised internal control framework.

The model framework, suggested by the SEC, is the one created by COSO.

The COSO framework states that internal control consists of five interrelated components that are derived from the way management runs the entity and that are integrated with the management process:

- Business and financial control environment
- Business and financial risk assessment
- Business and financial control activities
- Information transfer and communication
- Monitoring, correction and enforcement

COSO is at the heart of SOA and SEC related rules, therefore, to keep up with SOA compliance one must be kept abreast of COSO, its evolution and implementation.

Summary

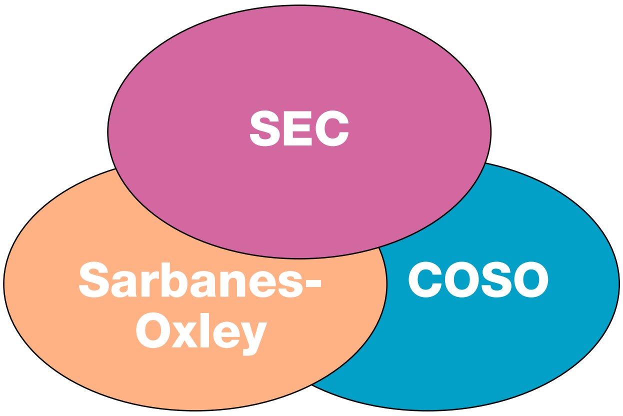
This paper outlines Sarbanes-Oxley and its complex issues. It has indicated that it is from a single discipline, it concerns business processes, finance, accounting, IT, security, operation and most other aspects of the company.

While there is no single 'silver bullet' to address and resolve all the challenges posed by SOA, the techniques described in this paper are helpful to achieve compliance.

One of these techniques, QCR3000, which is accredited by the Institute of Management Specialists, may be combined with other tools or methods, as it appears comprehensive and lends itself to web service style applications.

QCR3000 embraces a number of features:

1. Questionnaire-template adaptable and flexible scoring;
2. Information gathering, workshops etc;
3. Business process, data security and system application analysis;
4. Project planning, progress briefings and presentations;
5. PID (project implementation document) construction;
6. Project scope and work package definitions;
7. Roles and responsibilities and action points;
8. Deliverable reports and outline solutions;
9. Working together with the company's finance, accounting, audit, external advisors, operational-business people, IT department, system application users, third party suppliers and outsource service providers;
10. Integrating SOA compliance with business balance scorecard (above);
11. Solution build, including web service integration;
12. QA/QC verification;
13. Testing;
14. Training;
15. Solution rollout.



Abe Abrahami works for Peach (registered as quality compliance limited). Peach delivers business change, Sarbanes-Oxley, and other compliance, including information storage and management solutions, and related processes and procedures. It also runs workshops and training courses. For more information call Abe Abrahami on +44 (0)795 007 1830, email: info@peachqc.com or visit www.peachqc.com (under construction).