**M A N O N M A N I A M  S U N D A R A N A R  U N I V E R S I T Y**
**TIRUNELVELI-627 012, TAMILNADU, INDIA**

**C E N T R E  F O R  I N F O R M A T I O N  T E C H N O L O G Y  A N D  E N G I N E E R I N G**

# Board of Studies Meeting

## Master of Science (M.Sc.) Degree course in Information Security

**(CBCS-University Department)**

**Regulations, Scheme and Syllabus**
**For those who joined from the academic year 2017-2018 onwards**

**Submitted By**

**Chairman, BOS and Head i/c,**
**Centre for Information Technology and Engineering, MSU**

**To**

**The Registrar**
**Manonmaniam Sundaranar University**
**Tirunelveli – 626 012**

**MANONMANIAM SUNDARANAR UNIVERSITY**
**TIRUNELVELI-627 012, TAMILNADU, INDIA**

**CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING**

Master of Science (M.Sc.) Degree course in Information Security

**(CBCS-University Department)**

**Regulations, Scheme and Syllabus**
**(For those who joined from the academic year 2017-2018 onwards)**

## A. Regulations

M.Sc. degree programme in Cyber Security exposes students, **Learn a practical skill-set in defeating all online threats**, including - advanced hackers, trackers, malware, zero days, exploit kits, cybercriminals and more.

### A1: Duration of the Course:

The M.Sc. programme is a 2 years full time programme spread over two years under semester pattern, with Choice Based Credit System.

### A2: Eligibility for Admission:

The minimum eligibility conditions for admission to the M.Sc. programme in Cyber Security are given below.

The candidates who seek admission into the first semester of the M.Sc. programme in Cyber Security course will be required to have passed the Bachelor's degree (B.Sc./ B.C.A./B.E. equivalent) from Manonmaniam Sundaranar University or any other Indian University or equivalent in any one of the following disciplines:

1. Information Technology
2. Information Technology and E-Commerce
3. Computer Science
4. Computer Technology
5. Software Engineering
6. Computer Applications
7. Physics, Forensics, Electronics
8. Any other discipline with Mathematics or Computer Applications as a subject.

### A3. Structure of the Programme:

This Master's programme will consist of:

a. *Core courses* and *Elective courses* which are compulsory for all students;

b. *I Semester*: 4 Core, 1 Elective and 2 Practical– *II Semester*: 3 Core, 1 Elective, 1 supportive course and 2 Practicals – *III Semester*: 2 Core, 1 Elective , 1 Internship / Industrial Training, 1 supportive course and 2 Practicals – *IV Semester*: 1 Core, 3 Electives and 1 Major Project / Dissertation.

c. Supportive courses which students can choose from amongst the courses offered in other departments of this University

d. **Institutional Visits (Field work), Internship and Dissertation/ Project** are compulsory and included as core.

**A4: Credit Requirement for the Degree:**

The general Regulations of the Choice Based Credit System programme of Manonmaniam Sundaranar University are applicable to this programme. The University requirement for the M.Sc. programme is completion of 90 credits of course work, out of which 12 credits should be through the 4th semester main project work, remaining 78 credits should be through Core, Elective, Internship / Industrial training and Supportive Course papers. A typical theory course (Core/ Elective/ Supportive Course) has 4 credits and lab course weighs 2 credits. No candidate will be eligible for the Degree of Master of Science in Cyber Security, unless the candidate has undergone the prescribed courses of study for a period not less than 4 semesters and has acquired 90 credits and other passing requirements in all subjects of study. The marks, $M_i$ obtained by the student in each subject, $i$ shall be multiplied by the credit of that subject, $C_i$; such marks of all '$n$' subjects are added up and divided by the total credit (90) to obtain the Consolidated Percentage of Marks.

$$\text{Consolidated Percentage of Marks} = \frac{\sum_{i=0}^{n} C_i \times M_i}{\sum_{i=0}^{n} C_i}$$

**A5: Attendance Requirement:**

A candidate will be permitted to appear for the semester examination only if the candidate keeps not less than 75 percent attendance. The University condonation rules are applicable for those who lack minimum of 75% attendance. The candidates with less than 60% attendance will have to repeat the concerned entire semester.

**A6: Assessment**

The assessment will comprise Continuous Internal Assessment (CIA) comprising of tests, seminars and assignments carrying a maximum of 25% marks and end-semester Examination carrying a maximum of 75% marks in each theory subject (Core/Elective/Supportive Course). For practical subjects, Mini Project and Major Project, the CIA is carried out for 40% marks and the External Assessment (Final Lab Exam, Lab Report, Viva-Voce for Practical Subjects and Final Project Presentation, Project Report, Viva-Voce for Mini Project and Major Project) is for 60% marks.

Semester examination will be conducted for all subjects of study, at the end of each Semester.

If a Student wants to carry out the final Major project work in 4th semester in an IT company, the student can get permission from the concerned Project Supervisor and Head of the Department after submitting the Acceptance Letter from the IT Company.

**A7: Passing Requirements**

A candidate who secures not less than 50 percent marks in end-semester examination and not less than 50 percent of the total marks (Continuous Internal Assessment + end-semester examination) in any subject of study will be declared to have passed the subject.

A Candidate who successfully completes the course and satisfies the passing requirements in all the subjects of study and curricular requirements will be declared to have qualified for the award of the Degree.

**A8: Classification of successful candidates**

The candidates who passed written papers, practical papers and Projects shall be classified as follows. Total Marks secured in written papers, practical papers and Project work altogether put as overall percentage along with the credits.

The classification is as follows,

| | Marks Overall % | Classification |
|---|---|---|
| 1. | 75% and above with a First attempt Pass in all subjects | I Class with Distinction |
| 2. | i) 75% above from multiple attempts | I Class |
| | ii) 60% to below 75% | I Class |
| 3. | 50% to below 60% | II Class |

**A9. Power to Modify**

The University may from time to time revise, amend or change the regulations, scheme of examinations and syllabus, if found necessary and such amendments, changes shall come into effect from the date prescribed.

The academic year normally begins in July every year and ends in April. These regulations will come into effect from the academic year 2017-2018 onwards.

