Val-Ed™

Valiant Technologies Education & Training Services

SOX – Structure & Implementation

Welcome to Valiant Technologies. We are a specialty consulting and training organization that focuses on information security at the strategic and operational levels. With significant strength also in information security assurance services, Valiant CISSTech, as were formerly known, has been serving clients across many countries - Bahrain, Hong Kong, India, Kuwait, Malaysia, Maldives, Saudi Arabia, Sri Lanka, South Africa, Sultanate of Oman, Thailand, United Arab Emirates, and Zambia.

Val-Ed™, our educational services division offers a variety of ready-packaged and tailor-made educational and training programs in the area of information security. This catalogue provides detailed information on one of the educational and training offering to clients in the area of information security technology, management and assurance.

We have a full range of services that we offer covering the full spectrum of information security and our services catalogue provides details of the following services that we provide to clients. Please ask for a services catalogue for more details on these services:

- Testing and hardening of information system defenses:
  - Vulnerability assessment
  - Penetration testing
  - Application security testing
  - Hardening of servers and network components
  - Periodic evaluation of network security
- Information Security Management Services
  - Security Policies, Procedures and Guidelines
  - Security Awareness Program
  - Risk Assessment and Analysis
  - Executive Management briefings on Security
  - Vendor selection for security products
  - Computer Forensics Investigation\
  - ISO-27001 preparatory services
  - Fill-in Security Manager program
- Control and Assurance Services
  - Gap analysis against ISO-27001, COBIT, ISSAF
  - Information security controls review
  - Information Systems Security Audit
  - Control assessment for SOX compliance
- Business Continuity and Disaster Recovery Management

We look forward to being of service to you and look forward to hearing your interest.

- Valiant Team

List of regular programs offered by Valiant Technologies

	Course Name	Duration (days)
1	Workshop for CISSP certification aspirants	4
2	Workshop for CISA certification aspirants	5
3	Workshop for CISM certification aspirant	4
4	Workshop for CBCP certification aspirants	5
5	Workshop for Security+ certification aspirants	6
6	Workshop on BCP and DRP	2
7	Workshop on Change Management	1
8	Workshop on Information Security Policies	3
9	Information Security for Senior Management	½
10	Security Awareness for IT user management	2
11	Ethical Hacking and securing your networks	6
12	Sarbanes Oxley Act – Structure and Implementation	2
13	Digital Evidence for IT / IS Auditors	1
14	IS Audit: Principles and Practices	3
15	ISO 27001: Process and Implementation	5
16	Auditing Information Technology	3
17	Management for Technology Professionals	3

CV of principal instructor, Dr. Rama K Subramaniam is found on the last page

Sarbanes Oxley Act – Structure and Implementation

If Companies view the new laws as opportunities to improve internal controls, improve the performance of the board and improve their public reporting – they will ultimately be better run, more transparent and therefore more attractive to investors
--- William Donaldson, Chairman,
Securities and Exchange Commission, USA

Sarbanes Oxley Act, 2002 (SOX) was discussed and enacted into law by the 107th Congress of the United States that began on the 23rd of January, 2002. The culmination of efforts by Senator Paul Sarbanes and Representative Michael Oxley to bring into being a comprehensive legislation to remedy the situation arising out of corporate failures in quick succession and falling investor confidence. While it had long been recognized that internal controls is the responsibility of top management, this law formalizes this recognition and sets it in a firm and enforceable legal framework. SOX requires senior management and business process owners to establish and maintain an adequate internal control structure. In addition and perhaps more importantly, it expects them to assess the effectiveness of the control system on an annual basis.

Hardly any enterprise today can have an internal control system that is not dependent on information technology. Recognizing this relationship well, the Public Companies Accounting Oversight Board (PCAOB) states in its Accounting Standard No. 2 that *"the nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting."* Formalizing the process, SOX identifies certain managerial positions as certifying officers and expects that they make periodic certifications with respect to the internal controls in the organization with special reference to financial reporting.

Professionals who are in positions of responsibility under SOX for ensuring internal controls and attesting to its effectiveness are therefore faced with the following set of challenges:

1. Getting to be well versed in Internal control theory and practice so as to be comfortable certifying the effectiveness of the internal controls
2. Developing and monitoring a plan of action for compliance with SOX requirements
3. Identifying IT controls in the organization and re-aligning them to be compliant with SOX requirements
4. Doing a periodic gap analysis between compliance to internal control requirements as found in SOX and the internal controls as found in the organization. To put in place a mechanism to constantly reduce the gap, as found.

The above is a general set of challenges and additional organization specific challenges would be found in many cases. It is becoming increasingly clear that SOX compliance is not restricted to the internal control professionals or the internal auditors or the IT / Security professional in organizations.

