

Information Systems Onsite Training Booklet



Quality Management Systems.9000

Consultants and Trainers

Corporate Office: FF-9, Leeds Center, Main Boulevard
Gulberg III, Lahore - Pakistan
Phone: +92-42-35717909-10 | Fax: +92-42- 35783948
Email: lhr@gmsiso.com

UAE Office: Office No.302, Sobha Sapphire, Business Bay,
Sheikh Zayed Road, P.O. Box No. 50082, Dubai – UAE
Phone: +971-44-473229 | Fax: +971-44-473228
Email: marketing@gmsiso.com

Qatar Office: AMI Technology, 14 & 15 Level, Commercial
Bank Plaza, West Bay, Doha, Qatar
Tel: +974-4452 7902
Mob:00974-66418287 (Mr Qasim Khalid)
Email: marketing@gmsiso.com, qasim@ami-technology.com

www.gmsiso.com

TABLE OF CONTENTS

Course Code	Training Title	No. of Days	Page No.
-	Corporate Profile	-	2
IS	ISO 27001: Information Security Management System	-	3
IS-01	Introduction to ISO 27001	01	3
IS-02	Advanced Training on ISMS-ISO 27001 (ISMS Lead Implementer)	03	4
IS-03	Risk Management (based on ISO 27001)	01	5
BC	Business Continuity Management (BS 25999) <i>NEW</i>	-	6
BC-01	Introduction to BCMS	01	7
BC-02	Advanced Training on BCMS (Lead Implementer)	03	7
IT	ISO 20000: Information Technology Services Management System	-	9
IT-01	Introduction to ISO 20000	01	9
IT-02	Advanced Training on ISO 20000 (Lead Implementer)	03	10
IL	ITIL-Information Technology Infrastructure Library	-	12
IL-01	ITIL V.3 Foundation	03	12
SS	CISSP: Certified Information Systems Security Professional <i>NEW</i>	-	13
SS-01	CISSP CBK Review	05	13
EH	Certified Ethical Hacker	-	15
EH-01	Certified Ethical Hacker	04	15
HF	Computer Hacking Forensic Investigator	-	16
HF-01	Computer hacking forensic investigator	03	17
CS	CISM: Certified Information Security Manager	-	19
CS-01	CISM Boot Camp	01	19
PM	Project Management Training <i>NEW</i>	-	20
PM-02	Project Management Foundation	02	20
Terms & Conditions			22
Registration Form			23



CORPORATE PROFILE:

Quality Management Systems.9000 (**QMS.9000-Est since 1998**) is one of longest running Consultancy and Training organization in this region, with our expertise in various best practices and international standards. The testament of our experience and reliability in this field is evident of our **800 clients**, to whom we have provided these services in the last 15 years of our existence. In addition, we have also imparted exclusive onsite and seminar based trainings to various local and multinational organizations, with over **7000 professional** resources trained and prepared to increase their capability to strengthen their organizations. More details can be accessed via our website.

QMS.9000 offers exclusive **onsite (at your premises) training services** of your own choice and based on your requirement. For your convenience, we have divided these trainings into FOUR domains:

I. CERTIFICATIONS AND COMPLIANCES:

These trainings are more focused on improvement of industrial and service sector based organizations where organization needs to improve their internal operations, Human Resource Management, ensure legal and regulatory compliances as well as Foreign Buyer Compliances.

II. INFORMATION SYSTEMS

These trainings are more focused on Information System and related topics that support organizations in ensuring stability of their businesses against certain levels of issues, problems and risks as well as advanced trainings on various certification courses. These topics range from Information Security, Information Technology Services Management and Business Continuity Management to Risk Management, CISSP, CISA, CISM, etc.

III. LABORATORY ACCREDITATION

We also offer basic & advanced (Lead Implementer) trainings on Lab Management for Industrial testing / calibration Labs based on ISO 17025 and Medical Labs based on ISO 15189

IV. SIX SIGMA & FOCUSED IMPROVEMENT TOOLS

These trainings are more focused on Six Sigma Champion, Six Sigma Green Belt, Six Sigma Black Belt, Implementing Statistical Process Control and Understanding and Measuring Process Performance. Six Sigma is a business improvement approach that seeks to find and eliminate causes of mistakes or defects in business processes by focusing on outputs that are of critical importance to customers. As a result process performance is enhanced, customer satisfaction is improved and the bottom line is impacted through cost savings and increased revenue. Six Sigma is a strategic approach that works across all processes, products, services, company functions and industries.