**B. Scheme of Examination**
**M.Sc. Cyber Security (CBCS) - FULL - TIME**
**(For those who joined from the academic year 2017-2018 onwards)**
**Duration: Two Years (Four Semesters – 90 Credits)**

| Sem. | Sub. No. | Subject Status | Subject Code / Title | Contact Hrs/Week | Credits |
|---|---|---|---|---|---|
| I | 1. | C | **MCYC11**/ Fundamentals of Cyber Criminology | 4 | 4 |
| | 2. | C | **MCYC12**/Foundations of Information Security | 4 | 4 |
| | 3. | C | **MCYC13**/Introduction to Hardware, Software, Networks and Databases | 4 | 4 |
| | 4. | C | **MCYC14**/Introduction to Data Privacy | 4 | 4 |
| | 5. | E | Elective 1 | 3 | 3 |
| | 6. | L | **MCYL11**/ Information Security Lab | 4 | 2 |
| | 7. | L | **MCYL12**/Networking and Databases Lab | 4 | 2 |
| I Semester Total Credits | | | | | **23** |
| II | 8. | S | LITSA/Supportive Course | 3 | 3 |
| | 9. | C | **MCYC21**/Forms of Cyber Crimes | 4 | 4 |
| | 10. | C | **MCYC22**/Introduction to Digital Forensics | 4 | 4 |
| | 11. | C | **MCYC23**/Cyber Laws and Regulations | 4 | 4 |
| | 12. | E | Elective 2 | 3 | 3 |
| | 13. | L | **MCYL21**/Digital Forensics Lab | 4 | 2 |
| | 14. | L | **MCYL22**/Cyber Law Case Presentations Lab | 4 | 2 |
| II Semester Total Credits | | | | | **22** |
| III | 15. | S | LITSB/Supportive Course | 3 | 3 |
| | 16. | I | **MCYI31-**Internship / Industrial Training * | 4 | 2 |
| | 17. | C | **MCYC31**/ Advanced Digital Forensics | 4 | 4 |
| | 18. | C | **MCYC32**/Advanced Information Security | 4 | 4 |
| | 19. | E | Elective 3 | 3 | 3 |
| | 20. | L | **MCYL31**/Advanced Information Security lab | 4 | 2 |
| | 21. | L | **MCYL32**/Advanced Digital Forensics lab | 4 | 2 |
| I Semester Total Credits | | | | | **20** |
| IV | 22. | C | **MCYC41**/Cyber frauds in the BFSI | 4 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | | sector | | |
| | 23. | E | Elective 4 | 3 | 3 |
| | 24. | E | Elective 5 | 3 | 3 |
| | 25. | E | Elective 6 | 3 | 3 |
| | 26. | P | Dissertation / Major Project work | 6 | 12 |
| I Semester Total Credits | | | | | **25** |

## Electives List

| Sem. | Sub. No. | Subject Status | Subject Code / Title | Contact Hrs/Week | Credits |
|---|---|---|---|---|---|
| I | 1. | Group A | **MCYEA-**Foundations of Cloud Computing Security | 3 | 3 |
| | 2. | | **MCYEB-**Introduction to Networking | 3 | 3 |
| | 3. | | **MCYEC-**Email, Mobile Devices Security | 3 | 3 |
| | 4. | | **MCYED-**Mobile and Wireless Security | 3 | 3 |
| II | 5. | Group B | **MCYEE-**Fundamentals of Blockchains and Crypto-currency | 3 | 3 |
| | 6. | | **MCYEF-**Storage Management and Security | 3 | 3 |
| | 7. | | **MCYEG-**Big Data Technology | 3 | 3 |
| | 8. | | **MCYEH-**Android Mobile Application Development | 3 | 3 |
| III | 9. | Group C | **MCYEI-**Fundamentals of Research Methods and Statistical Applications | 3 | 3 |
| | 10. | | **MCYEJ-**Mobile and Digital Forensics | 3 | 3 |
| | 11. | | **MCYEK-**Data Mining and Warehousing | 3 | 3 |
| | 12. | | **MCYEL-**Big Data Security | 3 | 3 |
| IV | 13. | Group C | **MCYEM-**Detecting and Investigating Cyber Frauds | 3 | 3 |
| | 14. | | **MCYEN-**IT Governance, Risk and Compliance | 3 | 3 |
| | 15. | | **MCYEO-**Business Continuity & Disaster Recovery Management Systems | 3 | 3 |
| | 16. | | **MCYEP-**Incident Response | 3 | 3 |

## C. Syllabus for M.Sc. (Cyber Security)

| Core 1 | MCYC11/ Fundamentals of Cyber Criminology | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble**: Provide instruction to enable students to understand human behavior within a social context. Cybercrime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

**Unit – 1: Concepts of Crime, Law and Criminology**

What is Criminology - Criminology and Deviance - Law and Criminology - Principles of Common Law - Criminal law and justice system - Brief History of Criminology - Role of Criminologists in modern society - Understanding & defining Crime - Consensus view of crime - Conflict view of crime - Interactionist approach to crime - Ethical issues in Criminology (14L)

**Unit 2: Contemporary Forms of Crimes**

White Collar Crimes - Economic Offences - Organized Crimes – Terrorism - Crime and Media - Technology or cyber-crimes - IP related crimes (10L)

**Unit 3: 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. (12L)

**Unit 4: 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 (13L)

**Unit 5: Crime Prevention**

Crime and sense of security - Social control and crime prevention - Community and crime prevention - Contemporary crime prevention approaches (11L)

Total (60L)

**References:**

1. Cyber Criminology: Exploring the internet crimes and criminal behavior by K. Jaishankar, Illustrated Edition, CRC Press, 2011.

2. Cyber Law: Law of Information Technology and Internet by Anirudh Rastogi, L.L.M Harvard, 1st Edition, Lexis nexis Publication, 01 Sep 2014
3. Computer Forensics and Cyber Crime by Britz M T , 3rd Edition, Pearson Education Publication, 2013.
4. Cyber Crime: Issues, Threats and management by Jain Atul, 1st Edition, Isha books Publication, 15 Nov 2014

| Core 2 | MCYC12/Foundations of Information Security | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble:** In order to understand the value and requirements of security awareness. The module provides an overview over several foundational areas in information security. The core of the module is given over to a rigorous discussion of security models and their relation to access control models with selected issues in identification and authentication and their required trust and reputation models also covered.

**Unit 1: Conceptual foundation of information security**

Information as an asset to be protected – the CIA triad – threats to information assets: loss, copying, altering, denial of service, malware injection, natural threats like fire, flood, etc. – intangibility of information as an asset – Policies and procedures to protect information assets – the AAA paradigm (11L)

**Unit – 2: Risk management**

Introduction to information risk management – threat horizon – vulnerabilities – CVE databases - attack path – probability of occurrence of risky events – impact of risky events – risk appetite – risk treatment plans – quantitative and quantitative risk assessment (12L)

**Unit – 3: Information classification and valuation**

Rationale for asset classification – approaches to classification – Benefits of classification – Determining the value of information – Data retention – Disposal of information assets – owners and custodians of information – roles, responsibilities and liabilities of owners and custodians of information – De-classification of information – reclassification of information (13L)

**Unit-4: Access Controls**

Concept of restricted and regulate access to information assets – physical vs. logical access controls – user identity and access management – provision and escalation of privileges of access – single sign on – access to networks, databases, applications and operating systems – Access monitoring and review process – event logging – providing access to data at rest and in transit (14L)

**Unit-5: Perimeter security**

Defining physical and logical perimeters of information assets - Integrating physical and logical security - Physical assets as repositories of information assets – choke points on perimeter – physical security standards as applied to data centers (10L)

Total (60L)

**References:**

1. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
2. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
3. ISO/ IEC 27002: 2005, First Edition

| Core 3 | MCYC13 / Introduction to Hardware, Software, Networks and Databases | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble**: To learn basic components of information technology. An information system is the combining of users, technology and processes to complete a specific goal. The network model is a database model conceived as a flexible way of representing objects and their relationships.