It is the responsibility of all business process owners to comply with the internal control requirements of SOX. In the US, the SEC in its final ruling on the use of a recognized internal control framework has made references to the Committee of Sponsoring Organizations of the Treadway Commission (COSO). There have been cases where SEC registrants who had to comply with SOX had found that they have to move beyond the COSO framework as far as IT controls are concerned in order to be fully compliant. PCAOB too, while discussing the importance of IT controls, have not clearly pointed to any framework that could serve as a guidepost for establishing and / or assessing IT controls. Some control frameworks that could be used include COBIT of ITGI, ISO17799 and ITIL. However, given the comprehensiveness of COBIT, it is emerging to be a preferred framework to govern the IT controls that are part of SOX compliance process.

In India, the move towards greater disclosure and better corporate governance amongst public companies is taking the form of Clause 49 of the listing agreement governing listed companies. The initiative by the Government, Stock Exchanges and SEBI in bringing this clause as part of the listing agreement clearly indicates that governance and control issues are becoming relevant and significant in corporate India. While Clause 49 of the Listing Agreement may not be the same as SOX, it is appropriate for Indian conditions. In this workshop, alongside SOX, the relevant provisions of Clause 49 of the Listing Agreement, as envisaged now, will be presented and discussed.

This workshop presents the structure and implementation process that conforms to SOX for a listed company and also considers the control and governance requirements in the Indian context.

Who should attend?

- Senior Mangers who are responsible for SOX compliance
- Senior Managers who are concerned with Clause 49 of Listing Agreement in India
- Financial auditors and analysts – Chartered Accountants, CPAs, CFAs
- Company Secretaries
- Certified Internal Auditors, Internal Audit Managers
- IS Auditors – CISAs
- IT professionals involved in establishing and assessing controls
- Banking professionals
- Credit institutions including credit card issuers and credit rating agencies
- Academicians in the areas of finance, control, general management and IT

Agenda - Day 1

Session 1: The SOX Setting – Focus on Internal Controls.

The preamble to the Sarbanes-Oxley Act, 2002 states that it is an act "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws…" While avowedly it is an investor protection instrument, it has a complex structure and encompasses a wide area of governance and control issues all aimed at better governance, improved internal controls and performance measurement systems. While most discussions on SOX have focused on Sections 302 and 404, the Act has a large number of inter-twined provisions that will have an impact on the performance of those responsible for the creation and maintenance of appropriate internal controls in the organization. The 69 sections spread over 11 titles or divisions all point to a basic premise that good governance and ethical business practices are no longer optional bonus offered to investors; they are integrated into business necessities. This session would present the overall structure of SOX and present the concept of "internal controls" in perspective.

Session 2: Foundation for Reliable Financial Reporting

Reliable financial reporting is the guiding spirit in any corporate governance legislation. So is it with SOX. While the focus is ostensibly on financial reporting system, the process that culminates in the financial reporting system is inextricably linked to information technology systems. Recognizing this interrelationship, PCAOB clearly states that any assertion under the requirements of SOX should be after evaluating the nature and complexity of the systems, including the use of information technology by which the company processes and controls information supporting the assertion that those internal controls are effective. This session would provide the foundation for a structured understanding of control environment and structure within an organization and assurance framework.

Session 3 & 4: COSO Framework & use of COBIT:

SOX focuses on internal controls and their effectiveness. The first question often asked is whether there is a recommended or a preferred structure of internal controls that is appropriate to implement. SEC, which has taken significant interest in monitoring implementation of SOX driven control systems and structures, has clearly mandated that listed corporations use a recognized internal control framework established by a body or group that has followed due process and procedures. SEC has also made specific references to COSO. PCAOB's Auditing Standard No. 2 explicitly states that "the directions in the proposed standard are based on COSO framework." The Standard further recognizes that other standards are already in vogue or may evolve in other countries. While recognizing that these standards may not have the same elements as COSO, these other standards should have elements that encompass all of COSO's general themes.

Given the importance attached to COSO in SOX implementation and reporting, this session would present a comprehensive discussion on COSO, its structure, contents and implementation.

While the framework of COSO is broad enough to encompass the internal control structure generically, enterprise managements need clarity on identification, documentation and procedural guidelines for implementing effective IT controls. From among the various IT control objective listings found in different documents, COBIT is chosen for its comprehensiveness and for providing activity level objectives for IT controls. This session will assist participants to align the COBIT control objectives to SOX at an activity or functional level.

Agenda - Day 2

Session 1 & 2

This key session would be spread over two sessions and present a road map to ensuring compliance with SOX requirements. Compliance with SOX is neither limited to understanding the financial reporting cycle nor is it focused on the IT process that leads to reliable financial reporting. The entire compliance program should be business process led. This session would provide a project plan for SOX implementation and cover the following main parts:

- Planning and scoping the management initiative

  This stage involves an understanding of how the financial reporting process works and also determines IT controls that would have an impact on the process. This stage also identifies the technology involvement in the reporting process. As examples, the following areas need understanding in this stage of implementation cycle: controls over operations of IPF handling financial data; controls over all applications processing data that would end up in the reporting process; organizational and administrative controls; controls over handling of non-routine process, etc.

