Cyber Law Pioneers

WHEN TRUTH & JUSTICE CALLS

About the Company

Cyber Law Pioneers Pvt. Ltd. is a leading company in the field of Cyber Security & Compliance Services, cyber education, Cyber Law, IPR & Cyber security solutions, training, awareness and Techno-legal consultancy. Established under the Company Act, 2013, we are a registered company working for last 10 years dedicated to providing efficient and effective services to combat the rising threat of cybercrime.

Course Overview

A cyber security management solutions course is designed to provide individuals/professional with the knowledge and skills necessary to effectively manage cyber security within organizations while ensuring protect organizational assets from cyber threats, compliance with relevant laws, regulations, Risk management and industry standards

Course Objective

To gain expertise in risk management, security governance, regulatory compliance, and incident response and have comprehensive understanding of cyber security principles, compliance frameworks, and best practices while preparing them for future careers in the field.

Why CSMS course with our Company?

Cyber Law Pioneers is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals & working professionals. We offer role-specific certification training programs and prepare professionals for the future. Our Cyber Systems Implementer Online Hands-on Training course will equip you with comprehensive skills in implementing the Cyber Security Management framework according to ISO 27001 standards.

CERTIFICATE PROGRAM ON

CYBER SECURITY MANAGEMENT SOLUTION (CSMS-ISA-2024 V1)

Implementation, Compliance & Audit CLPCSMSF-01

Career Opportunities

- **Compliance Analyst/Officer**
- **Associate Cyber Security Consultant**
- **Cyber Security Advisor**
- **Assistant Security Consultant**
- **Security Consultant**
- **Assistant Cyber Security Analyst**
- **Auditor**
- **Cyber security Manager**
- **Risk Manager**
- **Policy Developer**

Eligibility

For 12th and passed out	Have to purse Foundation course first & then Advance
Undergraduate & Post Graduate	**For Technical degrees**- B. Tech / BCA / B.Sc. (IT)/ M-Tech/MCA and equivalent- **Can directly join Advance Course.** **Any Non-Technical degrees have to complete Foundation Course first then will be able to join Advance Course** **OR who had completed Foundation course can directly enter for the advance.**

Outcomes

-Understand client control environment
-Determine controls objective by studying business function gathering information evaluating output requirements and format
-Develop InfoSec policies standard and processes ensure policies are reviewed and updated regularly
-Design and new governance risk and control by analyzing requirement constructing overflow chart and diagram.
-Monitor and analyses the email for thread including phishing and malware and make recommendation for emails rules to minimize malicious or undesirable emails,
-Perform security testing manual and automated perform network VAPT
-Make recommendation against security infrastructure threat and tune all security monitoring tools in the organization.

6 MONTHS FOUNDATION
+
6 MONTHS ADVANCED COURSE
CAN CHOOSE ANY COURSE

CERTIFICATION

Cyber Law Pioneers will add value to your professional Resume by providing

CERTIFICATES OF EACH SPECIFIED COURSES ONCE COMPLETED

+

DIPLOMA OF 6 MONTHS COURSE

Cyber Law Pioneers Pvt. Ltd.
Plot no. C 203 3rd Floor M.P. Nagar Zone 2 Bhopal

Contact: 7354133333, 8770303862

Email: cyberlawpioneers@gmail.com

Course Details

The training program will be of 06 Months consist of 03 COURSEs. Each COURSEs will be of 02 months+10 days project work followed by exams and certification. Students will get study material provided by the company.

Examination & Assessment- Participant need to qualify exam conducted after the completion of each COURSE. Also needs to submit assignment and project work. An online examination will be conducted & will be Multiple Choice Questions attempted in an Hour

Participant have to:
- ✓ Attend 05 Classes in a Week
- ✓ Daily 02 Hours Session
- ✓ Can be Online/Offline
- ✓ Theory and Practical Classes

Fees Structure

Rs. 45,000/- for single course.

