V-Tech

Valiant Technologies – Training Offerings

5 – day workshop for CBCP aspirants

Welcome to **Valiant Technologies.** We are a specialty consulting and training organization that focuses on information security at the strategic and operational levels. We have 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. We were formerly known as Valiant CISSTech.

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 technology, management and assurance.

Valiant offers certification oriented, custom made and generic non-certification training and education programs:

- *Certification oriented* – Pioneering efforts have been made by Valiant to bring in a new learning experience in a variety of information security related certifications in our target market region – South Asia and the Middle East. This includes workshops for the aspirants of certifications like CISSP, SSCP, CBCP, CISA, CISM … Our expert faculty blend real-life experience with academic brilliance to bring to the class-room the best of learning experience for participants. These factors have contributed to Valiant's candidates attaining excellent scores in certification examinations and our enjoying well above the global pass rates for participants in our training programs.

  Most of Valiant trainings lead to vendor neutral certifications while a few vendor specific programs are also offered where the programs are highly focused on security like CCSP.

- *Custom made training programs* are designed and delivered to business enterprises, law enforcement, armed forces, judiciary and government departments after carefully assessing training needs of specific groups. The complete training process cycle of assessing training need, discussing and finalizing needs and training approaches with training managers or executive management, creating need-based courseware and delivering highly focused training programs are all done in conformance with IBSTPI competency standards.

- *Generic non-certification programs* – Not all skill sets required for a security professional result in a certification. Recognizing this and also recognizing that managers require upgrading of skills rather than prepare for examinations, Valiant offers training programs that are oriented towards imparting knowledge and skills that can be adapted to organizational requirements. Some of our highly successful programs in this category include Creation and Implementation of Information Security Policies, Executive Management Security Briefings, Security Awareness for users, Security Self Assessment…

Why Valiant

- We are pioneers in information security training in India and Middle East
- Our trainers are certified in their respective areas of specialization and have relevant industry experience
- Our instructional design and delivery conform to IBSTPI standards
- Our training programs blend theoretical rigor, industry practice knowledge, and excellent presentation skills
- Our programs have structured presentations supported by case studies and hands-on skill enhancement sessions
- Our programs have in-built evaluation modules to assist participants focus on areas requiring further knowledge or skill enhancement
- Our training program participants go back with appropriate knowledge, skills and requisite confidence needed to secure information assets.

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 provided on last page

Partial LIST OF CLIENT ORGANIZATIONS whose employees were trained by Valiant

Banks, Financial Services and Insurance

- Bank Dhofar, Muscat, Oman
- Oman Housing Bank, Muscat, Oman
- National Bank of Oman, Muscat
- Citibank, Bangkok, Thailand
- Indian Bank, Chennai, India
- Syndicate Bank, Bangalore, India
- Commercial Bank of Qatar, Doha, Qatar
- City Union Bank Ltd, Chennai
- ING Vysya Bank
- State Bank of Mysore
- Gulf Union Insurance, Saudi Arabia
- Vijaya Bank
- National Bank of Dubai
- National Bank of Sharjah
- Gulf Bank, Kuwait
- International Leasing & Investments, Kuwait
- Seylan Bank, Colombo
- New Union Insurance, Bahrain

Oil Industry

- Saudi Aramco, Dhahran, Saudi Arabia
- ADCO, Abu Dhabi, UAE
- PDO, Oman
- Kuwait Oil Corporation, Kuwait
- Dubai Petroleum Co, Duabi, UAE

Banking Regulators

- Central Bank of Oman, Muscat
- Reserve Bank of India, Chennai
- Saudi Monetary Agency, Riyadh
- Central Bank of UAE, Abu Dhabi, UAE

Telecom

- Saudi Telecom, Riyadh and Al-Khobar
- Omantel, Muscat, Oman
- VSNL, Chennai
- Etisalat, Abu Dhabi, UAE
- Batelco, Bahrain
- Gulfnet International, Kuwait

Military & Law Enforcement – Training & Advisory

- Abu Dhabi Police, UAE
- City Police Cyber Crimes Cell, Chennai
- Saudi National Guards, Riyadh
- Sultan's Armed Forces, Muscat, Oman
- Combat Support Associates of the US Army in Kuwait