**Unit-1: Computer Hardware Basics**

Components of a computer – CMOS and BIOS – processors: types and functions – RAM: role and types – Hard disks – FAT and NTFS – RAID – Removable storage devices – Common forms of data ports – Display standards and cards – printers and scanners (11L)

**Unit-2: Operating Systems and Interface**

OS basics – functions of OS – Windows and Linux family of OS – Client and Server operating systems: principal roles and differences – Command line access – device drivers (10L)

**Unit-3: Databases**

The evolution of databases – types of databases – relational databased management systems – ERP – security issues in RDBMS – databases as back-end to web sites – access control granularity in databases – SQL: process and vulnerabilities (14L)

**Unit-4: Networks**

Concept and need for networking – Components: Switches and routers – Cables: types and choice – LAN and WAN: architecture and protocols – OSI 7-layer model – Routing – Packet and Circuit switched connections – DNS, DHCP and ADS as parts of end-user networking (12L)

**Unit-5: Cloud Computing**

Concepts and fundamentals – types of clouds – challenges to storage of data in cloud - cloud computing service models – deployment strategies – standards for security in cloud environment (13L)

Total (60L)

**References:**

1. Basic of Networking – Prentice Hall (ISBN 8120324897)
2. Introduction to Networking – Prentice Hall (ISBN 8120313860)
3. Computer Networking First Step – Odom Wendell – (ISBN 8129706075)

4. Carl Hamacher V. Zvonko G.V. Safwat G. Z. (2002) Computer organization (5th ed.),Tata McGraw Hill
5. Morris Mano (2007) Computer System Architecture (3rd ed.), Pearson Education
6. Ramez, E. Shamkant, B. Navathe (2008) Fundamentals of database systems (5th ed.), Pearson Education
7. Date, C. J, (2012) An Introduction to Database Systems (8th ed.), Pearson Education

| Core 4 | MCYC14 / Introduction to Data Privacy | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble:** To learn online privacy techniques in modern day and also sensitive online information. Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.

**Unit-1: Privacy – Common Principles and Approaches :** Historical and social origins of privacy – information types: personal and non-personal – Elements of personal information – data subjects – personal data – personally identifiable information - sensitive personal information – processing of personal data – data controller and processor – data protection authorities – privacy by design – privacy policy and notice (14L)

**Unit-2: Privacy Lifecycle Principles and Risk Management :** Privacy drivers and challenges – Privacy lifecycle: collection, use and retention, disclosure, management and administration – move to another system or location, monitoring and enforcement - privacy impact assessment (13L)

**Unit-3: Modern Day Privacy Principles :** US Fair information practices – OECD guidelines on privacy – APEC principles of privacy – Indian laws and regulations impacting collection, storage, use and transfer / destruction of sensitive personal information – EU directive 95/46 – evolution of GDPR – Safe harbor and privacy shields (12L)

**Unit – 4: Online Privacy :** Standard web protocols impacting privacy of data stored / transmitted via web applications – threats to online privacy – web user authentication – active and passive collection of personal information on web sites – P3P: Platform for Privacy Preferences Project – Active and passive collection of privacy data – Online identification mechanisms – policies and disclaimers (11L)

**Unit-5: Sensitive Online Information :** Privacy in e-mails – commercial e-mails – spams, phishing and spear-phishing – search engine optimization – search engine marketing – online behavior marketing – social media – online seal of trust – dispute resolution of online privacy violation – self regulatory framework – privacy self determination (10L)

Total (60L)

**References:**

1. Cannon, J.C. Privacy: What Developers and IT Professional Should Know. (Addison Wesley, 2004)
2. Cranor, Lorrie Faith. I Didn't Buy it for Myself, in Clare-Marie Karat, Jan O. Blom, and John Karat (ed.), Designing Personalized User Experiences in eCommerce. Kluwer
   Academic Publishers. 2004.
3. Microsoft Corporation. Privacy Guidelines for Developing Software Products and Services (Microsoft, 2007)

4. Spiekermann, Sarah and Cranor, Lorrie Faith. Engineering Privacy. IEEE Transactions on Software Engineering. Vo. 35, No. 1, January/February, 2009, pp. 67-82.
5. Chaum, David. Security without Identification: Card Computers to make Big Brother Obsolete. Communications of the ACM, Vol. 28, No. 10, pages 1030-1044; October 1985.
6. Cranor, Lorrie S. Chowdhury, Abdur, Egelman, Serge, McDonald, Aleecia M., and Sheng, Steven. P3P Deployment on Websites. (Electronic Commerce Research and Applications, 2008)
7. Sun Microsystems, Inc., The CIO and the CPO – A Vision for Teamwork and Success. (Sun Microsystems. 2006)
8. Sun Microsystems, Inc., Engineering for Data Protection and Accountability. (Sun Microsystems. 2007).

| Lab 1 | MCYL11/ Information Security Lab | L | T | P | C |
|---|---|---|---|---|---|
| | | | | 4 | 2 |

A. **Information Security**

1. User Identity and Access Management
2. Account Authorization
3. Access and Privilege Management
4. System and Network Access Control
5. Operating Systems Access Controls
6. Monitoring Systems Access Controls
7. Intrusion Detection System
8. Event Logging

Total (45L)

| Lab 2 | MCYL12 / Networking and Database Lab | L | T | P | C |
|---|---|---|---|---|---|
| | | | | 4 | 2 |

**B. <u>Networking</u>**

1. Understanding different types of topologies eg: Bus, Star and Ring topologies.
2. Understanding Client – Server Architecture.
3. Understanding the basics of cabling.
4. Understanding Domain controller.
5. Understanding User Controller and assigning the user rights.
6. Understanding the functions of Routers, firewalls and IDS and configuring.
7. Draw the Layout of your LAB and study all the technical details of the components used to connect the systems in LAN (layer wise devices).
8. Setting up of a simple network and subnet it.
9. Analyzing Logs, routing protocols.
10. Send a request from client with a file name and read the same from the server, display it in client side.

11. Compare emails provided by yahoo, MSN, Google, Rediff and bring out the pros and cons.
12. Browse atleast 5 local inter online banking sites and bring out the mechanism used by them for secure transfer of information (include credit card transactions).
13. Read the content from an URL using Java networking facilities and explore.

Total (45L)

| Core 5 | MCYC21/Forms of Cyber Crimes | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble:** To know the various cyber attacks and crimes. Cyber crimes are criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as the use of online social networks to bully others or sending sexually explicit digital photos with a smart phone.

