UNIVERSITY OF MADRAS
INSTITUTE OF DISTANCE EDUCATION
MSC Cyber Forensics & Information Security
Under Choice Based Credits System
(With effect from the academic year 2018-2019)

SCHEME OF EXAMINATION

SEMESTER - I COURSE COMPONENT	SUBJECTS	CREDIT	MAX MARKS		TOTAL
			INT	EXT	
Core Paper-I	Introduction to Cyber Criminology	4	20	80	100
Core Paper-II	Networking and Communication Protocols	4	20	80	100
Core Paper-III	Introduction to Information Security	4	20	80	100
Core Paper-IV	IT Infrastructure and Cloud Computing	4	20	80	100
Elective Paper-I	Forms of Cyber Crimes	3	20	80	100

SEMESTER -II COURSE COMPONENT	SUBJECTS	CREDIT	MAX MARKS		TOTAL
			INT	EXT	
Core Paper-V	Network Security and Cryptography	4	20	80	100
Core Paper-VI	Basics of Cyber Forensics	4	20	80	100
Core Paper-VII	IT and Telecom Frauds & Countermeasures	4	20	80	100
Core Paper-VIII	Practical- I – (Networking and Information Security)	4	40	60	100
Elective Paper-II	BFSI Frauds & Countermeasures	3	20	80	100

SEMESTER -III COURSE COMPONENT	SUBJECTS	CREDIT	MAX MARKS		TOTAL
			INT	EXT	
Core Paper- IX	Database Management Security	4	20	80	100
Core Paper- X	Advanced Cyber Forensics	4	20	80	100
Core Paper- XI	Advanced Information Security	4	20	80	100
Core Paper- XII	Practical – II (Cyber Forensics)	4	40	60	100
Elective Paper- III	Data Privacy	3	20	80	100

SEMESTER IV COURSE COMPONENT	SUBJECTS	CREDIT	MAX MARKS		TOTAL
			INT	EXT	
Core Paper- XIII	Application Security	4	20	80	100
Core Paper- XIV	Governance, Risk &Compliance	4	20	80	100
Core Paper- XV	Business Continuity & Disaster Recovery Management	4	20	80	100
Core Paper- XVI	Security Testing	4	20	80	100
Elective Paper-IV	Cyber Laws & Intellectual Property Rights	3	20	80	100

CREDIT DISTRIBUTION

		CREDITS
Core Paper	16 X 4	56
Core Practical	2x4	08
Elective	4 X 3	12
TOTAL		**76**

MSC Cyber Forensics & Information Security
Under Choice Based Credits System
(With effect from the academic year 2018-2019)
REVISED SYLLABUS

SEMESTER I

Core Paper I -Introduction to Cyber Criminology

Unit 1 : Principles and Concepts of Cyber Criminology – Crime, Tort, Misdemeanour, Cyber Space, Cyber Crime, Cyber Criminology, Information Security, Penetration Testing, Incident Response, GRC, etc.- Conventional crimes vs. Cyber Crimes.

Unit 2: Contemporary Forms of Crimes - White Collar Crimes, Economic Offences, Organized Crimes, Terrorism, Crime and Media and other contemporary forms of crimes.

Unit 3: Psychology of Cyber Criminals – Types of Cyber Criminals – Modus Operandi of Cyber Criminals – Profiling of Cyber Criminals - Tools and Techniques adopted by Cyber Criminals – Psychological theories relating to cyber criminals.

Unit 4 : Cyber Crime– Sociological and Criminological Perspectives – Causes of Cyber Crimes - Criminological Theories and Cyber Crime – Routine Activity Theory, Social Learning Theory, Differential Association Theory, Differential Opportunity Theory, Media and Crime and latest theories and other related theories.

Unit 5: The Role of Criminal Justice Administration and Cyber Crimes :

a. Police – Organizational structure of Police in India – Different wings in the States and Districts and their functions - Police & Law Enforcement – F.I.R. – cognizable and non-cognizable offences, bailable and non-bailable offences – arrest , search, seizure – Interrogation of suspects and witnesses – charge sheet – Cybercrime cells – structure & investigation of cybercrime cases .
b. Judiciary - Different types of courts – Cyber Appellate Court / Tribunals / Powers – Proceedings in the court before trial, after trial, plea of guilty, sentencing.
c. The Role of N.G.O.s in the Prevention of Cyber Crimes
d. The Role of Victims of Cyber Crimes in the Criminal Justice Administration

Crime Prevention - Crime and sense of security - Social control and crime prevention - Community and crime prevention - Contemporary crime prevention strategies.

Core Paper II -Networking and Communication Protocols

Unit 1 Networking models- OSI Layered model - TCP/IP Model - MAC Address representation - Organisationally Unique Identifier - Internet Protocol - Versions and Header lengths - IP Identification - IP Flags - IP fragmentation and reassembly structure - Transport Layer protocols - Port numbers - TCP Flags - Segmentation - TCP 3 way handshake and Options - encapsulation and De-encapsulation - Payload.

Unit 2 Static and Dynamic Routing - IP Routing Protocols - Classful and Classless Routing - RIPv1 - RIPv2, Broadcast and Multicast domains - OSPF, EIGRP - Network Address Translation - IP Classes - Private IP - Public IP - Reserved IP - APIPA.

Unit 3 Subnetting IP network - Class A, B, C subnetting - Classless Inter-domain Routing (CIDR) - Subnet mask - Wild card mask - WAN Technologies - Frame Relay - Data link Connection Identifiers (DLCI) - Committed Information Rate (CIR) - Permanent Virtual Circuits (PVCs) - Multiprotocol Label Switching (MPLS) - Edge Routers - Label Switching - CE and PE Routers - Data Terminal Equipment (DTE) - Data Communication Equipment (DCE) - Clock speed.