Manufacturing and IT / ITES

- IBM, Bangalore and Bahrain
- HP, India
- Infosys
- Wipro
- Nestle – Middle East, Duabi, UAE
- SABIC, Riyadh and Al-Khobar, Saudi Arabia
- Netsol, Bangalore
- Kodiak Networks, Bangalore
- Reuters, India
- Larsen and Toubro
- Zamil – Tata Steel, Saudi Arabia
- Patni Computers, Mumbai, India
- Philips India
- TNT Worldwide, Dubai
- Dubai Electricity & Water Supply Authority
- Dubai Aluminium, Dubai
- Al-Marai, Riyadh, Saudi Arabia
- Schlumberger, Dubai and Abu Dhabi, UAE
- PWC Logistics, Kuwait
- Kuwait News Agency (KUNA), Kuwait
- Olympics Committee of Qatar, Doha
- Qatar Post, Doha
- Kanoo Group – Bahrain & Saudi Arabia
- Saudi Electricity Corporation, Riyadh
- Mphasis
- Metlife, India
- Unisys, India
- Accenture, India
- ITC Infotech
- TCS
- McAfee, India
- Fidelity, India
- LG Soft, India
- BT -India
- Risk Diversion LLC, Dubai
- Polaris
- Prosecutors Office, Qatar
- Ernst & Young, Muscat, Oman
- KPMG, Colombo
- Sri Lankan Airlines, Colombo
- KBSL, Division of John Keels, Colombo
- Ministry of Education, Government of Oman
- SBS, Division of Sundaram Finance Ltd
- GECIS, Division of General Electric
- Cable and Wireless, Bangalore
- Toyota, India
- General Motors, India

Our Consulting Services:

In addition the training services listed above, Valiant Technologies offers the following range of solutions for enterprises that desire to secure their information assets.

- **Information Security Consulting Practice**
  - Network Security Architecture Design and Review
  - Security Stance and Implementation Assessment
  - Enterprise Risk Assessment and Analysis
  - Application Security Assessment
  - Business Continuity Management and Disaster Recovery Planning

- **Information Security Management Practice**
  - Security Policies, Procedures and Guidelines
  - Security Awareness Program
  - Executive Management briefings on Security
  - Vendor selection for security products
  - ISO-27001 preparatory services
  - Fill-in Security Manager program

- **Information Security Assurance and Control Practice**
  - Vulnerability assessment
  - Penetration testing
  - Hardening of servers and network components
  - Periodic evaluation of network security
  - Gap analysis against ISO-27001, COBIT, ISSAF
  - Information security controls review
  - Information Systems Security Audit
  - Control assessment for SOX compliance

- **Cyber Crime Investigation Practice**
  - Computer Forensics Investigation

Five-Day workshop on Business Continuity Planning & Disaster Recovery Planning for CBCP aspirants

Background:

Disaster can strike any business, anywhere, at any time. Be it natural disasters, threat of terrorist attacks, loss of power, theft, hardware failure or security breaches, businesses that are reliant on their IT infrastructure need to ensure that they can recover their systems, quickly and with minimal disruption. Yet less than 30% of organizations have comprehensive disaster recovery plans. 40% of the companies that experience disaster go out of business, say experts. Those without appropriate business continuity plans lose significant market share and profits, not to mention the intangible yet devastating damage to the image of the organization. According to a study by AMR Research, the costs of downtime, planned or unplanned, per hour can be as high as $600,000.

"'For many real-time enterprises, a 4 to 24 hour site outage would cause irreparable damage to the enterprise,'" says Donna Scott, Vice-President and Research Director for Gartner and adds: "because the risks are greater with real-time enterprises, the business continuity plan must address new scenarios, and BC processes must integrate with a greater number of enterprise processes."

Surviving a disaster cannot be left to chance; business continuity planning must become embedded in strategic and operational plans for the business functions, human resources, facilities and technology.

The course of events that have influenced understanding of risks and vulnerabilities in the recent past has ensured that every standard that governs business continuity management has enhanced the scope of coverage to consider wider issues in greater depth. The importance of managing business continuity in corporations is more pronounced now than earlier because of a significant governance dimension to business continuity management that is well recognized now.

Notwithstanding all that has been said about the importance of business continuity and disaster recovery planning, most corporations still either look at BCP and DRP with a bit of skepticism or with a sense of bewilderment.

This workshop will focus on the key issues of BCP and DRP and following this workshop, participants will:

- Understand how to develop a Business Continuity plan
- Learn proven techniques to assess and reduce risk and impact
- Understand how to carry out a Business Impact Analysis
- Understand why many plans fail
- Gain the latest techniques adopted in creating Disaster Recovery Plans
- Discover how to organize for survival in a disaster
- Create scenarios simulating disasters and evolve appropriate response strategies

Who should attend?