**Unit-1: Introduction to Cyber Crimes**

Definitions – nature and extent of cyber crimes in India and other parts of the world – sources of information on cyber crimes – interpretation of cyber crime statistics eg., data provided in "Crimes in India" – cross border nature of cyber crimes – taxonomy of cyber crimes (13L)

**Unit-2: Generic Forms of Cyber Crimes**

Hacking – cracking - denial of service – malware: viruses, worms, trojans – data diddling – salami techniques – cyber stalking – phishing and vishing – crimes in social media – spamming – abuse of or stealing of computer resources – cyber vandalism – cyber crimes on social media (10L)

**Unit-3: Vertical Specific Cyber Crimes**

Cyber frauds and crimes in BFSI, Telecom, logistics, energy credit cards vertical. Cyber attacks on military installations – cyber attacks on national critical information infrastructure – attacks on public utilities (11L)

**Unit-4: Advanced and Persistent Cyber Attacks**

Attacks on SCADA networks, ICS vulnerability exploits – compromising crypto systems – cyber terrorism and cyber warfare – violation of IP rights – attacks on military installations – cyber attacks on maritime assets (12L)

**Unit-5: Modus Operandi**

Modus operandi of common forms of cyber crimes – investigation of cyber frauds and crimes – cyber fraud triangle – profile of cyber criminal – cyber crime risk assessment – multi disciplinary approach to cyber crime management – support to cyber crime victims – insurance against oss from cyber crimes. (14L)

Total (60L)

References:

1. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats by Will Gragido, John Pirc, 1st edition, Syngress, 7 January 2011
2. Cyber Crime & Warfare: All That Matters by Peter Warren, Michael Streeter, Kindle Edition, Hodder & Stoughton, 26 July 2013
3. Digital Evidence and computer crime by Eoghan Casey, 3rd Edition, Academic Press Publication, 17 June 2011
4. The Psychology of Cyber Crime: Concepts and Principles by Grainne Kirwan, Andrew Power, 1 edition, Business Science Reference , 15 March 2012

| Core 6 | MCYC22 / Introduction to Digital Forensics | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble**: The ability to reduce or even eliminate sampling risk. Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

**Unit-1: Digital Forensic Investigation**

Evolution of investigative process of compute crimes – Terminologies and definitions used in digital forensic investigations – the investigation life cycle – digital evidence under common law systems – chain of custody – presentation in court (10L)

**Unit-2: Understanding Digital Data**

Systems of storage of data in digital format – character codes, record structure, file formats and file signatures – storage of graphic files – recognition of file formats and intern storage architecture – extraction from forensic artifacts – retrieval of deleted data (11L)

**Unit-3: Forensic Principles Applied to Digital Space**

Applying common principles of forensic science to digital space – various core principles of forensic sciences eg., principles propounded by Frye, Coppolino, Marx and Daubert – best practices in evidence gathering – best operational practices in forensic sciences ported to digital forensics (12L)

**Unit-4: Collecting digital evidence**

Identifying evidence of probative value – obstacles in collection of digital evidence – volatility of digital evidence – live vs dead forensic process – collection, storage, backup and archiving of evidence – controlling contamination – copying vs. bit mapping of data – analysis of evidence on site or at remote location – challenges due to commingled data on evidence computers (14L)

**Unit-5: Standards and best Practice Guidelines**

Handling the Digital Crime Scene - Digital Evidence Examination Guidelines – ACPO – IOCE – SWGDE – DFRWS - ISO 27037 (13L)

Total (60L)

**References:**

1. Computer Forensics, Computer Crime Investigation by John.R.Vacca, 2002, Firewall Media
2. Computer Intrusion Forensics by George Mohay et al, 2003, Artech House
3. Handbook of Digital Forensics by Eoghan Casey, 2010, Elsevier
4. NIST guidelines on digital forensic processes

| Core 7 | MCYC23 / Cyber Laws and Regulations | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble: T**o learn the Basic Technologies used in Cyber Law. A cyber security regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber attacks like viruses, worms, Trojan horses, phishing, denial of service attacks, unauthorized access and control system attacks. There are numerous measures available to prevent cyber attacks. (12L)

**Unit-1: Cyber Laws**

Indian Information Technology Act, as amended up to data - rules framed under the Act; in particular the rules relating to regulation of cyber cafes, certification authority and digital signature and other commercially significant aspects – selected comparative cyber laws in other countries

**Unit-2: Related Laws**

Indian Penal Code, Evidence Act, Bankers Book Evidence Act, Negotiable Instruments Act, Contracts Act and Reserve Bank of India Act – selected comparative laws of other countries and their use in a cyber environment (11L)

**Unit-3: Legal and Related Issues in Cyber Cases**

Process of complaint and in cyber law matters in India – cross border data flow and cross border jurisdiction – incompatibility of cyber laws of different countries – UNCITRAL model law on electronic commerce – prosecution at point of apprehension – cyber jurisprudence – decided cases in India – popular cases outside India – sentencing the cyber criminals(10L)

**Unit-4: Procedural Legal Issues**

Seizure of evidentiary data and backups - data Disclosure - Dealing with third party and confidential / privileged material - Virtual Drives, Virtual Connectivity - Emergent Issues - Civil Issues and General Enforcement - Potential defamation - Intellectual Property Infringement - Confidentiality Obligations - Internal Boardroom Disclosure and the traps - duties of Disclosure - Data Preservation and Retention (13L)

**Unit-5: Basic Technology used in Cyber Law Framework**

Cryptography – hashing – web cache handling – operating system registry – social media applications – network architecture and end user networking including DNS and DHCP – ISP protocols – WAN and LAN protocols and connectivity – wireless communication protocols – database architecture and industrial control systems (14L)

Total (60L)

**References:**

1. Cyber law by Nandan kamath, Fifth Edition, Universal law Publication, 01 Jan 2012
2. Intellectual property by Robert P Merges, 3rd Edition, Aspen Publication, 2003
3. Computers , Technology and the new internet laws by Karnika Seth, Updated Edition, Lexis nexis Publication, 01 Jan 2013
4. Legal dimensions of cyber space by S.K.Verma, Volume 1, Ashgate Publication, 01 Jan 2001

| Lab 3 | Digital Forensics Lab | L | T | P | C |
|---|---|---|---|---|---|
| | | | | 4 | 2 |

1. **The Practice of Digital Forensics -** Boot Process – Partitions - File Systems - Procedures
2. **Forensic Hardware and Software tools –** Encase - Cyber Check Suite - Email Tracer – FTK - Open Source Tools
3. **Forensic Imaging Process –Acquiring the Digital Evidence -** Cyber Check Suite – Encase – FTK - Open Source Tools.
4. **Operating System Forensics**
   1. **Windows Forensics** - Windows dates and times - Adjusting for time zone offsets - Recycle Bin and INFO records - Windows Recycle Bin - Link files - Windows folders -Recent folder - Desktop folder - My Documents folder - Send To folder - Temp folders - Favorites folder - Windows Low folders - Cookies folder - History folder - Temporary Internet files - Swap file -Hibernation file - Printing artifacts - Windows volume shadow copy - Windows event logs.
   2. Linux Forensics
   3. MAC forensics
5. Data Loss Prevention software tools and techniques
6. Report Generation and Preparation

Total (45L)

| Lab 4 | Cyber Law Case Presentations | 2 |
|---|---|---|

1. Tampering with computer source documents
2. Hacking with computer system
3. Publishing of information which in obscene in electronic form
4. Power of the controller to give directions
5. Directions of controller to a subscriber to extend facilities to decrypt information
6. Publication for fraudulent purpose