Unit 4 Virutal LANs - Access links and Trunk links - Switchport modes - Vlan Trunking - Server, Client and Transparent modes - VTP Domain - Configuration Revision numbers - Inter Vlan Communications - Broadcast domain - Collision Domain

Unit 5 Communication protocols - Address Resolution Protocol (ARP) - Reverse Address Resolution Protocol (RARP) - Internet Control Message Protocol (ICMP) - Internet Protocol (IP) - Transmission Control Protocol (TCP) - User Datagram Protocol (UDP) - American Standard Code for Information Interchange (ASCII) - Hypertext Transfer Protocol (HTTP) - File Transfer Protocol (FTP) - Simple Mail Transfer Protocol (SMTP) - Telnet - Trivial File Transfer Protocol (TFTP) - Post Office Protocol version 3 (POP3) - Internet Message Access Protocol (IMAP) - Simple Network Management Protocol (SNMP) - Domain Name System (DNS) - DNS Flags - Dynamic Host Configuration Protocol (DHCP).

Core Paper III – Introduction to Information Security

Unit 1: Overview of Information Security - What is Information and why should be protect it? - Information Security - Threats - Frauds, Thefts, Malicious Hackers, Malicious Code, Denial-of-Services Attacks and Social Engineering - Vulnerability – Types - Risk – an introduction - Business Requirements - Information Security Definitions - Security Policies - Tier1 (Origination-Level), Tier2 (Function Level), Tier3 (Application/Device Level) – Procedures - Standards - Guidelines

Unit 2: Information Asset Classification - Why should we classify information? - Information Asset – Owner, Custodian, User - Information Classification - Secret, Confidential, Private and Public – Methodology - Declassification or Reclassification - Retention and Disposal of Information Assets - Provide Authorization for Access – Owner, Custodian, User

Unit 3: Risk Analysis & Risk Management - Risk Analysis Process - Asset Definition - Threat Identification - Determine Probability of Occurrence - Determine the Impact of the Threat - Controls Recommended - Risk Mitigation - Control Types/Categories - Cost/Benefit Analysis

Unit 4: Access Control - User Identity and Access Management - Account Authorization - Access and Privilege Management - System and Network Access Control - Operating Systems Access Controls - Monitoring Systems Access Controls - Intrusion Detection System - Event Logging - Cryptography

Unit 5: Physical Security - Identify Assets to be Protected - Perimeter Security - Fire Prevention and Detection - Safe Disposal of Physical Assets.

Core Paper –IV IT Infrastructure and Cloud Computing

Unit 1: Computer Hardware Basics

- Basics of Motherboard including CMOS and BIOS
- Working of processors and types of processors
- System memory
- Introduction to RAM
- System storage devices
    - Types of hard disks - FAT, NTFS, RAID etc.
    - Optical drives
    - Removable storage devices
    - Tape drives and backup systems
- Common computer ports – Serial – Parallel - USB ports etc.
- Different input systems - Key Board - Mouse etc.
- Display arrays – VGA – SVGA – AGP
- Additional display cards
- Monitors and their types
- Printers and their types

Unit 2: Operating Systems

- Operating system basics
    - Functions of operating system
    - Functions of Client Operating System
    - Functions of Server operating system
    - Introduction to Command line operation
- Basics on files and directories
- Details about system files and boot process
- Introduction to device drivers

Unit 3: Computer Principles and a Back Box Model of the PC

- Memory and processor
- Address and data buses
- Stored program concept
- **Physical components of the PC and how they fit together and interact**
- Basic electrical safety
- Motherboards and the design of the PC
- Dismantling and re-building PCs
- **Power On Self Test and boot sequence**
    - Architecture of real mode
    - Interrupts
    - Start of boot sequence
    - Power On Self Test (POST)

Unit 4: Enterprise and Active Directory Infrastructure

- Overview of Enterprise Infrastructure Integration
- Requirement to understand the Enterprise Infrastructure

- Enterprise Infrastructure Architecture and it's components
- Overview of Active Directory (AD)
- Kerberos
- LDAP
- Ticket Granting Ticket {TGT}
- Forest
- Domain
- Organization Unit (OU)
- Site Topology of a Forest
- Trust Relationships
- Object – Creation, Modification, Management and Deletion
    - User
    - Group
    - Computer
    - OU
    - Domain
- Group Policy (GPO) Management
    - Structure of GPO
    - Permissions and Privileges
    - GPO Security Settings
        - Password Settings
        - Account Lockout Settings
        - Account Timeout Settings
        - USB Enable/ Disable Settings
        - Screen Saver Settings
        - Audit Logging Settings
        - Windows Update Settings
        - User Restriction Settings
    - Creation of GPO
    - Linking a GPO
    - Application of GPO
        - Linking a GPO
        - Enforcing a GPO
        - GPO Status
        - Inclusion / Exclusion of Users/ Groups in a GPO
    - Precedence of GPO
    - Loopback Processing of GPO
    - Fine-Grain Policy / Fine-Grain Password Policy
- Addition of Windows Workstations to Domain and Group Policy Synchronisation
- Addition of Non-Windows Workstations in AD Environment
- Integrating Finger-Print, Smart Card, RSA or secondary authentication source to Active Directory
- Single-Sign On Integration
- Active Directory Hardening Guidelines

Unit 5: Cloud Computing

- Concept – Fundamentals of Cloud Computing
- Types of clouds
- Security Design and Architecture

- Cloud Computing Service Models
- The Characteristics of Cloud Computing
- Multi Tenancy Model
- Cloud Security Reference Model
- Cloud Computing Deploying Models
- Cloud Identity and Access Management
    - Identity Provisioning – Authentication
    - Key Management for Access Control – Authorization
    - Infrastructure and Virtualization Security
    - Hypervisor Architecture Concerns.