- Continuity Management Professionals
- Information Systems and Security Professionals
- Information Systems Auditors
- Information Security Auditors
- System Administrators
- Security Administrators
- Internal Auditors
- Assurance Professionals
- Compliance Professionals

The presentations at the program will be mapped to the knowledge requirements for CBCP certification examination that is divided into the following domains:

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
6. Developing and Implementing Business Continuity Plans
7. Awareness and Training Programs
8. Exercising and Maintaining Business Continuity Plans
9. Crisis Communication
10. Coordination with External Agencies

Detailed program contents follow

DOMAIN – 1: PROJECT INITIATION AND MANAGEMENT

This session would assist the BCM professional in the process of clearly establishing the need for business continuity management in an organizational setting. This includes the key process of getting top management commitment to support the BCM process; set the objectives clearly, establish and implement policies for BCM practices and determine critical success factors. The professional is expected to spearhead the formation of a group to own and drive the process of BCM right throughout its life cycle.

- What constitutes business discontinuity?
- What is a Disaster?
- BCP and DRP – differentiated and defined
- Features of a Business Continuity and Disaster Recovery program
- Contingency planning concepts

DOMAIN – 2: RISK EVALUATION AND CONTROL

Presentations in this session would take the participants through the key process of risk evaluation and implementation of appropriate controls. The BCM professional is expected to identify threats, vulnerabilities, exploit path and exploit processes that will result in a risk scenario. Understanding the probability of occurrence and impact of occurrence of risky events is a crucial first step in identifying and implementing appropriate control mechanisms. In an organizational context, it is important to understand the function of risk reduction / mitigation and identify the need for getting external support and expertise. The entire process of risk reduction / mitigation will involve choosing from alternatives and such an exercise will depend on Executive Management's stance on acceptable risk levels.

- Understanding Risks, Threats, Vulnerabilities and Countermeasures
- Risk Assessment methodologies – choosing what is relevant
- Risk Assessment process
- Risk Management and risk appetite of organizations
- Residual risks and IT Governance issues
- Fine-tuning risk assessment process

DOMAIN – 3: BUSINESS IMPACT ANALYSIS (BIA)**

BIA is regarded by most BCM professionals as one of the most important constituents of the entire BCM cycle. It identifies the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify such impacts.

The primary contribution of BIA to the BCM process is the structured manner in which criticality of business functions are established, differentiating between continuity-critical vs. perceived-important. An objective assessment of criticality of business functions leads to determination of their recovery priorities, interdependencies to be considered while recovering critical business functions and establishing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). This session will assist participants in the program to carry out the eight-stage process through which a BCM professional goes to determine the criticality of business functions while performing BIA.

- Business Impact Analysis [BIA]
- Business Process identification for BIA
- Assessing and quantifying impact of disruptions to business processes
- Computing and justifying MTD /RTO and RPO figures
- Prioritizing based on RTO / RPO data and obtaining consensus on prioritized list
- BIA Reporting and getting Executive Management approval

DOMAIN – 4: DEVELOPING BUSINESS CONTINUITY STRATEGIES**

This session is devoted to the process of determining various business recovery strategies available and establishing a process for selection of appropriate recovery operating strategies for business and IT functions and processes within the RTO such that the organization's critical functions are not disrupted. This will involve the identification of off-site requirements and alternative facilities and development of recovery strategies for specific business units if adoption of an enterprise-wide strategy were not possible. The key process of getting executive management to support the set of strategies chosen for adoption will be discussed in this session.

- Structure and Content of the BC and DR Plan
- Writing the BC and DR Plan
- Determining the teams to be formed
- Composition of teams
- Tasks to be assigned to each team and the CSF for major task groups
- BC and DR Plan Draft – understanding and review
- Delineating Computer systems from other business process?
- Strategies to contain damage from attacks on computers
- Cost effective recovery strategies vis-à-vis information stored and in transit
- The human factor in responding to attacks on organization IPF
- Strategy implementation

DOMAIN – 5: EMERGENCY RESPONSE AND OPERATIONS

The need for a clearly established set of procedures as a response to situations following a disaster or a continuity threatening event will be discussed in this session. Presentations in this session would include the process for establishing and managing an Emergency Operations Center (EOC) to be used as a command center during the emergency. Participants will be taken through major types of emergencies and appropriate responses to each of them; integrate business continuity and disaster recovery procedures with emergency response procedures and the process of defining the roles, authorities, and communication processes during an emergency. It is also important to consider the need for integrating the emergency procedures with any requirements laid down by governmental or other public authorities.