CYBER SECURITY ESSENTIAL-FOUNDATION Course

COURSE I

Unit I: Overview of Cyber security Management Solution

·Introduction of CSMS

·Scope of CSMS

·Functional Layers of CSMS-ISA

·Implementation of CSMS Framework

·Consultancy Services Offered under CSMS-ISA

·Function and Services

Unit-II Evolution and growth of ICT

·Definition of Computer, legal aspects of computer, Computer system

·Characteristics and applications, History of Computer, Generation of Computer, Number System, Data & Information,

·Basic components of a computer system Control unit, ALU, Input/output Devices and characteristics, memory: Primary Vs Secondary memory units, RAM, ROM. Hardware Components.

·Overview of Internet: Architecture, Applications, Protocols, Internet Vs. Intranet, ISP, Connectivity Dial-up, Leased line, VSAT etc., URLs, Domain names, Portals, WWW, Web Browser.

·Computer Network: Networking, LAN, MAN, WAN, Internet

Unit-III Operating System

- Characteristics and applications, functions,
- File Management- File, attributes of file, operations of file, file extension, File system. Access methods.
- Software: Types of Software

Unit-IV E-Commerce

1 Internet and E-Commerce

·E-commerce Frameworks

·E-Commerce operation

·Applications of E-Commerce

2. Business Models

3. E-Banking and operations

3.1 Application of E-banking

4. E-governance

Unit-V Cyber Space and Security

1. Cyber Space, Operation of Cyber Space.

2. Understand the Cyber Security aspects.

3. Principal of Cyber Security

4. Importance and need of Cyber Security.

5. Forms of Cyber-attacks- DOS, DDOS, Sniffing& phishing

Unit-VI Cyber Crime and the Law

1. Cyber crimes

2. Category of Cyber crime

3. Different forms of cybercrime that can affect teenager

4. Activities comes under cybercrime.

5, Introduction of Cyber Law

6. Indian Cyber Law- Introduction of Information Technology Act, 2000

7. Digital Signature

PRACTICAL

Unit-1- Editing and Processing work

- MS Word
- MS Excel
- MS PowerPoint
- E-mail
- Secure usage of Internet
- Digital Transaction

Unit-2.-General Computer Security Concepts

1. Practice of Desktop security, E-mail Security

2. Social networking site security

3. User Security,

4. File Security

5. Password Security

6. Firewall, Configuring Windows Firewall

7. Installation and configuration of Antivirus

8. Wi-Fi Security

9. Safe Browsing etc.

COURSE-II

1. **Unit-1 Computer Networking**

1. Introduction of network and networking devices

1.1 What is networking

1.2 Networking devices: router, modem, hub, switch, repeater/booster, cables and connector.

2. Introduction of IP address and class

2.1 What is IP address

2.2 Class of IP address

2.3 IPV4/IPV6 Introduction

2.4 Public & Private IP address

2.5 Introduction IPV6

PRACTICAL

Unit I- Implementation of Computer Network

- Network cabling
- Established an Office Local area network
- Established a Home Wi-Fi Network
- Configuration of Printer
- Configuration of Router

Unit-II-Advance Cyber Security Measures

- Mobile security
- Windows security
- Do's and Don'ts about E-Transaction
- Do's and Don'ts about online shopping

Unit-III-Secure Use of Internet and Online Application

- Threats on Internet
- Search Engines & Web Browsers security
- Filtering Services in Web Browser
- Email usage best practices
- How to view E-mail Header and understand the details and parameters
- Safe Downloading
- Social Engineering
- Phishing, VoIP phishing

COURSE III

UNIT I- ETHICAL HACKING

-Introduction of Ethical Hacking

-Types of Hackers, Foot printing

-Faces of Hacking, Information Gathering

- Scanning, Password Breaking

-Virus, Worm, Botnet, Trojan

-Website Hacking

-Web-Server Hacking

-Wi-Fi Hacking
-Vulnerability Assessment
-Ids/IPS Honeypot
-Cryptography & Steganography
-Android Hacking
-Operating System Hacking
-Risk Management
-Information Security Policies
-Access Control
-Information Security Threats and Attack Vectors
-Data Backup & Data Recovery.
- Deceiving IDS firewall & security

CYBER SECURITY MANAGEMENT SYSTEM
ADVANCE Course
COURSE I

Unit I: Cyber Security Management System

- Introduction of cyber-security
- Phases of ethical-hacking
- Understand the Cyber Security Management
- Reasonable Security Practice And Procedure Defined Under The Information Technology Act, 2000.
- Introduction of Information Security Management System Standard ISO 27001 Implementation and Audit Process.
- Access Controls and Security Measures for Secure Management of Computer Resources at Workplace.
- Key Elements of Cyber Security Policy.