Total (45L)

| | Internship / Industrial Training | 2 |
|---|---|---|

1. Industrial Training
2. Online course

| Core 8 | MCYC31 / Advanced Digital Forensics | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble:** Advanced digital forensics techniques. Advanced digital forensics is education intended as an upgrade on basics of digital forensics. Goal is to introduce attender to advanced and more complex usage of digital forensics in real situations. (10L)

**Unit-1: Windows & Virtual machine Forensics**

Forensic Analysis of the Windows Registry – Comparison of registry in different versions of Windows client and server OS - Use of registry viewers, use of Regedit and WinHex - Analysis of complete and partial strings and streams, Understanding of User Assist - Examination of Control Set, Mounted Devices, Event Log - Extracting USB related artifacts - Understanding and examination of protected storage - Use of VMware to establish working version of suspect's machine - Overcoming product re-activation; - Networking and virtual networks within VMware. (12L)

**Unit-2: Forensic Analysis of Storage Media and Web**

Dynamic disks compared with basic disks – data storage structure and impediments to retrieving forensically relevant evidence - Spanned and striped volumes; - Forensic treatment – Developing, administering and managing a remotely hosted web site - Use of HTML browsers on ports other than 80 – C-Panel - forensic traces left on web site admin machine - Forensic traces left on hosting servers - Anti Forensic Techniques - Approaches that may be used to reduce the effectiveness of forensic methods (10L)

**Unit-3: Managing Forensic Data**

Import, export, and cloning of disk images -Working with split, compressed or encrypted images - Advanced Forensic Format (AFF) – extensible open format for forensic image data - Use of standard Unix features for data management and analysis - Tools for basic process functions, such as viewing, converting, cryptographic hashing - Open source analysis tools and their Use - Identification and acquisition of disks and partitions - Search concepts, including grep, find, and regular expression. - Using NSRL (National Software Reference Library) known-good databases for file exclusion - Analysis and Carving tools (including Coroners Toolkit, Sleuthkit). (11L)

**Unit-4: Memory Forensics**

Volatility framework - Memory acquisition -Windows Objects and Pool allocation - Process, Handles and Tokens - Process Memory internals - Hunting Malware in Process Memory - Event Logs - Registry in Memory - Kernel forensics and rootkits - Disk artifacts in memory - Event reconstruction – Timelining - Linux Memory Forensics - Linux memory acquisition - Linux OS - Process and Process Memory - Process Address space - Open File Handles - Saved Context state - Bash Memory Analysis - Networking artifacts-Network socket file descriptors - Network connections - Network interfaces -ARP cache - Kernel memory artifacts - Physical Memory maps - Virtual memory maps - Kernel debug buffer - Loaded kernel modules - File systems in memory - Mounted file systems - Listing files and directories - Extracting file

metadata -Recovering file contents Rootkits -Shell code injection - Process hollowing - Shared library injection - Rootkits - overwrites - Inline hooking - Kernel Mode Rootkits - Accessing kernel mode - Hidden kernel modules - Hidden processes - Elevating privileges - System call handler hooks - Keyboard notifiers - Network protocol structures - Net filter hooks - Inline code hooks. Mac acquisition and internals - Mac design - Memory acquisition - Mac volatility profiles – Mach – O executable format - Mac memory overview (14L)

**Unit-5: Forensics of cloud and social media**

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 - Microsoft SkyDrive Cloud Storage Forensic Analysis - Evidence Source Identification and Preservation in Microsoft SkyDrive - Preservation of evidence collected from cloud storage devices -Examination and analysis of collected data – Skype forensics – Facebook and Twitter forensics – LinkedIn forensics (13L)

Total (60L)

**References:**


1. Windows Registry analysis by Harlan Carvey, 2010
2. The Law Enforcement and Forensic Examiner's Introduction to Linux, 2008
3. Cloud Storage Forensics by Darren Quick, 2014
4. Malware Forensics Field Guide for Windows System , Camero H.Malin, Eoghan Casey, James M.Acuilina, Curtis W.Rose, Syngress, 2012


| Core 9 | MCYC32 / Advanced Information Security | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble:** To learn various application security techniques

**Unit-1: Cryptology**

Cryptography and cryptanalysis – Asymmetric and Symmetric crypto systems – evolution of crypto systems – uses and limitations of symmetric and asymmetric crypto systems – confidentiality using crypto systems – DES, 3-DES, AES and Rijndeal crypto systems – FIPS tests for crypto strength – work factor – RSA, ECC and Quantum crypto systems – TTP services in PKI, X.509 protocols for PKI infrastructure – Digital signature and digital envelopes – PKCS implementation – Digital signature applications - Key management life cycle (14L)

**Unit-2: Application Security**

SDLC concepts – Testing for security: 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. (13L)

**Unit-3: IPSec Communication Protocols**

IPSec, - 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 (12L)

**Unit-4: Common authentication protocols**

Various authentication protocols - Password Authentication Protocol (PAP) - Challenge Handshake Authentication Protocol (CHAP) - Extensible Authentication Protocols - Remote Access with RADIUS and DIAMETER - TACACS and TACACS Plus - Single Sign on – Kerberos, SEASAME – Authentication in Wireless networks (11L)

**Unit-5: 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 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 (10L)

Total (60L)

**References:**


1. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
2. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012
3. The World Beyond Digital Rights Management by Jude Umeh, 1st edition, BCS - The Chartered Institute for IT, 2009
4. Cryptography and Network Security by Dr. William Stallings, 6th Edition, Pearson Education Publication, 01 Jan 2013
5. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
6. Certified Information Systems Security Professional, Study Guide by Ed Tittel, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012

| Lab 5 | Advanced Information Security Lab | L | T | P | C |
|---|---|---|---|---|---|
| | | | | 3 | 2 |

1. Learn to install Cygwin Software on the host Operating System.
2. Perform a experiment to grab a banner with telnet and perform the task using Netcat.
3. Perform an experiment to demonstrate the use of DumpSec.
4. Perform a wireless audit of an access point / router and decrypt WEP and WPA.
5. Install IPCop on a linux system and learn all the functions available on the software
6. Implement the following Substitution & Transposition Techniques concepts: Caesar Cipher
7. Setup a honey pot and monitor the honeypot on network

Total (45L)

| Lab 6 | Advanced Digital Forensics lab | L | T | P | C |
|---|---|---|---|---|---|
| | | | | 3 | 2 |

1. Ethical hacking in mobile, system
2. Perform an experiment on Active and Passive finger printing using XProbe2 or nmap
3. Demonstrate Intrusion Detection System (IDS) using any tool such as Snort or any other Software
4. Perform an experiment for Port Scanning with nmap, superscan or any other equivalent software
5. Generate minimum 10 passwords of length 12 characters using OpenSSL command
6. Performa a experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / Wireshark / tcpdump
7. Implement the Signature Scheme - Digital Signature Standard

Total (45L)

| Core 10 | Cyber Frauds in the BFSI Sector | L | T | P | C |
|---|---|---|---|---|---|
| | | 4 | | | 4 |