- Creating a command center
- Understanding disaster or 'incident' control
- Objectives and roles of command center staff
- Roles, rights and obligations of command center personnel
- Emergency Procedures – creation, testing, validation and updating
- Damage Assessment and salvage process
- Moving to disaster recovery location – process, logistics, internal controls
- Communication – internal & external during a disaster

DOMAIN – 6: DEVELOPING AND IMPLEMENTING BUSINESS CONTINUITY**

The principal purpose of all BCM exercises is to design, develop, and implement Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) that provide continuity within the recovery time objective and meet the recovery point objective. Structured processes involving the choice of appropriate planning methodology, plan organization and staffing requirements need to be considered before developing BCP and DRP. The importance of testing the plan and the methodologies for testing the plans will be discussed in detail. The process to fine-tune the various elements of BCP and DRP based on test results is a sure recipe for its successful implementation. The ability to update and maintain the plan such that it reflects the current business processes and technology architecture is a key requirement of a successful BCM professional.

- Plan review process
- Implementation time frame and organizational requirement
- Interface with other activities while implementing the DR plan
- Control over access to BC and DR Plan content
- Control over distribution of the plan
- Version Control and library routines as applicable to BC and DR Plan
- Identifying special circumstances

- Cataloguing contingency situations and consequences
- Concept of 'minimum response'
- Evaluating alternative contingency plans

DOMAIN – 7: AWARENESS AND TRAINING PROGRAMS

Successful implementation of a Business Continuity Management process involves not just the BCM professionals or the members of the team that developed the plans and evolved recovery strategies; it requires the participation of the entire organization. Achieving this requires the creation and maintenance of an enterprise-wide awareness program and its supporting activities. This involves carrying out a training need analysis, developing awareness and training methodology, identifying relevant training tools and assessing the impact of the awareness program.

- Untested BCP / DRP is no Plan at all!
- Creating right degree of awareness of DR Plan content and action required as needed
- Testing methods and objectives
- Testing Process
- Follow up on test results
- Documenting and updating test objectives and results

DOMAIN – 8: EXERCISING AND MAINTAINING BUSINESS CONTINUITY PLANS (BCP)

Exercising the plan is a key process to be done to ensure it delivers the desired results. The need to evaluate the results of exercising the plan and documenting the results of this process is the responsibility of a BCM professional. The exercising of BCP cannot be carried out as an ad-hoc process and requires significant efforts at the pre-planning phase and coordinating the exercising process. This also involves the mapping of continuity and recovery plans to enterprise strategic directions. Efforts need to be made to compare the plan with appropriate standards and the results of this comparison will yield significant insight into the efficacy of the plans and will provide inputs to the process of updating the plans. The process and the results of exercising the plans will assist in establishing audit programs for the BCP.

- Plan review process
- Implementation time frame and organizational requirement
- Interface with other activities while implementing the DR plan
- Control over access to BC and DR Plan content
- Control over distribution of the plan
- Version Control and library routines as applicable to BC and DR Plan
- Identifying special circumstances
- Cataloguing contingency situations and consequences
- Concept of 'minimum response'

- The BC and DR Plan is a live document!
- Change control process – the 5 stage cycle
- Rapid response to changed threats, vulnerabilities and organizational structure

DOMAIN – 9: CRISIS COMMUNICATIONS**

The domain considers the relevance and significance of communication, in a crisis scenario, with internal stakeholders (employees, corporate management, etc.), external stakeholders customers, shareholders, vendors, suppliers, etc.), and the media (print, radio, television, Internet, etc). The need to establish proactive crisis communication rather than adopting a reactive communication process has been well established and the BCM professional must put in place significant planning efforts to achieve this. Establishing and exercising well orchestrated media handling plans for the organization and its business units will pay rich dividends while communicating under a crisis scenario.

- What do Internal stakeholders expect to know in a disaster?
- What is required to be informed to external stakeholders?
- Handling the media – What to Do and What Not to Do
- Planning for Crisis Communication

DOMAIN – 10: COORDINATION WITH EXTERNAL AGENCIES

This domain is focused on the process of establishing applicable policies and procedures for coordinating response, continuity, and recovery / restoration activities with external agencies - local, state, national, emergency responders, medical help, fire fighting, defense, etc. Those responsible for this function must also maintain current knowledge of laws and regulations concerning emergency management as it pertains to their organization

- Role of External Agencies in disaster management and recovery of critical business systems
- Identifying the role of each of the external agencies

** *At the end of presentations and discussions in these domains, participants will go through a case analysis; form themselves into small groups and carry out an activity that will give them hands-on experience on what was presented in the training session. Such an exercise will not only enhance the participants' preparedness for the examination but will also add to their skill sets, which they can use in their work place.*

Principal Instructor

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.