Val-Ed™

Valiant Technologies Education & Training Services

Workshop for CISA Aspirants

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 we 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

Workshop Description	Workshop Benefits & Methodology
Certified Information Systems Auditor (CISA) certification, designed and administered by the Information Systems Audit and Control Association (ISACA) is by far the most preferred certification to perform attest and assurance function in an IS environment. The purpose of the examination, as stated by ISACA, is to evaluate a candidate's knowledge and experience in conducting information systems audit and reviews. Valiant Technologies has designed and offered many workshops for aspirants of this certification during the past many years. This is one of our oldest programs and we have taught this for over twelve years in different parts of the world including India, Thailand, Zambia, the UAE, Bahrain, Oman, Saudi Arabia and Sri Lanka.	This course would provide a review of the domains of knowledge on which candidates are examined in the CISA examinations so that they have a good understanding of the concepts and principles of information systems audit and control; both for the examination and in their professional practice as auditors. The program is designed to explain the concepts contained in the domains of knowledge examined in the CISA examination and also making the participants comfortable with handling real life situations involving the concepts learned. Such an approach would be particularly useful in CISA type examinations where questions often tend to evaluate if the candidate has appropriate exposure to real like scenarios
Who should attend?	**Instructor**
Primarily for CISA aspirants, this program would also be beneficial to: ▪ Systems Administrators who need a better understanding of information assurance mechanisms ▪ Auditors requiring a generic view of information assurance & governance. ▪ IT Mangers who may want to integrate attest and assurance functions into their activities	The principal instructor for this course is Mr Rama K Subramaniam who has successfully conducted many workshops for CISA aspirants both as public programs and as in-house programs for very large corporations during the past twelve years. He has also contributed to the CISA review manual in the past. His CV is available later in this brochure
Broad Content Areas	
▪ The IS Audit Process ▪ IT Governance ▪ System and Infrastructure Lifecycle Management	▪ IT Service Delivery and Support ▪ Protection of Information Assets ▪ Disaster Recovery and Business Continuity

Thought Leadership...
Valiant Technologies

Workshop Contents based on the Content Area and Knowledge Statements published by Information Systems Audit and Control Association, Inc. [ISACA]

IS Audit Process

Participants are trained for the primary task of *"providing IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled."*

Approximately 10% of the examination questions are expected from this domain. Candidates are expected to demonstrate knowledge of IS Audit practices and techniques in line with ISACA IS Audit Standards, Guidelines & Procedures and Code of Professional Ethics. Starting off with risk assessment in an audit context, this domain considers audit planning and management issues, reporting and communication of audit results including facilitation, negotiation and conflict resolution that may arise between auditor and auditee. Presentations in this domain will cover requirements of techniques to gather information including observation, interviews, inquiry, use of CAATs, and other electronic means of data capture and analysis. A good grounding will be provided on how preserve evidence through appropriate processes of collection, protection, analysis, interpretation and chain of custody. This domain would also familiarize participants with COBIT, Control Self Assessment and Continuous Audit Techniques.

IT Governance

This domain expects candidates to have knowledge and skills to assure *"that the organization has the structure, policies, accountability, mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT."*

Approximately 15% of the questions in the examinations are expected from this domain. Candidates would be taken through the process for development, implementation and maintenance of IT strategies, policies, standards and procedures and exposed to some of the control frameworks - COBIT, COSO & ISO 17799 in addition to generally accepted international IT standards and guidelines. Good knowledge is expected of IT Governance frameworks coupled with exposure to monitoring and reporting IT performance via balanced scorecards, KPIs and CSFs, which would be presented in detail in the sessions. Participants would understand issues relating to IT resource investment and allocation practices.

System & Infrastructure Lifecycle management

This domain expects candidates to have knowledge and skills required to *"assure that management practices for the development / acquisition, testing, implementation, maintenance and disposal of systems and infrastructure will meet the organization's objectives."*

Approximately 16% of the questions in the examinations are expected from this domain. Focus will be on understanding project governance practices, project management practices, risk management tools and techniques as applied to project management, critical success factors of IT projects, configuration, change and release management processes. Candidates will also be taken through system development methodologies, quality assurance methods, management of testing processes, hardware and software certification and accreditation processes. Candidates would also be familiarized with post implementation review process, system migration and deployment practices.

IT Service Delivery & Support

This domain expects candidates to have knowledge and skills to *"provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives."*

Approximately 14% of the questions in the examinations are expected from this domain. With primary focus on service level management practices, candidates are expected to be familiar with operations management best practices, systems performance monitoring processes, tools and techniques and functionality of hardware and network components. Participants would be exposed to database administration practices and functionality of system software from an assurance and audit perspective. Knowledge of capacity planning and monitoring techniques will be a key focus area. This domain of knowledge includes processes for managing scheduled and emergency changes to the production systems and /or infrastructure including processes and assurances relating to change, configuration, release and patch management practices. Presentations covering this domain will examine system resiliency tool including fault tolerant systems, elimination of single point of failure, clustering, electronic journaling and electronic vaulting.

Protection of Information Assets

This domain expects candidates to have knowledge and skills to *"provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets."*

Approximately 31% of the questions in the examinations are expected from this domain. This domain provides clear understanding of information security management, including understanding of cyber crimes, hacking and malware related issues. It provides significant focus on exposures and controls in logical access to information assets fully considering the IA3 paradigm. LAN, WAN and Internet exposures, vulnerabilities, countermeasures and audit process are explained in detail. The basic components of a typical security architecture including Firewalls, IDS, VPN, Anti-Virus and Content control are studied in sufficient detail required to carry out an audit. Symmetric and Asymmetric cryptographic applications including Digital Signatures, PKI, TTP, CA and RA are discussed in detail. Physical and Environmental exposures, vulnerabilities and countermeasures are presented so assist in building an audit program in these areas. The domain is completed with an introduction to computer forensics and wireless vulnerabilities and controls

Business Continuity & Disaster Recovery

This domain expects candidates to have knowledge and skills to *"provide assurance that in the event of a disruption the business continuity and disaster recovery process will ensure the timely resumption of IT services while minimizing the business impact."*

Approximately 14% of the questions in the examinations are expected from this domain. The primary goal of any BCP and DRP is to restore the organization's business capabilities to the pre-accepted level of performance within the MTD or RTO. Also involved is the process of ensuring that the RPO requirements are fully met. Presentations in this domain start off with understanding the BC and DR plan initiation and move on to carrying out a Business Impact Analysis [BIA]. The results of the BIA would influence the choice of recovery strategies and having chosen from among alternative strategies, a clear plan is evolved, tested and maintained. Candidates will also be taught the components of a plan, the issues in recovery cycle management and the process of carrying out an audit to determine the efficacy of the BC and DR Plans.

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.