**Preamble :** learning various cyber frauds in BFSI sectors

**Unit-1: Banking and Financial Services Operations :** Basic concepts of banking, insurance and financial services – deposit and loan products – ancillary services like trade finance, remittances, specialized lending like agricultural fnance, priority sector lending, etc. – types of banks: retail, corporate, investment, development, etc. – KYC (12L)

**Unit-2: Computerized CBS :** Structure of CBS – infrastructure required – parametrization – user empowerment – access to enterprise-wide information – customer access to database and records – multiple access paths like net banking, ATMs, mobile banking and branch banking – anti money laundering controls (10L)

**Unit-3: Security and Controls :** Log of user activities in the application - Logging exception events - Audit tools to analyse data for exceptions - Change management procedures - Internal data consistency checks – Controls over account related frauds and manipulations - Input & output manipulation - User rights escalation methods - Internet Banking related - Social Engineering, Phishing tactics - Some common frauds with ATMs (11L)

**Unit-4:Money Laundering Controls :** Money laundering techniques – money laundering vulnerabilities in banking products and operations – organizational and technical controls against money laundering – recognition, handling and reporting of money laundering – money laundering reporting process – post reporting process – responding to enforcement orders – customer due diligence and risk profiling (13L)

**Unit-5: Regulatory Frameworks :** Internal regulatory frameworks for best practices – Reserve Bank of India regulatory framework – Reserve Bank of India Act, Negotiable Instruments Act, Bankers Book Evidence Act, Impact of technology on implementing these legal frameworks – Basel norms – Various classes of risks under Basel norms – Operational Risk and technology risk management (14L)

Total (60L)

**References**


1. Retail Banking by Raghu Palat
2. Information System for Banks – Indian Institute of Banking & Finance
3. Core Banking Solution – Evaluation of Security & Controls by M Revathy Sriram, P K Ramanan and R Chandrasekhar

## SUPPORTIVE COURSE – I

**(Supportive Course –I shall be chosen from the list of Supportive Papers in other department)**

## SUPPORTIVE COURSE – II

**(Supportive Course –I shall be chosen from the list of Supportive Papers in other department)**

## Electives - Group A

| Elective A1 | Foundations of Cloud Computing Security | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** Learning various cloud services and deployment models

**Unit-1: Introduction to Cloud Computing:** Delivery Models – Software as a Service (SaaS) – Platform as a Service (PaaS) – Infrastructure as a service (IaaS) – Cloud types: Public, Private and Hybrid – Jericho Cloud Cube Model – Virtualization and multi-tenancy – risk assessment for cloud migration (7L)

**Unit-2: Infrastructure Security in Cloud:** Patch management – configuration management – change management – network and virtualization security – application security for SaaS, IaaS and PaaS – BC and DR planning in the cloud – Privacy concerns (11L)

**Unit-3: Policy and Compliance in Cloud Environment:** Policy framework for cloud management – contract requirements for security – service level agreements – governance model for cloud – legal and geographical location and jurisdiction – compliance requirements and reporting (8L)

**Unit-4: Cloud Data Security:** Data lifecycle – information classification and storage – retention and disposal / destruction of data stored / processed in the cloud – encrypting data on the cloud – encryption types available and choosing the right process for data on the cloud – key management – IAM architecture in the cloud context (10L)

**Unit-5: Cloud Security Architecture :**Assessing security risk in the cloud – establishing security baseline for the cloud operations – penetration testing of cloud networks – incident detection and response – security incident and event management – auditing cloud security: onsite and remote (9L)

Total (45L)

**Books:**


1. Mather, Kumaraswamy and Latif: Cloud Security and Privacy – An Enterprise Perspective on Risk and Compliance, O'Reilly
2. Kurtz and Vines: Cloud Security: A Comprehensive guide to secure cloud computing, Wiley
3. Buyya, Broberg and Goscinski: Cloud Computing – Principles and Paradigms, Wiley

| Elective A2 | Introduction to Networking | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble**: To learn the basics of Networking

**Unit 1: Introduction -** What is networking - Need for computer networks - Network Topologies - Types of networks - Hardware needed for setting up simple LAN, Wireless networks and for inter-connecting LANs and WAN -Communication media - Network topologies and access methods - IEEE 802 series standards - Wireless technology - Spread spectrum - WAP and WML - Access points - Service Set ID (SSID) - Authentication methods (OSA, SKA) - Devices used in networking – Hubs – Switches – Routers - Wireless Access Points etc - Physical connectivity between systems - Types of Cables – Ethernet - Token Ring - Optical Fibre - Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting - Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast (11L)

**Unit 2: Routing** - Fundamentals of routing - Link State Routing - Distance Vector Routing – RIP – EIGRP – OSPF - Configuring Routers - Understanding the router architecture - Assigning IP address to the routers - Configuring routing protocols (7L)

**Unit 3: Packet Switched Connection -** Types of connections – Circuit switched, Packet switched - Why packet switched is preferred - Types of protocols and need for protocols - Packet switched Protocols - TCP/ IP (10L)

**Unit 4: OSI Layers** - Interconnecting disparate systems/ networks – issues - Open Systems Interconnect - 7 layers and their functionality - **Introduction to TCP/ IP -** Origins of TCP/ IP and evolution of Internet - IP Layers Vs OSI - IP number concepts - Network address - Classes of Networks - Subnet masking - Static and dynamic IP numbers - UDP - Establishing a TCP session (Three way handshake) - Name to address translation - Domain Name System (8L)

**Unit 5: Networking to the end user -** Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - Introduction to ADS (Active Directory Service) - File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server - Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools. (9L)

Total (45L)

**Reference Books:**


1. Basic of Networking – Prentice Hall (ISBN 8120324897)
2. Introduction to Networking – Prentice Hall (ISBN 8120313860)
3. Computer Networking First Step – Odom Wendell – (ISBN 8129706075)

| Elective A3 | Email, Mobile Devices Security | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn device security Techniques.

**Unit 1: Basics of email** - How email works - The role of Mail User Agent, Mail Delivery Agent, Mail Transfer Agent, and DNS servers - An overview of various protocols (SMTP, POP, IMAP) involved in a typical email infrastructure - A brief introduction to security issues relevant to emails as well as the typical email infrastructure. (8L)

**Unit 2: Simple Mail Transfer Protocol** - SMTP model including the basic structure as well as the extension model - The SMTP terminology - SMTP procedures (session initiation, mail transaction, forwarding mail, relaying, mail gatewaying, support for mailing lists as well as aliases, termination etc) - Important SMTP commands including their sequencing as well as the corresponding replies / response codes - Commands for debugging addresses - SMTP trace information - Address resolution & mail handling - Problem detection & handling - Security considerations (7L)

**Unit 3: Focused attacks against email systems** - Common attacks against SMTP, POP3 and IMAP services - Vulnerabilities in web mail systems - Exploits targeting the supporting infrastructure - Cryptographic techniques to protect against email eavesdropping and masquerading attacks - Architectural guidelines for secure mail infrastructure - Hardening email infrastructure (9L)