- **Understanding Cloud Security**
    - Securing the Cloud
    - The security boundary
    - Security service boundary
    - Security mapping
    - Securing Data
    - Brokered cloud storage access
    - Storage location and tenancy
    - Encryption
    - Auditing and compliance
    - Establishing Identity and Presence
    - Identity protocol standards

Elective 1 – Forms of Cyber Crime

Unit 1: Cyber Crime – Introduction – History and Development – Definition, Nature and Extent of Cyber Crimes in India and other countries - Classification of Cyber Crimes – - Trends in Cyber Crimes across the world.

Unit 2 : Forms of Cyber Crimes , **Frauds** – hacking , cracking, DoS – viruses, works, bombs, logical bombs, time bombs, email bombing, data diddling, salami attacks, phishing, stegnography, cyber stalking, spoofing, pornography, defamation, computer vandalism, cyber terrorism, cyber warfare, crimes in social media, malwares, adware, scareware, ransomware, social engineering, credit card frauds & financial frauds, telecom frauds. Cloud based crimes – understanding fraudulent behaviour, fraud triangle, fraud detection techniques, Intellectual Property Rights and Violation of Intellectual Property rights, Ecommerce Frauds and other forms .

Unit 3 : Modus Operandi of various cybercrimes and frauds – Definition of various types of cyber frauds **–** Modus Operandi **-** Fraud triangle – fraud detection techniques including data mining and statistical references - countermeasures.

Unit 4: Profile of Cyber criminals – Cyber Crime Psychology – Psychological theories dealing with cyber criminals

Unit 5: Impact of cybercrimes – to the individual, to the corporate and companies, to government and the nation.

SEMESTER II

Core Paper V - Network Security and Cryptography

Unit 1 Network Security - The CIA Triad - DAD - Internet Key Exchange (IKE) - Internet Protocol Security (IPSec) - AH and ESP Header - Security Associations - Transport Layer Security (TLS) - Secure Electronic Transaction (SET) - Extensible Authentication Protocol (EAP) - Protected Extensible Authentication Protocol (PEAP) - Lightweight Extensible Authentication Protocol (LEAP) - Secure Multipurpose Internet Mail Extensions (S/MIME) - Pretty Good Privacy (PGP).

Unit 2 Point-to-Point Protocol (PPP) - Challenge Handshake Authentication Protocol (CHAP) - Password Authentication Protocol (PAP) - High Level Data link Control (HDLC) - Remote Authentication Dial-In User Service (RADIUS) - Terminal Access Controller Access-Control System (TACACS+) - Tunneling Protocols in the Data Link Layer - Layer 2 Forwarding (L2F) - Layer 2 Tunneling Protocol (L2TP) - Point-to-Point Tunneling Protocol (PPTP)

Unit 3 Security Threats and Vulnerabilities - Virus - Trojan - Rootkits - Backdoors - Botnets - Man in the middle attack - Dos and DDos - Replay attack - Spoofing - Spam - Phishing - privilege escalation - DNS poisoning - Brute force - Dictionary attack - Cross-site scripting - SQL injection - Zero-day attack - Session hijacking - Vulnerability scanning vs Port Scanning - Honeypots - Banner grabbing - Social Engineering.

Unit 4 Cryptology - Cryptosystems - Symmetric vs asymmetric cryptosystem, Goals of Cryptographhy - Confidentiality, Integrity and Non-repudiation - Ciphers, (Block ciphers and stream ciphers), Transposition Ciphers - Substitution Ciphers - One-Time Pads - Codes vs. Ciphers - Cryptographic keys, - Hashing Algorithms - IPSec - AH and ESP - Security Associations - ISAKMP. Wireless Network security, WEP, WPA, WPA2, TKIP - CCMP.

Unit 5 Symmetric Key Algorithms - Data Encryption Standard (DES) - DES Keys - DES Algorithm - Electronic Codebook Mode - Cipher Block Chaining Mode - Cipher Feedback Mode - Output Feedback Mode - Counter Mode - Triple DES (3DES) - DES Variants - DES-EEE3 - DES-EDE3 - DES-EEE2 - DES-EDE2 - International Data Encryption Algorithm (IDEA) - Blowfish - Skipjack - Advanced Encryption Standard (AES) - CAST - Password hashes and Salting - Asymmetric Key Algorithms - RSA - Diffie-Hellman - Private key and Public key - Digital Signature - Public Key Infrastructure (PKI) - Certificate Authorities - Certification Revocation List (CRL) - Digital Signature.

Core Paper VI – Basics of Cyber Forensics

Unit 1: Digital Investigation - Digital Evidence and Computer Crime - History and Terminology of Computer Crime Investigation - Technology and Law - The Investigative Process -Investigative Reconstruction - Modus Operandi, Motive and Technology -Digital Evidence in the Courtroom.

Unit 2 :**Understanding information** - Methods of storing data: number systems, character codes, record structures, file formats and file signatures - Word processing and graphic file formats - Structure and Analysis of Optical Media Disk Formats - Recognition of file formats and internal buffers - Extraction of forensic artifacts– understanding the dimensions of other latest storage devices – SSD Devices.