Practical
- Development Of Cyber Security Policy
- Internal Audit Of CSMS
- CSMS Security Audit Report Preparation

Unit II- ROUTING PROTOCOLS & CONFIGURATION
INTRODUCTION TO ROUTING PROTOCOL
STATIC ROUTING
DEFAULT ROUTING
DYNAMIC ROUTING
RIP PROTOCOL
IGR PROTOCOL
OSPF PROTOCOL

UNIT III- Operating System
-Features of Linux/Unix Operating System,
-Kernel, Kernel Functions
-The Shell Basic Commands,
-Shell Programming, Shell Variables,
-Branching Control Structures,
-Loop-Control Structure,
-Continue and Break Statements,

-File Server, Directory Server,
-Application Server, DNS Server,
-SMTP Server, Firewall, Proxy Server

UNIT IV -File System
Definition of File System, Defining Geometry,
Disk Controller,
Solaris File System,
Disk Based File Systems,
Network-Based File Systems,
Virtual File Systems,
UFS File System.
The Boot Block,
The Super Block,
The INODE, Tuning File System,
Repairing File System.

UNIT V- Process Control
Viewing a Process,
Command to Display Process,
Process Attributes,

UNIT VI- NETWORK SECURITY
VLAN
PORT SECURITY
NAT
ACL
FRAME RELY
WIFI

COURSE-2

UNIT I- WINDOWS OS & SERVER
- Introduction Of Windows Operating System
- Windows Client And Server
- Windows Control Panel
- Deploying Windows Server
- Windows Server Update Services
- Advanced File Services Configuration
- Server Monitoring And Auditing
- Remote Access Configuration
- Network Policy Configuration
- Domain Controller And Active Directory Management
- User And Service Account Configuration
- Group Policy Settings And Preferences
- Managing Group Policies
- Managing And Configuration DNS
- Windows Security

UNIT II- HTML & Python:-
Basic intro of HTML and Python
Types of tags, Header, operator, etc.
Anyone project in the final test.

UNIT III- DATA LOSS PREVENTION (DLP)
1. Overview Of DLP
- Introduction and objective of DLP
- Common themes in DLP
- People, Process, Technology
- Need in DLP and its risk
- Areas of Data Loss
- Data Leakage v. DLP

2. Data Loss And Recovery
- Data loss and its types
- Scenarios and numbers involved in Data Loss
- How to respond to Data Loss
- Backup Strategy for Data Recovery

3. Computer Security
- Introduction and its importance
- How to secure OS
- Computer Security Threats
- Improving Computer Security

4. Cyber Security Standards (CSS)
Introduction of CSS
History of CSS

5. DLP Solution
- Introduction and Objectives
- DLP features v. Solution
- Things to consider in DLP Solution

COURSE-3

UNIT I- LINUX
- Overview Of Unix/Linux: -
- Concepts, Unix/Linux Installation Process,
- Hardware Requirements For Unix/Linux,
- Advantages Of Unix/Linux,
- Reasons For Popularity And Success Of Linux/Unix
- Process States, Process Fields,
- PS Commands Options, PGREP,
- PRSTAT,
- CDE Process Manager,
- Scheduling Process,
- Scheduling Priorities,
- Changing The Priority Of A Time-Sharing Process
- Killing Process.