**Unit 4: Spam & Phishing** - History of Spam - Harvesting email addresses - Anonymous emails - forging headers, using open relays & proxy servers, employing proxy chaining techniques, botnets - Sending Spam - Tools of trade - Historical anti-spam approaches - Language classification and statistical filtering anti-spam techniques - Anti-spam solution offerings - Definitions - What is phishing and what's not - Email security issues that aid in phishing - Role of emails in common types of phishing attacks (impersonation, forwarding and popups) - Anti-phishing solution offerings **Email Forensics** - Understanding message headers - Forging message headers and identifying forged headers - General approaches to tracking the email sender - General approaches to inspect attachments - Spam and steganography. (10L)

**Unit -5 Mobile & Wireless Devices :** Introduction – Types of Mobiles and wireless devices and their functionalities - Proliferation of Mobile and Wireless Devices - Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing - Types and Techniques of Credit Card Frauds - Security Challenges Posed by Mobile Devices - Registry Settings for Mobile Devices Authentication Service Security - Mobile phone camera and microphone hacking - On-Screen Keyboard keyloggers - : Cryptographic Security for Mobile Devices - LDAP Security for Hand-Held Mobile Computing Devices - RAS Security for Mobile Devices - Media Player Control Security - Networking API Security for Mobile Computing Applications - Attacks on Mobile/Cell Phones - Mobile Phone Theft - Mobile Viruses - Mishing, Vishing, Smishing, Hacking Bluetooth - Mobile Devices: Security Implications for Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices, Protecting Data on Lost Devices, Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing Mobile Device Security Policies,

Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures (11L)

Total (45L)

Reference Books:

1.Mobile Security and Privacy 1st Edition Advances, Challenges and Future Research Directions by Man Ho Au Raymond Choo

| Elective A4 | MOBILE AND WIRELESS SECURITY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble**

Gain in-depth knowledge on wireless and mobile network security and its relation to the new security based protocols. Apply proactive and defensive measures to counter potential threats, attacks and intrusions. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks. (8L)

**UNIT I - INTRODUCTION:** Security and Privacy for Mobile and Wireless Networks: Introduction- State of the Art- Areas for Future Research- General Recommendation for Research. Pervasive Systems: Enhancing Trust Negotiation with Privacy Support: Trust Negotiation- Weakness of Trust Negotiation- Extending Trust Negotiation to Support Privacy. (7L)

**UNIT II - MOBILE SECURITY:** Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security. (10L)

**UNIT III - SECURING WIRELESS NETWORKS:** Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, Zigbee Security, Zigbee Attacks .

**UNIT IV - ADHOC NETWORK SECURITY :** Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks (9L)

**UNIT V-RFID SECURITY :** Introduction, RFID Security and privacy, RFID chips Techniques and Protocols, RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems, Digital Signature Transponder, Combining Physics and Cryptography to Enhance Privacy in RFID Systems, Scalability Issues in Large-Scale Applications, An Efficient and Secure RFID Security Method with Ownership Transfer, Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs, User-Centric Security for RFID based Distributed Systems, Optimizing RFID protocols for Low Information Leakage, RFID: an anti-counterfeiting tool. (11L)

Total(45L)

**References**

1. Kia Makki, Peter Reiher, “Mobile and Wireless Network Security and Privacy“, Springer, ISBN 978-0-387-71057-0, 2007.
2. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, Prentice Hall, x ISBN 9788131706885, 2007.
3. NoureddineBoudriga, ”Security of Mobile Communications”, ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan , “RFID Security Techniques, Protocols and System-On-Chip Design “, ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu,” Hacking Wireless Exposed: Wireless Security Secrets & Solutions “, second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

**Electives - Group B**

| Elective B1 | Fundamentals of Blockchains and Crypto-currency | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn cryptography techniques.

**Unit-1: Introduction :** What are blockchains – Characteristics of blockchains: efficiency, transparency, Resilience, governance and trust – immediate impact on banks and financial intermediaries – concept of one-trade one-version – impact on trading floor and control practices – removing TTP concepts in financial sector – risk of attacks on data concentrations – cross border legal and jurisdiction issues (7L)

**Unit-2: Understanding Technology :** Shared, replicated and append only database – data replication across number of systems in real time – peer-to-peer network topology – cryptography driven proof of identity, authenticity and access rights management – managing conflicting data entries and conflicting blocks - proof of work – applications to crypto currencies (9L)

**Unit-3: Blockchain Architecture :** Public vs. private block chains – enforcing smooth information transfer – difficulty in changing historical records – concept of polling and majority acceptance – the creation of block cascades – concept of permission-less databases (8L)

**Unit – 4: Block Chain Applications :** Bitcoins – Ripple – NXT – Ethereum – Fraud prevention – improving corporate governance – prevent double accounting or double spend – seamless back office operations – resistance to high degree of transparency – resistance to adopting a totally new technology – common ledger applications (10L)

**Unit-5: Regulatory Framework :** Regulations over crypto currencies like Bitcoins – use on underground economy and darkweb – impact on trade with multiple countries having different degrees of freedom to use crypto currency – unregulated exchange to trade in crypto currencies – abrupt loss of value – fraud in usage (11L)

Total(45L)

**References:**

1. Crosby M, *et.al* (2015) Blockchain technology – beyond Bitcoin, Sutardja Center for Entrepreneurship and Technology, Univ of California, Berkley
2. Lewis, A (2016) A Gentle Introduction to Blockchain technology, BNC Digital Currency Insights, Bitsonblocks, Singapore

3. Swan, M (2015) Blockchain – Blueprint for a New Economy, O'Reilly, Sebastopol, CA

| Elective B2 | STORAGE MANAGEMENT & SECURITY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn the various backup and Recovery Techniques.

**Unit – I – Introduction to Storage Systems** : Storage System - Introduction to Information Storage and Management, Storage System Environment, Data Protection Raid, Intelligent Storage System. (9L)

**Unit – II – Storage Area Networking :** Storage Networking Technologies and Virtualization, Storage Networks, Network Attached Storage, IP SAN, Content Addressed Storage, Storage Virtualization. (7L)

**Unit – III - Backup and Recovery Mechanisms :** Introduction to Business Continuity, Backup and Recovery, Local Replication, Remote Replication. (8L)

**Unit – IV – Storage Security:** Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking. (10L)

**Unit – V – Storage Infrastructure Management:** Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice. (11L)

Total(45L)

**References:**

1. Information Storage and Management, "Storing, Managing, and Protecting Digital Information", Wiley; 1 edition, EMC Corporation, 2009.
2. John Chirillo, Scott Blaul, "Storage Security: Protecting SAN, NAS and DAS", Wiley Publishers, 2003.
3. David Alexander , Amanda French , David Sutton ,"Information Security Management Principles" The British Computer Society, 2008.

| Elective B3 | BIG DATA TECHNOLOGY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about Big Data and Business analytics

**Unit I** – **Introduction to Big Data: Introduction** : Distributed file system – Big Data and its importance, Four Vs, Drivers for Big data, Big data analytics, Big data applications. Algorithms using map reduce, Matrix-Vector Multiplication by Map Reduce. (10L)