Unit 3: **Computer Basics for Digital Investigators -** Computer Forensic Fundamentals - Applying Forensic Science to computers - Computer Forensic Services - Benefits of Professional Forensic Methodology -Steps taken by computer forensic specialists.

Unit 4:Standards, Guidelines and Best Practices- Handling the Digital Crime Scene - Digital Evidence Examination Guidelines –ACPO – IOCE – SWGDE -DFRWS – IACIS – HTCIA - ISO 27037

Unit 5: Types of Computer Forensics Tools and Technology -Tools and Types of Military Computer Forensics Technology -Tools and Types of Law Enforcement Computer Forensic Technology -Tools and Types of Business Computer Forensic Technology

Core Paper VII – Telecom Frauds & Countermeasures

Unit 1 : Frauds in IT - IT Frauds (Theft of Proprietary Information, Insider abuse of internet access, system penetration, unauthorised access to information, laptop/mobile theft, financial fraud, misuse of public web application, virus, abuse of wireless network) – Countermeasures.

Unit 2: Frauds in Software development and Management – Software industry frauds – counter measures.

Unit 2: Introduction to Telecom Frauds - What is 'Telecommunication Fraud'? - Telecommunication Technologies referred (GSM, CDMA, GPRS, PBX, NGN Networks, Analog Networks) - About Fraudsters - Benefits to Fraudsters - Using a service without - Call selling to others - Root Causes of Fraud - Mitigation and Demographics - Penetration of new technology - Staff Dissatisfaction – Illustrative cases

Unit 3: Classification of Telecommunication Fraud - Frauds in different segments of Telco operations (such as Customer Care, Operational Support Systems, Network Management Systems)Organizational or Non-Technical Fraud (involving Administration services, processes) - Human Fraud - Insider Fraud - Call-sell Fraud - Facilitation Fraud - Creeping Fraud - Chaining Fraud - Calling-Card Fraud - Phantom Account - Partnership Fraud - Process Fraud – Ghosting - Abuse of test or emergency lines or accounts - Unauthorized Feature/Service Activation – Accounting - Dealer or Reseller Fraud - Subscription Fraud - Roaming Subscription Fraud - Premium-Rate Services Fraud- Illustrative Cases - Technical Fraud (involving Network Systems, Billing Systems) – Cloning – Tumbling - Voice-mail Hacking - PBX Hacking - SIM Stuffing- Clip-on Fraud - Line Tapping - War Dialing - Handset Fraud

Unit 4: Frauds in Fixed Network & Mobile Network: Fixed network Fraud **-** The development of Fixed Networks - Common types of Frauds affecting Fixed line telcos - Subscription Fraud - Physical attacks on networks - Premium rate fraud - PBX/DISA fraud - Threat of SS7 attacks - Methods of mitigating the risks these practices present Mobile network Fraud **-** The security of mobile networks - Frauds in wireless domain - Before Pre-Call Validation - After Pre-Call Validation - Fraud Detection Systems - Subscription Fraud - The best ways to reduce the risk of mobile network fraud

Unit 5: Common Telecommunication Frauds - Clip-on and Boxing Fraud - EPABX Hacking - Unauthorized disclosure of information - Unauthorized amendment of data - Denial of Service attack - Toll Fraud (call theft) - Mailbox abuse - Fax abuse - Vulnerabilities and their Impact – Controls - Security Policy - Managing the Risks - Awareness Training - Controlling Physical Access - Controlling Logical Access - Illustrative Cases - Calling-Card Theft - Call Forwarding Scams – Cloning - Cloning in GSM Networks - Tumbling or Magic Phones - Dealer or Reseller Fraud - Pre-paid Fraud - Social Engineering and Friendly Fraud - Insider Fraud - Identity Theft – Delinquency - Local Subscription Fraud - Roaming Subscription Fraud - Content and Value Added Services (VAS) Fraud - Common Fraud Techniques used today **Frauds in 3G Networks -** Introduction to 3G Technology and Services - The 3G Business Model - Telecom Frauds in a 3G environment - Subscription Fraud - Credit-card Fraud on M-commerce - Micro-payment Fraud - Premium rate Services (PRS) Frauds - Copyright Infringement and content resale frauds ('piracy') - IP Security issues in 3G – Hacking - DOS Attacks - Virus, Worms and Trojans - Data Interception -

Database attacks – Spam - How network security needs to change with the move to 3G - Security and Law enforcement issues in 3G – Fraud Management Perspective - **– A Strategic Perspective -** Telecom Laws – Domestic and International - Fraud Management System - Architecture of an FMS solution

Core Paper VIII – Practical-Networking & Information Security

Elective II - BFSI Frauds & Countermeasures

Unit 1:Introduction to BFSI - Banking Concepts - Broad features of Deposit and Loan Products - Types of banks: Retail, Corporate, Investment, Development, Private, etc. - Ancillary services like Trade Finance, Remittances, etc. - Anti Money Laundering and KYC concepts.

Unit 2: Computerized operations of banks

Evolution of computerization in banks - Core Banking Solution - Infrastructure requirements - Broad software features - Various methods, options available for customizing like Setting up Chart of Accounts Parameterising Products, Interest Rates and Charges - User restrictions and transaction types - Delivery Channel Options for direct customer access to databases

Unit 3 :Basel II

Need for Basel Regulations - Three pillars - Types of risks - Operational Risk overview with focus on IT risk - Relation of Bank related cyber crimes to Operational risk

Unit 4: Vulnerable areas in CBS and their exploitation - Application related - Parameters and freedom available to users - Empowerment of users - Access to -organization -wide data - Direct access to database and records - Multiple interfaces with other applications ATM Network, Anti-Money Laundering Application

Unit 5: Money Laundering and Anti Money Laundering - Money laundering techniques and the vulnerabilities of specific financial services products - The process of money laundering - How is money laundered? - Limitations of the staged interpretation of money laundering - Vulnerabilities of specific services and products - The duties and responsibilities of the Money Laundering Reporting Officer (MLRO) - The role of the MLRO - Generating management information - Common MLRO problems - Recognition, handling and reporting transactions - The legal obligation to report - Designing an effective internal reporting system - The MLRO's evaluation process **-** Corruption in BFSI Sector – Types – Security Controls - Counter Measures.