-Sleep Command, Debugging Script
-Use of Linux as Web-Server,

UNIT II- System Security:-
- Physical Security,
- Controlling System Access,
- Restricted Shells Controlling File Access,
- File Access Commands, Access Control List(ACL),
- Setting ACL Entries,
- Modifying ACL Entries on A File,
- Deleting ACL Entries On A File, Restricting FTP,
- Securing Super Use Access,
- Restricting Root Access, Monitoring Super User Access,
- TCP wrappers.
- DHCP leased Time,
- DHCP scopes,

UNIT III- Cyber Forensics
- Cyber-forensics & Cyber-crime
- Malware-Analysis.
- Investigating web Attacks
- Auditing & Reporting

COURSE-4

UNIT I- Cyber Law and Cyber Crime
- Cyber Jurisprudence and,
- Introduction to Cyber Law

1: Introduction to Cyberspace, Architecture and Digital Divide
- Introduction of Cyber Space
- Characteristics of Cyber Space
- Emerging Issues from Cyber Space

2: Introduction to Cyber Law and Regulation of E- Governance
- Introduction of Cyber Law
- Need of Cyber Law
- Primary Law in India
- Overview of the Information Technology Act, 2000 Legal Framework for E-Governance in India

3: Jurisdiction Issues In Cyber Space: Dispute Resolution,
- Indian and International Approach
- Concept of Jurisdiction
- Jurisdiction Issues in Cyber Space
- Indian and International Approach In Cyber Jurisdiction

4: Computer Wrongs & Cyber Crimes
- Definition of Cyber Crime
- Conventional Crimes through Computer
- Category of Cyber Crime
- Different Forms of Cyber Crimes and Modus Operandi Offence Defined Under the Information Technology Act, 2000
- Case Study on Cyber Crimes under the Information Technology Act.

5: Electronic Evidence and Relating Law
- Electronic Evidence and Classification
- Digital Devices: Sources for Digital Evidences
- Searching and Seizing Of Digital Evidence and Devices
- Law Relating To Electronic Evidence and Admissibility of Electronic Evidence

UNIT II- Regulation of E-Commerce and E-Banking Transactions
1: Regulation of E-Commerce
- Internet and Role of ISPS, Concept of E-Commerce,
- E-Business Models,
- UNCITRAL Model Law
- E-Commerce Frameworks and Standards
- Electronic Data Interchange

2: Contract Formation and Licensing:
- Introduction of e-Contract
- Online Contract Formation
- Software License Agreements
- Contract Formation and Mail Box Rule
- Mail Box Rule
- Legal Recognition of E-Contract
- Electronic Contract and Information Technology Act

3: Privacy Protection in Online Commercial Environment and Legal Framework
- Jurisdiction Issues
- Privacy, Internet, E-Commerce and Data Protection Issues
- Threats to Personal Identity on Internet
- Online Technology Surveillance
- Provisions under the It Act, 2000 for Privacy and Data Protection

4: Emerging E-Banking System and Electronic Fund Transfer
- The Internet and E-Banking: Framework for Internet Banking In India:
- RBI Guidelines Electronic Money and Internet Payment System
- Core Banking Solutions
- Mobile Banking

COURSE-5

Unit 1: Website & Network Security Implementation and Audit
- Fundamentals And Need Of Vulnerability Assessment And Penetration Testing
- Difference Between Vulnerability Assessment And Penetration Testing
- VAPT and its Life Cycle
- Features And Characteristics Of Penetration Testing Tools
- Security Patches & Updates

Unit 2: Vulnerability Assessment
- Testing (White Box, Black Box, Gray Box) Assess The Vulnerabilities
- Virus And Trojan Detection
- Identify Vulnerabilities, Threats Etc.
- OWASP Top 10 Vulnerability
- Vulnerability Assessment Tools
- Vulnerability Classification And Severity Table Sample Report Of Vulnerabilities With Categorization Of Vulnerabilities (High, Medium, Low)

Unit 3: Penetration Testing
- Information Gathering
- Exploitation
- Website Penetrate
- Network Penetrate
- Password Cracking Penetration Testing
- Fundamentals Internal And External Penetration Testing
- Penetration Testing Tools

Practical
1. Installation And Usage Of Open Source VAPT Tools Hands On Practice On Different Tools Like Acunetix Web Vulnerability Scanner, Burp Suite Websploit Toolkit, and Penetration Testing Oriented Browser-Sandcat Browser. PHP Vulnerability Hunter, Openvas, Wireshark, Zenmap

2. Website Security Implementation, Website Security Audit And Report Preparation