

# Val-Ed<sup>TM</sup>

Valiant Technologies  
Education &  
Training Services

---

## Workshop for CISSP 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

	<b>Course Name</b>	<b>Duration (days)</b>
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
<p>CISSP was created by ISC2 (<a href="http://www.isc2.org">www.isc2.org</a>) as an industry standard to test and certify candidates' proficiency in information security best practices. This certification is a combination of testing candidates' proficiency in information security best practices, relevant experience, conformance to ethics and continuing educational credits.</p> <p>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 five years in different parts of the world including India (Chennai &amp; Bangalore – multiple times), Thailand, UAE (Dubai and Abu Dhabi – multiple times), Bahrain (multiple times), Oman (multiple times), Saudi Arabia (Al-Khobar and Riyadh – multiple times), Kuwait and Sri Lanka (multiple times).</p>	<p>Participants in this program would learn the foundations of contents of the ten domains of knowledge expected to be known by CISSP aspirants. It would not only prepare the participants to take the CISSP examinations but would also significantly add to their knowledge base enabling them to perform better on their jobs as information security professionals.</p> <p>Classroom style presentations, extensive interactive sessions and quizzes. Before the course starts, all participants write a multiple choice test to assess their level of understanding of the contents of the ten domains of knowledge which would assist the faculty to fine tune their presentations to assist participants who may need special attention.</p>
Who should attend?	Instructor
<p><b>Primarily for CISSP aspirants</b>, this program would also be beneficial to:</p> <ul style="list-style-type: none"> <li>▪ Systems Administrators who need a better understanding of information security mechanisms</li> <li>▪ Auditors requiring a generic view of information security assurance</li> <li>▪ IT Mangers who may want to integrate security functions into their overall IT plans and activities</li> </ul>	<p>The principal instructor for this course is Dr K Rama Subramaniam who has successfully conducted many workshops for CISSP aspirants both as public programs and as in-house programs for very large corporations during the past five years. He has to his credit hundreds of CISSPs who have gone through his sessions. His CV is available later in this brochure</p>
Broad Content Areas	
<ul style="list-style-type: none"> <li>▪ Security Management</li> <li>▪ Cryptography</li> <li>▪ Telecom and Network Security</li> <li>▪ Access Controls</li> <li>▪ Security Architecture and Models</li> </ul>	<ul style="list-style-type: none"> <li>▪ Application Security</li> <li>▪ Operations Security</li> <li>▪ Physical Security</li> <li>▪ Law, Investigation &amp; Ethics</li> <li>▪ BCP and DRP</li> </ul>

Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines aimed at securing those assets. This domain would expose participants to risk management concepts, and the process of identification, measurement, control and minimization of loss associated with uncertain events. It would include presentations in change control methodologies, personnel policies and practices in so far as they impact information security policies, security awareness programs and training initiatives for enforcing security in the organization.

---

## Security Management

Cryptography is vitally important to information security. One of the main goals of cryptography is to help frustrate the attempts of eavesdroppers. Communicating over any kind of medium has the inherent risk of an unauthorized third party listening in, and cryptography minimizes that risk. Although there are many ways to perform cryptography, most follow similar methodologies.

## Cryptography

This domain covers a study of both symmetric and asymmetric crypto systems and their implementations as security mechanisms. A detailed understanding of the architecture and implementation of asymmetric crypto systems follow a thorough study of the symmetric family of cryptosystems. Participants in this workshop will understand the design and implementation of digital signatures and the security processes and assurances that are associated with it. The session presents some common and powerful implementations of crypto systems in networks and web applications before considering the various forms of attacks on cryptosystems.

This will include both management and technology of securing information networks. The managerial part of this area of study will include remote access management, IDS, incident response and management, network availability considerations, redundancy including RAID, back-ups and managing single points of failure.

## Network and Telecom Security

The technological issues would include OSI model, layered architecture concepts, TCP/IP protocol, security enhanced and security focused protocols. Applications in LAN and WAN environments would be discussed from a security perspective. Security issues in communication networks would be considered along with discussions on detection, defense and proactive measures to secure networks and communication links.

The architecture of the Internet and how it is inherently insecure would be considered for a good understanding of the contents of this domain of learning. Attacks that are typical in an internet based environment would be considered alongside protective mechanisms including Firewalls, IDS, VPNs, etc. Issues such as password protection, virus prevention and management and IPSec, which provide good protection when supported by a strong and relevant security policy framework would be discussed.

Access controls represent a collection of physical and logical mechanisms that work together to implement security architecture to protect the information assets of any enterprise. It permits owners and custodians of information systems to exercise a directing or restraining influence over the behavior, use and content of a system. Access Control methods provide for establishment and implementation of mechanisms that relate various subjects to objects in an organization in terms of accessibility of the former to the latter. The access rights and relationships would be mapped to the Trusted Computing Base established in terms of the security policy. The participants would study access control concepts; techniques and implementations within both centralized and distributed computing environments

## Access Controls

---

This domain of knowledge covers some of the well known information security architectures, models, structures and standards for evaluation, implementation, enforcement and accountability. Different approaches to information security modelling to take care of the requirements of confidentiality, integrity and availability would lead the participants to implement security technologies adhering to security policies. In addition, these sessions would also discuss Common Criteria (CC) for IPF evaluation, ITSEC, TCSEC and related evaluation methods. The cryptography domain addresses the principles, concepts and methods of encrypting information to ensure its integrity, confidentiality, authentication and non-repudiation of transactions

## **Security Architecture & Models**

---

Good application development includes considering and implanting security and controls at each stage of systems development process. Irrespective of the development methodology used, due consideration to security and control is required for all application development process whether they are intended for distributed or centralized processing environment. Applications could include software, agents, databases, data warehouses, applets, and knowledge management systems. The integration of security control architecture with application development process leading to protecting applications against some of the common forms of attacks will be the core focus of this module of learning.

## **Application Security**

---

Operations Security is used to identify the controls over information processing assets and link access privileges of owners, operators and administrators to any of these assets. It also includes audit and monitoring of the mechanisms, tools, and facilities that are aimed at identification of security events and subsequent actions to identify the key elements and report pertinent information. Participants would be able to identify resources that require to be secured and determine restrictions to be placed on privileges granted to users of IPF.

## **Operations Security**

---

Participants would be familiarized with the different legal systems that address issues of computer crime handling and management from the legal and investigative perspective. In addition, the investigation cycle would be fully discussed. Security professionals often have to resolve situations in the light of conflicting demands and adherence to ethics could provide a good guidepost in such circumstances. RFC 1087 and ISC2 code of ethics would be discussed in this session.

---

## **Law, Investigation & Ethics**

The best first line of defense against security infraction at the IPF is restricting physical access to the information assets and processing facilities. Discussions would relate to this aspect of information security and would cover issues relating to choice of secure site, its design and configuration, and the suite of methods to protect against unauthorized access.

---

## **Physical Security**

This section addresses the restoration and recovery of business operations in the event of business discontinuity and disaster events. The process of preparation, testing and updating of the plans to protect critical business information assets and protections against system and network failures would be discussed in this session. A good first step to effective planning against factors adversely impacting business continuity is the performance of Business Impact Analysis (BIA) and participants would be taken through a structured approach to BIA. The Disaster Recovery Plan – DRP – includes procedures for emergency response, extended back-up and recovery operations, incident management practices and shift to hot/warm/cold alternative sites. The process cycle is completed when the organization reverts to the original site.

---

## **BCP & DRP**



### **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 established 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.