- Risk Assessment

  The SOX compliance officer would be required to rely significantly on the results of the risk assessment performed on the various IT assets and components that are identified at the stage of planning. Where the risk assessment is incomplete or has not been performed, a decision has to be made on the impact of such incomplete or non-existent risk assessment. Where risk assessment results are available, such results form the first step toward the determination of effectiveness of controls that are principally aimed at mitigating the assessed risks

- Understanding important business units/locations and corresponding controls

  Going by COSO, two broad genres of controls would be relevant to all organizations; viz. Application Controls and General Controls. The former deals with specific business processes that govern the correctness and completeness of processing information through the automated processes. These controls working in conjunction with manual and physical controls ensure the reliability of applications whose end results often find their way into final reporting to stake holders. General Controls refer, *inter alia*, to secure transactions including logical and availability controls. It is important that appropriate control objectives are set and used to assess these controls and in the process, those responsible for compliance will be required to relate these control objectives to critical business units and processes

- Documenting controls

  It is often said that an undocumented control is no control at all. Even those enterprises that have effective controls in place do not have appropriate documentation. The challenge of documenting existing and new controls needs careful attention in terms of evolving a time line and allocating sufficient resources to complete the documentation. The position in this regard is best summarized by PCAOB when it states "the more clearly management documents its internal control over financial reporting, the process used to assess the effectiveness of the internal control, and the results of that process, the easier it will be for the auditor to understand the internal control, confirm that understanding, evaluate management's assessment, and plan and perform the audit of internal control…"

- Evaluating control design and operating effectiveness

  The relevance of control design in evaluating the effectiveness needs no over-emphasis. The control attributes that go into the design of the control systems have a significant bearing on its implementation and effectiveness. The business process, in turn, controls the attributes. Given the importance of assessing the appropriateness of control design and its operating effectiveness, a grid similar to that used in CMM (Capability-Maturity Model) is recommended for assessment of the control design and effectiveness. The six-stage model is used to fit current organizational position into one of the following:

  1. Stage – 0: Non-existent
  2. Stage – 1: Initial / Ad-hoc
  3. Stage – 2: Repeatable but intuitive
  4. Stage – 3: Defined Process
  5. Stage – 4: Managed and Measurable
  6. Stage – 5: Optimized

- Identifying and correcting deficiencies

  The process of assessing and determining whether or not the organization has implemented effective internal controls cannot lead always to a dichotomous answer: Yes or No. More often than not, it would be in-between a typical "Yes" and a typical "No." Assurance professionals have found it appropriate to place the results of their assessment as being either *inconsequential shortcoming* or a *significant deficiency* or a *material weakness*. Each of these classifications of findings will lead to a different kind of follow up action. While SOX is definitely an assurance driven initiative, it lays equal emphasis on gap analysis and bridging the gap.

Session 3 & 4: Case Study Delegates Participation and presentation

Participants in this program will be divided into smaller groups and will be provided an opportunity to discuss a case study that would cover major elements that need to be addressed while preparing for and implementing SOX. Team leaders of each of the group would present their findings to the audience with the workshop facilitators adding value to the discussions as appropriate.

Participants to the workshop would be divided into groups such that each group has the right combination of skill sets for project management, IT controls, COBIT knowledge and the group would prepare a comprehensive plan for SOX implementation. In view of the limited time available, the workshop participants would be provided with templates that can be used for this case study session. These templates are expected to add value to the participants in their professional work.

Dr. Rama K Subramaniam

MBA(UK), PHD, FCA, CISA, CISM, CISSP, CEH, CHFI, CSQP, MCSE, Security+

He is Director of Valiant Technologies Pvt Ltd and Tejas Brainware Systems Pvt Ltd. He has been an information security consultant, trainer and educator for over a decade. He has trained experts in many information security domains across Gulf nations, India, Far East and Africa. He is a consultant to a number of organizations in the commercial, government, armed forces, judiciary and law enforcement segments in these countries.

He serves as India's country representative at International Federation of Information Processing (IFIP), serving on their Technical Committee TC-11 dealing with information security. He is current Chairman of ISCCRF, a not-for-profit trust carrying out research in cyber crime management

He is a certified and experienced professional in the areas of creating and implementing secure information security architecture; internal controls systems and processes; conceptualization, creation, testing and maintenance of business continuity and disaster recovery plans; security audits and certification of network infrastructure; conceptualization and implementation of multi-factor authentication processes (including PKI and X.509 compliant certification infrastructure); creation, assessment and certification of SOX, COSO, CoBIT, ISO-27001, ISO-17799 and ISO-15408 compliant information security management systems.

He served earlier as Global Chair of the Education and Awareness Principles Expert Group of Globally Accepted Information Security Principles (GAISP), based in the United States and is former Global Chair of the Accreditation Process committee of Open Information Systems Security Group (OISSG), based in the UK where he estblished their certification and accreditation processes. He is the charter President of the first chapter of ISSA (Information Systems Security Association) in Asia and served on the boards of Dubai and Chennai chapters of ISACA.

He was formerly Managing Director of Thewo Corporate Services based in Lusaka, Zambia; Group Operations Director or Benetone Group of Companies based in Bangkok, Thailand and Commercial Director of Dynaspede Integrated Systems Ltd, based in Mumbai.