Elective III – Data Privacy

<u>Introduction to Data Privacy</u>

Unit 1: Introduction to Privacy

Data Protection & Privacy Terminologies - Data Protection Principles and Approaches to Privacy - Code for protection of Personal Information - Information Life Cycle -Data Security Threats and Mitigation - Data Storage Security Issues in Cloud Computing

Unit 2: Data protection principles and Safeguards

Data protection principles - Subject access request Damage or distress - Preventing direct marketing Automated decision taking - Correcting inaccurate personal data - Compensation, Exemptions & Complaints - Big data - CCTV & Data sharing - Online & apps Privacy by design - Guidance Note on Protecting the confidentiality of Personal Data - Safeguarding Personal Information - Using Personal Information on Websites and with Other Internet-related Technologies - Privacy considerations for sensitive online information, including policies and notices, access, security, authentication identification and data collection. - Data Privacy in online data collection, email, searches, online marketing and advertising, social media, online assurance, cloud computing and mobile devices.

Unit 3: Data Privacy Management

Data Privacy Management controls & Plan - Data Privacy Management Reference Model – ISTPA - Data Protection in the context of Police and Criminal Justice - Cross Border data transfer - Do not Track Privacy Policy - Developing Privacy Management Tools - Information security practices for data privacy - Developing a privacy management plan - Rights of the Data Subject - Documenting the privacy baseline of the organization - Data processors and third-party vendor assessments - Physical assessments; mergers, acquisitions and divestures - Privacy threshold analysis; privacy impact assessments - Privacy Monitoring and Incident Management (MIM) - Auditing your privacy program; creating awareness of the organization's privacy program; Compliance monitoring; handling information requests; and handling privacy incidents.

Unit 4: Privacy Program Governance and Compliance and Legal Framework

Privacy Organization and Relationship (POR) - Privacy Policy and Processes (PPP) - Regulatory Compliance Intelligence (RCI) - Privacy legislations - applicability and interpretation - Privacy Awareness and Training (PAT) – Legal Framework for Data protection, Security and Privacy Norms

Unit 5: Privacy in cloud computing and IOT

Privacy in Cloud _ Introduction to Privacy in cloud computing - Cloud computing paradigm and privacy - Challenges to privacy in cloud computing - Privacy in IoT - IoT Governance - IoT Security & Privacy Issues - IoT Privacy challenges - IoT Privacy solutions

Core Paper IX – Database and Management Security

Unit -1: Fundamentals of Databases

- What is a Database?
- DBMS - Purpose of DB and Users of DB
- Components of DB
- Concepts of RDBMS

- Basic SET Concepts (SET, Subset)
- Set of Ordered Tuples - Relations as a DB (Concepts of PK, FK, Surrogate Keys, Composite Keys, Candidate Keys)
- Relational DB Operators (Cartesian Product, Union, Intersect, Difference)
- Relational DB Normal Forms (1NF, 2NF, 3NF) - E-R Model.

Unit 2: Database Security Lifecycle

- Concept of DB Security Lifecycle
- Creating Data Risk Assessment
- Analyzing data threats, risks & vulnerabilities
- Need for database security architecture
- Implementing feedback mechanisms
- Adjusting policies & practices based on feedback mechanisms using different security models

Unit 3: Database Security

- Models
    - Access Matrix Models
    - Objects & Subjects
    - Types of Objects & Subjects
    - Access Modes (Static & Dynamic)
    - Access Levels
- Issues in Database Security
- Database Access Controls
- Security Logs and Audit Trails
- Encryption
- SQL Data Control Language
- Security in Oracle
- Statistical Database Security
- SQL Injection
- Database Security and the Internet

Unit 4: Password Management

- Authentication and Password Security
    - Choosing an appropriate authentication option
    - Understanding system administration privileges
    - Choosing strong passwords, Implementing account lockout after failed login attempts
    - Creating and enforcing password profiles
    - Using passwords for all database components
    - Understand and secure authentication back doors

Unit 5: Virtual Private Databases

- Introduction to Virtual Private Databases (VPDs)
- Need for VPDs
- Implementing VPDs

Core Paper X - Advanced Cyber Forensics

Unit 1: Windows Forensics

- Volatile Data Collection
  - Memory Dump
  - System Time
  - Logged On Users
  - Open Files
  - Network Information (Cached NetBIOS Name Table)
  - Network Connections
  - Process Information
  - Process-to-Port Mapping
  - Process Memory
  - Network Status
  - Clipboard Contents
  - Service / Driver Information
  - Command History
  - Mapped Drives
  - Shares
- Non-Volatile Data Collection
  - Disk Imaging (External Storage such as USB and Native Hard Disk)
  - Registry Dump
  - Event Logs
  - Devices and Other Information
  - Files Extraction
  - Write-Blocking port
- Registry Analysis
- Browser Usage
- Hibernation File Analysis
- Crash Dump Analysis
- File System Analysis
- File Metadata and Timestamp Analysis
- Event Viewer Log Analysis
- Timeline Creation
- Evidence Collection in Linux and Mac Operating system

