Val-Ed™

Valiant Technologies Education & Training Services

ISO-27001 Process & 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 Technologies 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

Five day Workshop on

Understanding & Implementing ISO-27001 compliant ISMS

Workshop Description	Workshop Benefits & Methodology
Managers and others responsible for the information security function within an organisation regard ISO 27001 as a comprehensive guideline and reference document. It is intended provide a strategic and operating guideline to management of information security. It may be regarded as a basis upon which to build best practices driven security management system. Valiant Technologies has designed and offered many workshops covering information security management systems during the past many years in different parts of the world including India, Thailand, Zambia, the UAE, Bahrain, Oman, Saudi Arabia, Kuwait, and Sri Lanka.	• Acquire a thorough understanding of ISO-27001 from an audit and implementation perspective • Practical approaches and techniques that would enable participants to transfer this knowledge into business value-add upon return to their work desks • Since the principal instructor has assisted many companies to become compliant with ISO-27001 requirements, participants will benefit from real life case studies and practical examples • Effective knowledge transfer using case studies and group work where participants implement controls in a simulated environment
Who should attend?	**Logistics**
▪ IT Manager ▪ IS Managers ▪ IS/IT Auditors ▪ Internal Audit professionals ▪ Information Security Managers and professionals ▪ CISA / CISM / CISSP holders ▪ Quality Assurance Professionals ▪ Operations managers desiring to implement ISO compliant ISMS systems	Duration: Five days Timings: Seven hours daily with appropriate breaks Participants will be formed into teams for carrying out exercises that reinforce the learning objectives at the end of presentation covering each major domain
Broad Content Areas	
▪ Establish ISMS ▪ Implement & operate ISMS ▪ Monitor and Review ISMS ▪ Maintain and Review ISMS ▪ Documentation Requirements ▪ Management Responsibility ▪ Resource Management ▪ Training, Awareness & Competence ▪ Continuous improvement of ISMS	▪ Security Policy ▪ Information Security Organization ▪ Asset Management ▪ Human Resource Security ▪ Physical & Environmental Security ▪ Communications and Operations ▪ Access Controls ▪ IS Acquisition, Development & Maintenance ▪ Security Incident Management ▪ Business Continuity Management ▪ Compliance

The eleven broad requirements of an Information Security Management System (ISMS) as envisaged by ISO 27001 are briefly presented here and would constitute a major part of the presentation, discussion and group work. Wherever appropriate, the control requirement is briefly reproduced verbatim from the ISO 27001 document though in many cases, edited versions are presented in many of the following sections.

1. Information Security Policy:

The primary objective of this broad control area is to provide management with direction and support for information security in accordance with business requirements and relevant laws and regulations. Recommended processes include –

- Setting out the organization's policy for the protection of confidentiality, integrity and availability of its information assets, *viz.*, hardware, software and information handled by information systems, networks and applications.

- Establish the responsibilities for information security

- Provide reference to documentation, which comprises the complete ISMS.

2. Organization of Information Security

The primary control requirement is that a management framework be established to initiate and control the implementation of information security within the organization. Suitable management forum with appropriate leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization.

If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, *eg*. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as risk management.

3. Asset Management

The control requirement is that all major information assets should be accounted for and has a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

4. Human Resource Security

The requirement under this key control area includes attaching significant importance to the HR security aspects of ISMS. Controls should ensure that security responsibilities be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment. Potential recruits should be adequately screened, especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality and non-disclosure agreement.

5. Physical and Environmental Security

The primary goal of this control measure is to prevent unauthorized access, damage and interference to business premises and information. This requirement is expected to be achieved by ensuring that critical or sensitive business information processing facilities be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

6. Communications and Operations Management

Given that the primary goal of this branch of ISMS is to ensure the correct and secure operation of information processing facilities, various technical controls are discussed in this segment of ISMS. Responsibilities and procedures for the management and operation of all information processing facilities are required to be established. This includes the development of appropriate operating instructions and incident response procedures. Segregation of duties is recommended for implementation, where appropriate, to reduce the risk of negligent or deliberate system misuse.

7. Access Controls

Within the broad objective of wanting to control access to business information, this covers policies and practices for information dissemination and authorization.

This covers both technical and organizational controls governing access to business assets at the user level, network level, in mobile computing and data in storage and in transit.

8. Information System Acquisition, Development and Maintenance

This will include infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the acquisition or development of information systems. All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

9. Information Security Incident Management

The primary purpose of the set of controls in this domain is to ensure that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. It also requires that appropriate controls be put in place to ensure that a consistent and effective approach be applied to the management of information security incidents

10. Business Continuity Management

The primary goal is counteracting interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. To achieve this, businesses must establish a business continuity management process.

This should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

11. Compliance

The principal goal of controls in this area is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

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.