We provide trainings at your premises



CERTIFICATION & COMPLIANCE		
ISO 9001 Quality Management System	CE MARK Product Certification	ISO 22000 Food Safety Management System
ISO 14001 Environmental Management System	PM Project Management	COPC Customer Operations Performance Center
OHSAS 18001 Occupational Health & Safety	C-TPAT Customs-Trade Partnership Against Terrorism	FBC Foreign Buyers Compliances
SA 8000 Social Accountability	OEKO-TEX Textile Production Certificate	OD Organization Development
INFORMATION SYSTEMS		
ISO 27001 Information Security Management System	ISO 20000 Information Technology Services Management System	BS 25999 Business Continuity Management System
Computer Hacking Forensic Investigator (CHFI)	Certified Information Security Manager (CISM)	Certified Information Systems Security Professional (CISSP)
LABORATORY ACCREDITATION		
ISO 17025 Lab. Management System	ISO 15189 Medical Lab. Management System	CWA 15793:2008 Clean Work Area
SIX SIGMA AND FOCUSED IMPROVEMENT TOOLS		
Six Sigma Champion Awareness & Introduction	Six Sigma Green Belt	Six Sigma Black Belt
Implementing Statistical Process Control	Understanding and Measuring Process Performance	

QMS.9000 has a dedicated team of professionals to provide consultancy and trainings for Certified Ethical Hacker, Computer Hacking Forensic Investigator, Information Security Management System (ISMS), specializing in the fields of System Security, Network Security, Infrastructure (Physical) Security, Environmental Security, and Business Continuity & Disaster Recovery Planning.

We have also conducted trainings/ ISMS reviews/Audits for Banks, Financial Institutions, Telecom companies, ISPs, IT companies, Defense organizations etc.

Foreign Collaborations: NETS International -UAE, CONSAK Inc -Canada; Mount10-Switzerland, Global Management Inc – UK, AMI Technology Qatar.

ISO 27001: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Course Code: IS-01

Course Title: Introduction to ISO 27001

Duration: 01 Day

Objective

This course is designed to provide knowledge and awareness about ISMS to organizations related to IT Solutions, Information and Network System Development and Security Implementation, Financial Institutes, Banking, Database Management, Telecommunication, Military / Defense

Primary Objectives:

- At the end of course, delegates will be able to:
- Understand and Interpret the requirements of ISO 27001 standard with clarity
- Conduct initial Gap Analysis at respective organizations

Course Contents

- Major requirements of ISO 27001:2005 Standard
- How information can be secured.
- Information Security Assets identification and evaluation
- Confidentiality, Integrity & Availability (CIA)
- Documentation Requirements: Policies, Procedure, Security Manual
- Defining the Scope & Policy of **ISMS**
- Risk Assessment/Risk Evaluation/Risk Management
- Business Continuity Planning
- Disaster Recovery
- Network Security
- System Security





Course Code: **IS-02**

Course Title: **Advanced Training on ISO 27001 (Lead Implementer)**

Duration: **03 Day**

Objective

- To provide clear understanding of ISO 27001:2005 standard requirements
- To provide clear understanding of Applicable Control Objectives & Controls
- To develop ISMS professionals for Certification as Lead Implementers and help their organization to maintain Information Security

Course Contents

Information Security Management System:

- Detailed interpretation of requirements of ISO 27001:2005
- Code of practice for information security based on best practices
- Control objectives and related controls for information security

Asset Identification and Valuation:

- What are your information assets
- How do you evaluate in terms of classification and significance
- How to secure your information assets

Physical Security:

- How to secure your work place , equipment and personnel

Human Resource Security:

- Prior to employment ; During employment ; Change of employment

Risk Management (Risk Assessment & Evaluation):

- Identification of Threats & Vulnerabilities
- Identification & Evaluation of Risks
- Determine significance of risks & their impact
- How to mitigate risks
- Treatment of risks and residual risk acceptability
- Statement of applicability