Unit 2: Network Forensics

- Understanding Protocols with Wireshark

    - TCP
    - UDP
    - HTTP(S)
    - SSH
    - Telnet
    - SMTP
    - POP / POP3
    - IMAP
    - FTP
    - SFTP
    - ARP
- Packet Capture using Wireshark, tshark and tcpdump
- Packet Filtering
- Extraction of Data from PCAP file
- Netflow vs Wireshark
- Analysis of logs
    - CISCO logs
    - Apache Logs
    - IIS Logs
    - Other System Logs

Unit 3: Memory Forensics

- History of Memory Forensics
- x86/x64 architecture
- Data structures
- Volatility Framework & plugins
- Memory acquisition
- File Formats – PE/ELF/Mach-O
- Processes and process injection
- Windows registry
- Command execution and User activity
- Networking; sockets, DNS and Internet history
- File system artifacts including $MFT, shellbags, paged memory and advanced registry artifacts
- Related tools – Bulk Extractor and YARA
- Timelining memory
- Recovering and tracking user activity
- Recovering attacker activity from memory
- Advanced Actor Intrusions

Unit 4: Virtual Machine Forensics

- Types of Hypervisors
- Hypervisor Files and Formats
- Use and Implementation of Virtual Machines in Forensic Analysis

- Use of VMware to establish working version of suspect's machine
- Networking and virtual networks within Virtual Machine
- Forensic Analysis of a Virtual Machine
    - Imaging of a VM
    - Identification and Extraction of supporting VM files in the host system
    - VM Snapshots
    - Mounting Image
    - Searching for evidence

Unit 5: Cloud Forensics

- Introduction to Cloud computing
- Challenges faced by Law enforcement and government agencies
- Cloud Storage Forensic Framework
    - Evidence Source Identification and preservation in the cloud storage
    - Collection of Evidence from cloud storage services
    - Examination and analysis of collected data
        - Cloud Storage Forensic Analysis
        - Evidence Source Identification and Preservation
        - Collection of evidence from cloud storage devices
        - Examination and analysis of collected data
- Dropbox analysis:
    - Data remnants on user machines
    - Evidence source identification and analysis - Collection of evidence from cloud storage services
    - Examination and analysis of collected data -
- Google Drive:
    - Forensic analysis of Cloud storage and data remnants
    - Evidence source identification and analysis - Collection of evidence from cloud storage services
    - Examination and analysis of collected data –
- Issues in cloud forensics
- Case Studies.

Core Paper XI - Advanced Information Security

Unit 1: Digital Rights Management - Meaning of Digital Rights Management (DRM) - Need for DRM and preventing illegal file sharing on the Internet - DRM schemes - Microsoft DRM 2.0, and the Content Scrambling System - Reasons why DRM schemes have been unsuccessful so far - Requirements for a good DRM scheme - secure hardware, secure software, and an efficient legal system

Unit 2: Managing Identity and Authentication - Controlling access to assets – Comparing identification to Authentication- Implementing Identity Access Management – Access provisioning life cycle management – Physical Security

Unit 3: Common Authentication Protocols - Authentication concepts - Various authentication protocols - Password Authentication Protocol (PAP) - Challenge Handshake Authentication

Protocol and MS Chap - Extensible Authentication Protocols - Remote Access with RADIUS and TACACS - Single Sign on – Kerberos, SEASAME – Authentication in Wireless networks

Unit 4: Real World Protocols – IPSec, SSL, IKH, AH and ESP - Introduction to IPSec - IPSec building blocks - Security Associations (SAs) - Security Parameter Index (SPI) - IPSec Architecture - IPSec Protocols - Authentication Header (AH) - Encapsulation Security Payload (ESP) - Tunneling and Transport Mode - Internet Key Exchange (IKE) – ISAKMP

Unit 5: Application System Security - SDLC concepts - Different SDLC and cost estimation models - Testing: types, methods and issues - Program coding and security to be built into it - Software maintenance and change control processes - Configuration management - Software Capability Maturity model (CMM) - DBMS concepts & terms: types, with focus on Relational model - Data dictionary – Interfaces to databases (ODBC, ADOJDBC, XML) - Database security features - User access rights – Database auditing features and logs.

Unit 6 : Cryptology- Classical Encryption Techniques - Substitution Techniques - Transposition Techniques – Steganography - Permutation Methods - Confidentiality using conventional encryption - Placement of Encryption - Traffic Confidentiality - Key Distribution - Random Number Generation - Key Management - Generating Keys - Nonlinear Keyspaces - Transferring Keys - Verifying Keys - Using Keys - Updating Keys - Storing Keys - Backup Keys - Compromised Keys - Lifetime of Keys - Destroying Keys - Public-Key Key Management - Criminal Code Systems Analysis - Sports Bookmaking Codes - Horse Race Bookmaking Codes - Number Bookmaking Codes - Drug Codes - Pager Codes.

Core Paper XII – Practical II (Cyber Forensics)

Elective IV - Cyber Laws and Intellectual Property Rights

Unit 1: Fundamentals of Cyber Law

- Introduction on cyber space
- Jurisprudence of Cyber Law
- Scope of Cyber Law
- Cyber law in India with special reference to Information Technology Act, 2000 (as amended) and Information Technology Act, 2008.

