Val-Ed™

Valiant Technologies Education & Training Services

Workshop for CISM aspirants

All Trademarks and Copyrights recognized

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

Workshop Description	Workshop Benefits & Methodology
Certified Information Security Manager (CISM) is ISACA's certification program for information security mangers with experience in managing information security in corporate enterprises. According to ISACA, CISM is designed to provide executive management with assurance that those earning the designation have the required knowledge and ability to provide effective security management and consulting. It is business-oriented and focuses on information risk management while addressing management, design and technical security issues at a conceptual level. While its central focus is security management, all those in the IS profession with security experience will certainly find value in CISM. Valiant Technologies has designed and offered many workshops for aspirants of this certification during the past few years.	This course would provide a review of the domains of knowledge on which candidates are examined in the CISM 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 CISM examination and also making the participants comfortable with handling real life situations involving the concepts learned. Such an approach would be particularly useful in CISM type examinations where questions often tend to evaluate if the candidate has appropriate exposure to real like scenarios
Who should attend?	**Instructor**
Primarily for CISM aspirants, this program would also be beneficial to: ▪ IS / IT Managers who need a better understanding of information security and governance mechanisms ▪ Auditors requiring a generic view of information security & governance. ▪ IT Mangers who may want to integrate security and governance functions into their activities	The principal instructor for this course is Mr Rama K Subramaniam who has successfully conducted many workshops for CISM aspirants both as public programs and as in-house programs for very large corporations during the past few years. His CV is available later in this brochure
Broad Content Areas	
▪ Information Security Governance ▪ Risk Management ▪ Information Security Program[me] Management	▪ Information Security Management ▪ Response Management

Thought Leadership...
Valiant Technologies

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

Information Security Governance

Participants are trained for the primary task of "Establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations."

Approximately 21% of the examination questions are expected from this domain. Candidates are expected to demonstrate knowledge of information security concepts and relate them to business operations. Candidates should know methods to get executive management buy-in for information security governance and integrate it with enterprise governance mechanisms. Knowledge of governance related issues including risk management, data classification management, network security, system access processes are expected to be known by the candidates while answering questions in this domain.

Risk Management

Participants are trained for the primary task of "Identifying and managing information security risks to achieve business objectives."

Approximately 21% of the examination questions are expected from this domain. Candidates are expected to have sufficient expertise in developing a systematic, analytical and continuous risk management process in the organization by integrating the process of risk identification, analysis and mitigation activities. As part of the information security risk management process, candidates are expected to define strategies and prioritize options to mitigate risk to levels acceptable to the organization. As part of risk management process, candidates are expected to understand the need to create and implement a process to report significant changes to risks on a periodic and event-driven basis.

Information Security Program[me] Management

Participants are trained for the primary task of "Designing, developing and managing an information security program(me) to implement the information security governance framework."

Approximately 21% of the examination questions are expected from this domain. Candidates are expected to have knowledge that would enable them to create and maintain plans to implement the information security governance framework starting off with development of information security baselines and develop procedures and guidelines to ensure business processes address information security risks. Information security is the responsibility of all people in an organization and in keeping with this, candidates are expected to have knowledge and skills to promote accountability of business process owners and stakeholders in managing security risks.

Information Security Management

Participants are trained for the primary task of "Overseeing and directing information security activities to execute the information security program(me).

Approximately 24% of the examination questions are expected from this domain. Candidates should be in a position to design and implement rules that ensure that the user of the organization's information systems comply with the organization's information security policies. Candidates are also to ensure that the administrative procedures for enforcing information security policies are in place and that the security policies govern the services provided by third party vendors and consultants to the organization. Whenever a change management process is implemented in the organization, a process is in place to ensure that the change does not diminish the security levels required for the process and that that all change management processes consider security as a key variable before deciding on the change.

Response Management

Participants are trained for the primary task of "Developing and managing a capability to respond to and recover from disruptive and destructive information security events."

Approximately 13% of the examination questions are expected from this domain. Candidates would be expected to demonstrate that they have the requisite knowledge and skills for development and implementation of a process for detecting, identifying and analyzing security related events. Given that security events have been identified, the candidates are expected to know how to develop response and recovery plans including organizing, training and equipping recovery process. Apart from testing these plans to ensure that they stay current, candidates should also understand how to bring these plans to action whenever a security incident occurs.

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.