Business Continuity & Disaster Recovery:

- Scope of BCP and Team Selection
- Critical Operations Identification
- Disaster Recovery Planning
- Disaster Recovery Site
- Testing and Maintaining BCP & DR Site

Networks Security:

- To ensure the protection of information in networks and the protection of the supporting infrastructure



Course Code: **IS-03**

Course Title: **Risk Management on ISO 27001**

Duration: **01 Day**

Objective

Primary Objectives:

At the end of course, delegates will be able to:

- Understand and Interpret the requirements of Risk Management with clarity
- Conduct initial Risk Analysis at respective organizations

Course Contents

- Basic concepts behind Risk, Threat and Vulnerability
- Performing a Risk Assessment
- Methodologies to calculate Risk Factor
- Developing a Risk Treatment Plan
- Defining Risk rating criteria
- Modification of the Risk
- Corrective and Preventive measures
- Identification of information assets
- Determination of the value of information assets
- Identification of control objective
- Individual and Group Exercises
- Includes Practical Exercises of Asset Valuation, Risk Treatment Plan and Case Study Analysis

BUSINESS CONTINUITY MANAGEMENT SYSTEM (BS 25999)

Course Code: **BC-01**

Course Title: **Introduction To BCMS**

Duration: **01 Day**

Objective

Primary Objectives:

The course is aligned with the specification for Business Continuity Management Standard BS 25999. On completion of this course, delegates will have a comprehensive understanding of Business Continuity Management (BCM) and the processes involved in establishing a BCM program.

Course Contents

- **Introduction to Business Continuity Management (BCM)**
- **Business Continuity Best Practices and Standards**
- **BCM program**
- **Business Impact Analysis (BIA) & Risk Assessment**
- **Developing of a BCM strategy**
- **Develop plans for BCM response**
- **Exercising, maintenance and reviewing of BCM plans**
- **Disaster Recovery**





Course Code: **BC-02**

Course Title: **Advanced Training on BS 25999
Business Continuity Management System
(Lead Implementer)**

Duration: **03 Day**

Course Contents

Upon completion of this course, participants should be able to articulate the requirements outlined in BS 25999-2:2007, Business Continuity, understand the Management Specification, describe and implement the 6 steps of the BCM lifecycle, implement a business continuity management system and utilize the best practice techniques contained in BS 25999-1

Course Contents

Introduction to Business Continuity Management (BCM)

- The need for BCM and its suitability in your business
- Business Continuity lifecycle and Steps for Establishment
- Relation between Disaster Recovery and BCM

Business Continuity Best Practices and Standards

- About BCM standard & specification
- Overview of BS 25999 requirements
- Using the standard to your advantage

The BCM program

- PDCA Model in relation to BCMS Lifecycle
- Using Project Management Practices in BCMS Establishment

Business Impact Analysis (BIA) & Risk Assessment

- Identifying Services and Interdependent Processes
- Defining Criteria for selection of Critical Processes
- Performing BIA
- Estimating Maximum Tolerable Period of Disruption (MTPoD)
- Defining Recovery Time Objective (RTO)
- Defining Recovery Point Objective (RPO)
- Defining the Value of Criticality
- Defining Risk Assessment and Risk Acceptance Criteria
- Developing a Risk Treatment Plan
- Course Contents includes Performance Templates

Developing of a BCM strategy

- Establishing a BCM Objective
- Using MTPoD, RTO and RPO in defining your strategy
- Cost-Benefit Analysis and its implication on Risk Treatment, Business Continuity and Disaster Recovery



Develop plans for BCM response

- Developing BCP
- Invoking a BCP
- Developing Incident Response Structure
- Deploying Resources and Handling External Parties
- Managing Media Response
- BCM Awareness Programs
- Embedding BCM in Business Culture
- Appointment of BCM Team Lead and BCM Coordinators

Exercising, maintenance and reviewing of BCM plans

- Exercising BCM plans & Maintenance of plans
- Validation and Verification of BCM Arrangements
- BCM Internal Auditing
- Correcting and Improving BCM