Unit 2: E- Governance and E – Commerce

- Electronic Governance
- Procedures in India
- Essentials & System of Digital Signatures
- The Role and Function of Certifying Authorities
- Digital contracts
- UNCITRAL Model law on Electronic Commerce
- Cryptography – Encryption and decryption

Unit 3: Cyber Crimes Investigation

- Investigation related issues
- Issues relating to Jurisdiction
- Relevant provisions under Information Technology Act, Evidence Act
- Indian Penal Code
- Cyber forensics - Case studies

Unit 4: Trademark, Copyright and Patent laws

- Definitions and concepts
- **Trademark**
  - Introduction to Trademarks
  - Functions and types of Trademarks
  - Madrid Agreements
  - Trademarks Law Treaty (Geneva)
  - Indian Trademark Act
  - Registration of Trademarks
  - Rights conferred by Registration of Trademarks
  - Infringement of Registered Trademark
  - Defenses
  - Trademarks dilution
  - International Applications and Case Studies
- **Copyright**
  - Basics
  - Copyright Law
  - Terms of Copyright
  - Registration of Copyrights
  - Transfer of Ownership of Copyright
  - Infringement
    - Liability
    - Exemptions
    - Defenses
    - Case Studies
    - Copyrights Laws in India
- **Patent Law**
  - Basics
  - Conditions of Patentability
  - WIPO Patent Co-operation Treaty
  - Geneva convention on Patent Law
  - Software and Business Method Patents
  - Indian Patent Act
  - Infringement
  - Defenses

Unit 5: Intellectual Property Rights

- Concept of IPR
- Global Scenario with Case Laws
- IPR infringements
- Secrecy and Confidentiality in IPR
- Civil and Criminal liabilities in IPR

- International Applications and its advantages
- Important international conventions and Treaties
  - Paris Industrial Property
  - Berne convention literary and artistic work
  - WIPO copyright Treaty
  - ROME Convention for protection of Performers, producers and broadcasting organization
  - PRIPS Agreement on Trade related aspects of IPR
  - Brussels satellite convention
- IPR and Criminal Jurisprudence

SEMESTER IV

Core Paper XIII – Application Security

Application Security

Unit 1: Application Types

- Client/Server Applications
- Components of Client/Server Applications (Logical & Physical Architecture)
- Web Applications
  - About Web Applications
  - Technologies used to create Web Applications
  - Components of Web Application Architecture
- Data Warehouse Applications
  - About DW Applications
  - Uses
  - Physical & Logical Architecture
- Management Information Systems

Unit 2: Web application security

- Introduction to web application
  - Primer
  - OWASP Top 10 vulnerabilities
  - Mitigation techniques
- Web Application Security Fundamentals
  - What Do We Mean By Security?
  - The Foundations of Security
  - Threats, Vulnerabilities, and Attacks Defined
  - How to Build a Secure Web Application
- Secure Your Network, Host, and Application
  - Securing Your Network
  - Network Component Categories
  - Securing Your Host
  - Host Configuration Categories
- Securing Your Application
  - Application Vulnerability Categories
  - Security Principles

Unit 3: Threats and Countermeasures

- Overview : Anatomy of an Attack
  - Survey and Assess
  - Exploit and Penetrate

    - Escalate Privileges
    - Maintain Access
    - Deny Service
- Understanding Threat Categories
    - STRIDE
    - STRIDE Threats and Countermeasures
- Network Threats and Countermeasures
    - Information Gathering
    - Sniffing
    - Spoofing
    - Session Hijacking
    - Denial of Service
- Host Threats and Countermeasures
    - Viruses, Trojan Horses, and Worms
    - Foot printing
    - Password Cracking
    - Denial of Service
    - Arbitrary Code Execution
    - Unauthorized Access
- Application Threats and Countermeasures
    - Input Validation
    - Buffer Overflows
    - Cross-Site Scripting
    - SQL Injection
    - Canonicalization
- Authentication
    - Network Eavesdropping
    - Brute Force Attacks
    - Dictionary Attacks
    - Cookie Replay Attacks
    - Credential Theft
- Authorization
    - Elevation of Privilege
    - Disclosure of Confidential Data
    - Data Tampering
    - Luring Attacks
- Configuration Management
    - Unauthorized Access to Administration Interfaces
    - Unauthorized Access to Configuration Stores
    - Retrieval of Plaintext Configuration Secrets
    - Lack of Individual Accountability
    - Over-privileged Application and Service Accounts
- Sensitive Data

- Access to Sensitive Data in Storage
- Network Eavesdropping
- Data Tampering

- Session Management
  - Session Hijacking
  - Session Replay
  - Man in the Middle Attacks
- Cryptography
  - Poor Key Generation or Key Management
  - Weak or Custom Encryption
  - Checksum Spoofing

- Parameter Manipulation
  - Query String Manipulation
  - Form Field Manipulation
  - Cookie Manipulation
  - HTTP Header Manipulation
- Exception Management
  - Attacker Reveals Implementation Details
  - Denial of Service
- Auditing and Logging
  - User Denies Performing an Operation
  - Attackers Exploit an Application Without Leaving a Trace
  - Attackers Cover Their Tracks

Unit 4: Mobile application security

- Mobile Platforms
  - Top issues facing mobile devices
  - Secure Mobile application development
  - Android security
  - iOS Security
  - Windows, Blackberry & Java Mobile Security
  - Symbian OS security
  - Web OS security
  - WAP and mobile HTML Security
  - Blue tooth security
  - SMS Security
  - Mobile Geo location
  - Enterprise Security on Mobile OS
  - Mobile Malwares
  - Mobile security penetration security
  - Encryption and authentications
  - Mobile privacy concerns