Disaster Recovery

- Types of Disaster Recovery Sites
- Sites Comparison with Pros and Cons
- Role of DR Site with BCP
- Identifying requirements for invocation of DR Site
- Implication of RPO at Disaster Recovery Site
- Subcontracting DR



ISO 20000: INFORMATION TECHNOLOGY SERVICES MANAGEMENT SYSTEM

Course Code: **IT-01**

Course Title: **Introduction to ISO 20000**

Duration: **01 Day**

Objective

The objective of this course is to enable the participant in implementing best management practices at their organization in providing services related to Information Technology to its customers and clients. This course provides guidance on developing Information Technology Services Management objectives and plans for implementation of these services while ensuring applications of such measures as Capacity Measurement, their budgeting and accounting, ensuring availability and continuation of services and resolution of problems (internal and external). The training ensures that all steps from execution till closure of services are covered comprehensively.

Course Contents

- Development of IT Services Objectives and their achievement plan
- Development of procedures for IT Services management
- Development of System for reporting services
- Ensuring availability and continuity of services
- Capacity Management (Ensuring availability of required and relevant resources)
- Development of System to manage accounting budgeting of services (and related resources)
- Development of a system to evaluate suppliers on the basis of quality of their products and services
- Customer Handling (Customer Compliant handling and satisfaction level)
- Development of System for incident management
- Development of System for Corrective and Preventive actions
- Change and Configuration Management System



Course Code: **IT-02**

Course Title: **Advanced Training on ISO 20000 - ITSMS
(Lead Implementer)**

Duration: **03 Day**

Objective

This three day workshop is designed to explore the benefits of achieving ISO 20000 certification, how to plan for ISO 20000 certification and helps in defining pointers for making the business case for internal approval. The workshop examines approaches to implementation and potential issues that need to be managed to achieve ISO 20000 compliance. The course objectives include:

- To provide an understanding of the ISO 20000 Standard and associated ITSMS Certification process.
- To provide guidance on assessing and organizations readiness for ISO 20000
- To provide guidance on preparing organizations for ISO 20000 Certification

Course Contents

The course will include:

Overview of the ISO 20000 Service Management standard

- Introduction & background
- The certification scheme
- Use & application of the standard (Part 1 & 2)
- Assessments & Audits
- Role of Toolsets
- Eligibility & Scope

Coordination & integration Processes

- Requirements for a Management System
- Planning & Implementing Service Management
- Planning & Implementing new & changes services

Service Delivery Process

- Service Level Management
- Capacity Management
- Service Continuity & Availability Management
- Budgeting & Accounting for IT Services
- Service Reporting
- Information Security Management

Resolution, Control & Release Processes

Quality Management Systems.9000

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release management

Relationship Processes

- Business Relationship Management
- Supplier Management



ITIL: INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

Course Code:	IL-01
Course Title:	ITIL- V.3 Foundation
Duration:	03 Days

Objective

This hands on, instructor led, ITSM Version 3 Foundation certification training program introduces the student to the fundamentals of IT Service Management as described in version 3 of the IT Infrastructure Library (ITIL®). The course helps students prepare for the certification exam along with acquiring valuable insights from instructors who have actually managed IT operations and ITSM programs.

Course Contents

The course is structured around an interactive case study, and takes a process based approach to managing IT services throughout the Service Lifecycle. It does not focus on any specific technology, but rather on delivering services aligned with business needs. Delivered over three days, the course features lectures, discussion, team exercises and quizzes.

- Redefining business framework in accordance with the best practices.
- Defining Service Strategy of the organization.
- Working out the Service Design of the organization.
- Development of procedures for effective Service Transitions.
- Development of procedures for monitoring and improvement of Service Operations.
- Helping organizations in achieving Continual Service Improvement.
- Introduction of Service Desk Support.
- Development of Incident and Problem Management procedures.
- Development of Change and Release Management programs.
- Development of Capacity and Availability Management procedures.
- Management of Service Level Agreements.
- IT Service Continuity Management.
- IT Security Management.



CISSP: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

Course Code: **SS-01**

Course Title: **CISSP CBK Review**

Duration: **05 Day**

Objective

Our CISSP boot camp course contains "checkpoints" that help you self-evaluate your progress. You will know which key concepts you have a solid understanding of, and which of the CISSP domains you need to spend more time reviewing. The benefit of these checkpoints is that you will have an expert instructor on hand to help you through any trouble spots.