Unit 5: Threat Modeling

- Overview
- Threat Modeling Principles
  - The Process
  - The Output
- Step 1. Identify Assets
- Step 2. Create an Architecture Overview
  - Identify What the Application Does
  - Create an Architecture Diagram
  - Identify the Technologies
- Step 3. Decompose the Application
  - Identify Trust Boundaries
  - Identify Data Flow
  - Identify Entry Points
  - Identify Privileged Code
  - Document the Security Profile
- Step 4. Identify the Threats
  - Identify Network Threats
  - Identify Host Threats
  - Identify Application Threats
  - Using Attack Trees and Attack Patterns
- Step 5. Document the Threats
- Step 6. Rate the Threats
  - Risk = Probability * Damage Potential
  - High, Medium, and Low Ratings
  - DREAD
- What Comes After Threat Modeling?
  - Generating a Work Item Report

Unit 6: Application security standards and checklist

- Application security checklist **NIST**
- **OWASP** security checklist
- **OWASP** Application Security Verification Standard

Core Paper XIV – Governance, Risk & Compliance

Unit 1: Governance, Risk & Compliance definition, Scope and Objectives - IT Governance Metrics & Framework – BASEL - OECD

Unit 2: Best Practices for IT Governance – ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) - The Information Security Management Maturity Model - Capability Maturity Model – Any other latest standards and compliance technologies.

Unit 3: Information Security Governance - Effective Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment - Value Management - Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee - Policies and Procedures

Unit 4: Information Security Management Practices - Personnel Management - Financial Management – Quality Management - Information Security Management - Performance Optimization - Roles and Responsibilities - Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools - Case Study Analysis - Risk Management Process - Developing a Risk Management Program - RiskAnalysisMethods – Qualitative, Semi quantitative, Quantitative - Risk Management framework – COSO - The Internal environment - Objective Setting - Event Identification - Risk assessment - Risk Response - Control activities - Information & communication – Monitoring – NIST - Risk Assessment - Risk Mitigation - Evaluation & Assessment - Case Study Analysis

Unit 5: Compliance – Introduction - Information Technology and security - Evolution of Information systems - Roles and responsibilities - Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - Compliance officer activities - The requirements of a Compliance Officer - Drafting compliance reports - Designing an Internal Compliance System - Regulatory principles – Issues - Developing high-level compliance policies - Defining responsibility for compliance - The compliance function - Specific internal compliance control issues – Information System Audit - Scope of System Audit - Audit Planning - Audit Manual - Audit check lists - Audit Reports - Best Practices for IT compliance and Regulatory Requirements - IT Compliance requirements under clause 49 of SEBI Listing agreement - IT Compliance requirements under Sarbanes Oxley Act of USA - Control Objectives in Information Technology of ISACA

Core Paper XV – Business Continuity & Disaster Recovery Management

Unit 1: Introduction - Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR) - Terms and definitions - BCM principles - BCM lifecycle - (BCM programme management, Understanding the organization - Determining business continuity strategy, Developing and implementing a BCM response, BCM exercising, Maintaining and reviewing BCM arrangements, Embedding BCM in the organization's culture) - BCM in business: Benefits and consequence - Contemporary landscape: Trends and directions

Unit 2: Risk Management - BCM and DR – The relationship with Risk Management - Risk Management concepts and framework - Concepts of threat, vulnerabilities and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting - Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting - Relationship between BIA and Risk Management

Unit 3: Business Continuity Strategy and Business Continuity Plan (BCP) Development - Business continuity strategy development framework - Cost-benefit assessment - Site assessment and selection - Selection of recovery options - Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies - Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools

Unit 4: Business Continuity Plan Testing and Maintenance - Test plan framework - Types of testing - Business Continuity Plan Testing - Plan maintenance requirements and parameters - Change management and control - Business Continuity Plan Audits

Unit 5: Disaster Recovery – Definitions - Backup and recovery - Threat and risk assessment - Site assessment and selection - Disaster Recovery Roadmap - Disaster Recovery Plan (DRP) preparation - Vendor selection and implementation - Difference between BCP and DRP - Systems and communication security during recovery and repair

Core Paper XVI – Security Testing

Unit – 1: Access control Testing

Access control tests of Networks (External interface): Networks (Internal interface and DMZ); Physical access testing – piggybacking, anonymous entry and break-in; wireless access testing; Board classed of testing – Black box of zero knowledge; crystal box or full knowledge testing and grey box testing.

Unit – 2: Security Audit

Choosing the standard against which to audit – ISO27001; PCI-DSS; ISACA Standards; NIST guidelines; national and sector specific standards (eg., RBI guidelines for Bank in India); auditing security policies and procedures; Review and report on IT landscape; defining scope of security audit; maintaining independence and objectivity in audit; internal and third party audit.

Unit – 3: Software testing

Static Testing and dynamic testing; traceability matrix; synthetic transitions; fuzzing of fuzz testing; specific testing to meet different purposes – unit testing, installation testing, integration testing, regression testing, acceptance testing, alpha and beta testing; combinatorial software testing.

Unit – 4: Log Analysis

Identify, collect, collect and retain logs; maintain integrity of logs; types of logs – antivirus logs; IDS/IPS logs; Remote access logs; web proxy generated logs; logs from authentication servers; router logs and firewall logs; log filtering; response to log alerts; transpiration, storage and retrieval of logs.

Unit – 5: Test Management

Deciding objectives of testing; routine vs ad-hoc testing; periodicity of testing and coverage of key areas in the organizational; acting on test results; scheduling the test; selecting test participants; surprise vs planned tests; live vs; simulated tests; crating, using and destroying test data; sanitization of information for testing; precautions when using production data for testing.