This CISSP Boot Camp prepares you with the material you need in order to **PASS the CISSP EXAM, nothing else**. We concentrate on **helping you pass** the exam by **identifying deficiencies in your knowledge** of the 10 domains.

Course Contents

1. Information Security and Risk Management

Identifying an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines to identify risk.

2. Access Control

Access controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

3. Cryptography

Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

4. Physical (Environmental) Security

The physical security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

5. Security Architecture and Design

Contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality.

6. Application Security

Addresses the important security concepts that apply to application software development and outlines the environment where software is designed and developed.

7. Telecommunications and Network Security

8. Legal, Regulations, Compliance, and Investigations domain

It addresses:

9. Business Continuity & Disaster Recovery Planning

The BCP & DRP domain addresses business operations in the event of outages.

10. Operations Security

Identify the controls over hardware, media, and administration to any of these resources. And audit & monitoring that identify security events and subsequent actions.





CEH: CERTIFIED ETHICAL HACKER

Course Code: **EH-01**

Course Title: **CERTIFIED ETHICAL HACKER**

Duration: **01 Day**

Objective

The goal of this course is to help you master a repeatable, documentable penetration testing methodology that can be used in an ethical penetration testing or hacking situation. This ethical security training course has a significant Return on Investment; you walk out the door with hacking skills that are highly in demand, as well as the Certified Ethical Hacker certification!

Course Contents

The course covers the following 22 Modules in detail and highlights the issues that are of importance from exams perspective.

- Module 01: Ethics and Legal Issues
- Module 02: Footprinting
- Module 03: Scanning
- Module 04: Enumeration
- Module 05: System Hacking
- Module 06: Trojans and Backdoors
- Module 07: Sniffers
- Module 08: Denial of Service
- Module 09: Social Engineering
- Module 10: Session Hijacking
- Module 11: Hacking Web Servers
- Module 12: Web Application Vulnerabilities
- Module 13: Web Based Password Cracking Techniques
- Module 14: SQL Injection
- Module 15: Hacking Wireless Networks
- Module 16: Virus and Worms
- Module 17: Hacking Novell
- Module 18: Hacking Linux
- Module 19: IDS, Firewalls and Honeypots
- Module 20: Buffer Overflows
- Module 21: Cryptography
- Module 22: Penetration Testing Methodologies



CHFI: COMPUTER HACKING FORENSIC INVESTIGATOR

Course Code: **HF-01**

Course Title: **Computer hacking forensic investigator**

Duration: **03 Days**

Objective

Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. **CHFI** investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information.

Course Contents

- Module 01: Computer Forensics in Today's World
- Module 02: Law and Computer Forensics
- Module 03: Computer Investigation Process
- Module 04: First Responder Procedure
- Module 05: CSIRT
- Module 06: Computer Forensic Lab
- Module 07: Understanding File Systems and Hard Disks
- Module 08: Understanding Digital Media Devices
- Module 09: Windows, Linux and Macintosh Boot Processes
- Module 10: Windows Forensics
- Module 11: Linux Forensics
- Module 12: Data Acquisition and Duplication
- Module 13: Computer Forensic Tools
 - Part I: Software Forensics Tools
 - Part II: Hardware Forensics Tools
- Module 14: Forensics Investigations Using Encase
- Module 15: Recovering Deleted Files and Deleted partitions
 - Part I: Recovering Deleted Files
 - Part II: Recovering Deleted Partitions
- Module 16: Image Files Forensics
- Module 17: Steganography

- Module 18: Application Password Crackers
- Module 19: Network Forensics and Investigating Logs
- Module 20: Investigating Network Traffic
- Module 21: Investigating Wireless Attacks
- Module 22: Investigating Web Attacks
- Module 23: Router Forensics
- Module 24: Investigating DoS Attacks
- Module 25: Investigating Internet Crimes
- Module 26: Tracking E-mails and Investigating E-mail Crimes
- Module 27: Investigating Corporate Espionage
- Module 28: Investigating Trademark and Copyright Infringement
- Module 29: Investigating sexually harassment incidents
- Module 30: Investigating Child Pornography
- Module 31: PDA Forensics
- Module 32: iPod Forensics
- Module 33: Blackberry Forensics
- Module 34: Investigative Reports
- Module 35: Becoming an Expert Witness





CISM: CERTIFIED INFORMATION SECURITY MANGER

Course Code: CS-01

Course Title: CISM Boot Camp

Duration: 5 Days

Objective

The course covers all domains associated with CISM and provides the participants with insight details and knowledge on attempting CISM's exam. The training also provides comprehensive details about the role of an Information Security Manager in an organization.

Course Contents

Information Security Governance:

This objective covers developing an information security strategy aligned with business goals and objectives. It describes Budgetary planning strategies and roles, responsibilities and general organizational structures for Information security management, etc.

Information Risk Management:

This objective includes establishing a process for information asset classification and ownership. It identifies the factors used to determine risk reporting frequency and requirements.

Information Security Program Development:

This objective covers methods to interpret strategies into manageable and maintainable plans for implementing information security and methods to align information security program requirements with those of other assurance functions and implementation of information security architectures and their deployment.

Information Security Program Management:

This objective includes the implementing and interpreting of the information security policies and information security administrative processes and procedures. It describes the methods for managing the enterprise's information security



PROJECT MANAGEMENT TRAINING

Course Code: **PM-02**

Course Title: **Project Management**

Duration: **2 Days**

Objective

The training provides detailed understanding of Project Management practices through use of Workshops / Exercises while giving participants as close to reality scenarios as possible within a limited timeframe. The training ensures that participants are able to utilize this practice in their work environment to accomplish their time bound assignments with better planning and time management.

Contents

Project Initiation and Prerequisites

- Project Initiation Stage
- Project Lifecycle Model
- Project Management Roles
- Documenting Project Objective
- Final Result Description
- Determining Project Milestones
- Determining Preliminary Resources

Project Scoping

- Scope of Project
- Limitations and Assumptions
- Define Project Strategy
- Defining Project Resources
- Budgetary Assumptions

Project Planning & Costing

- Documenting Project Plan
- Describing Project Phases and Deliverables / Milestones
- Cost Analysis and Budgeting
- Finalization of Resources
- Defining Roles and Responsibilities
- Task Management



Project's Risk Management

- Understanding Risk Management
- Problem Identification & Management
- Risk Treatment
- Issue Identification and Rectification
- Effects of Problems and Issues on Timeline

Executing the Plan

- Project Team Management
- Team Motivation
- Team Communication
- Implementing the Project Plan
- Quality Controls
- Performance Tracking
- Budget Control
- Change Management

Project Closure

- Acceptance of Final Deliverable
- Closing Contractual Obligations
- Project Report Documentation



TERMS & CONDITIONS

Following are the terms and condition for offsite and onsite premises;

<p align="center">Offsite Premises QMS.9000 Responsibility</p>	<p align="center">Onsite Premises Client Responsibility</p>
<ul style="list-style-type: none"> ■ Multimedia, ■ White Board, ■ Training hall, ■ Lunch / refreshments etc. 	<ul style="list-style-type: none"> ■ Multimedia, ■ White Board, ■ Training hall, ■ Lunch / refreshments etc.

Important Note:

- Maximum of 18 participants will be accommodated in each training
- Training will be arranged for Minimum 10 participants in each training
- For two or more modules by an Organization there will be 10 % discount.
- Training charges are to be paid in advance
- One week notice is required to ensure availability of trainer
- Course Timings: 0900-1700 hrs
- Certificates will be provided to all participants



REGISTRATION FORM

FOR ORGANIZATION

Course ID:

--	--	--

Please write course code from the Brochure i.e. the courses that you wish to have at your organization

Name Of Organization	
Location Address (where you want to hold trainings)	
Contact Person (with designation)	
Phone	
Mobile	
Email	
Number Of People (mention how many people from your organization will attend)	
Tentative Dates On Which You Want To Hold These Trainings	
Postal Address For Correspondence (if it is different from location for training)	

Note: Organizations can make copies of the Registration Form

Send Your FILLED Registration Form via Email, Fax and Postal Address to our Office.