**Unit II – Introduction Hadoop:** Big Data – Apache Hadoop & Hadoop EcoSystem – Moving Data in and out of Hadoop – Understanding inputs and outputs of MapReduce - Data Serialization. (9L)

**Unit- III Hadoop Architecture:** Hadoop Architecture, Hadoop Storage: HDFS, Common Hadoop Shell commands , Anatomy of File Write and Read., Name Node, Secondary Name Node, and Data Node, Hadoop Map Reduce paradigm, Map and Reduce tasks, Job, Task trackers - Cluster Setup – SSH & Hadoop Configuration – HDFS Administering –Monitoring & Maintenance. (11L)

**Unit-IV Hadoop Ecosystem and Yarn :** Hadoop ecosystem components - Schedulers - Fair and Capacity, Hadoop 2.0 New Features Name Node High Availability, HDFS Federation, MRv2, YARN, Running MRv1 in YARN. (8L)

**Unit-V HIVE AND HIVEQL, HBASE** : Hive Architecture and Installation, Comparison with Traditional Database, HiveQL - Querying Data - Sorting And Aggregating, Map Reduce Scripts, Joins & Subqueries, HBase concepts Advanced Usage, Schema Design, Advance Indexing - PIG, Zookeeper - how it helps in monitoring a cluster, HBase uses Zookeeper and how to Build Applications with Zookeeper. (7L)

Total(45L)

**References:**


1. Boris lublinsky, Kevin t. Smith, Alexey Yakubovich, “Professional Hadoop Solutions”, Wiley, ISBN: 9788126551071, 2015.
2. Chris Eaton, Dirk deroos et al., “Understanding Big data”, McGraw Hill, 2012.
3. Tom White, “HADOOP: The definitive Guide”, O Reilly 2012. 6 IT2015 SRM (E&T)
4. Vignesh Prajapati, “Big Data Analytics with R and Haoop”, Packet Publishing 2013.
5. Tom Plunkett, Brian Macdonald et al, “Oracle Big Data Handbook”, Oracle Press, 2014.
6. http://www.bigdatauniversity.com/
7. Jy Liebowitz, “Big Data and Business analytics”,CRC press, 2013.

| Elective B4 | ANDROID MOBILE APPLICATION DEVELOPMENT | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about mobile computing and android activities

**UNIT –I Introduction to Mobile Computing**

Mobile Communication Concept - generations of wireless technology – Basics concept of cell, cluster and frequency reuse - Noise effects on mobile - Understanding GSM and CDMA - Basics of GSM architecture, its services like voice call, SMS, MMS, LBS, VAS - Different modes used for Mobile Communication - Architecture of Mobile Computing(3 tier) - Design considerations for mobile computing - Mobile Communication Characteristics - Mobile communication Application - Mobile Computing Security Concerns - Middleware and Gateway needed for mobile Computing - Making Existing Application Mobile Enable - Mobile IP - Basic Mobile Computing Protocol - Mobile Communication through Satellite (Low orbit satellite, Medium orbit satellite, Geo stationary satellite, Satellite phones) (10L)

**UNIT–II Introduction to Android**

Overview of Android - What does Android run On - Internals of Android? - Android for mobile apps development - Environment setup for Android apps Development - Framework - Android - SDK, Eclipse - Emulators –What is an Emulator / Android AVD (9L)

**UNIT –III Android Activities and GUI Design Concepts**

Android Application Design criteria: Consideration for Hardware Design, Design Demands For Android application, Intent, Activity, Activity Lifecycle and Manifest - Creating Application and new Activities - Simple UI - Layouts and Layout properties : Introducing Android UI Design, Introducing Layouts - XML Introduction to GUI objects viz.: Push Button, Text / Labels , EditText, ToggleButton , Padding (8L)

**UNIT –IV Advanced UI Programming**

Event driven Programming in Android - (Text Edit, Button clicked etc.) - Activity Lifecycle of Android (7L)

**UNIT –V**

Toast, Menu, Dialog, List and Adapters Menu: Basics, Custom v/s System Menus, Create and Use Handset menu Button (Hardware) - Dialog : Creating and Altering Dialogs - Toast : List & Adapters - Demo Application Development and Application Launching - Basic operation of SQLite Database - Priorities for Android Application (11L)

Total(45L)

**Text Book:**


1. J.F.De Marzio, Android –A Programmer's Guide, Mc Graw Hill Pub, 2008.
2. Building Android Apps IN EASY STEPS McGraw - Hill Education
3. Professional Android 2 Application Development by Reto Meier, Wiley India Pvt Ltd.,2012.
4. Beginning Android by Mark L Murphy,Wiley India Pvt Ltd.,2015
5. Pro Android, by Sayed Y Hashimi and Satya Komatineni Wiley India Pvt Ltd., 2015

## Electives - Group C

| Elective C1 | Fundamentals of Research Methods and Statistical Applications | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about research methodology techniques

**Unit I - Introduction** – Meaning of research - Preamble – Motivation – research approaches - significance of research - Types of Research – Research Methods versus Methodology – Research and Scientific Method – importance of knowing how research is done - Research Process – Finding a Research Advisor/Guide - The Advisor-Advisee Relationship - Finding a Topic and Beginning Research, Getting Research Ideas (7L)

**Unit-II – Research Formulation** – Defining and formulating the research problem – Selecting the problem – Necessity of defining the problem – Importance of literature review in defining a problem – Literature review – Primary and secondary sources – reviews, treatise, monographs, patents – web as a source – searching the web- Critical literature review – Identifying gap areas from literature review – Development of working hypothesis. (8L)

**Unit-III – Research design and methods** – Research design Basic Principles-Need of research design – Features of good design – important concepts relating to research design – Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction, Development of Models. Developing a research plan – Exploration, Description, Diagnosis, and Experimentation, Determining experimental and sample designs. (9L)

**Unit-IV – Data Collection and analysis-** Execution of the research – Observation and Collection of data – Methods of data collection – Primary data – Secondary Data – Data Presentation - Mathematical Tool for Analysis – Ethics in Research – Importance – Integrity in Research Sampling Methods-Data Processing and Analysis strategies – Data Analysis with Statistical Packages – Ethics in Research - Hypothesis-testing – Scientific Misconduct and Consequences . (11L)

**Unit-V – Reporting and thesis writing** – Structure and components of scientific reports-Types of report – Technical reports and thesis – Significance – Different steps in the preparation – Layout, Structure and Language of typical reports – illustrations and tables – Bibliography, referencing and footnotes – Oral presentation – Planning – Preparation – Practice – Making presentation – Use of visual aids – Importance of effective communication-Research ethics – Ethical issues – Copy right - royalty – Intellectual property rights and patent law – Reproduction of published material – Plagiarism – Citation and acknowledgement. (10L)

Total(45L)

**References:**


1. "Engineering Research Methodology: A Computer Science and Engineering and Information and Communication Technologies Perspective", Krishnan Nallaperumal, https://www.researchgate.net/publication/259183120_Engineering_Research_Methodology_A_Computer_Science_and_Engineering_and_Information_and_Communication_Technologies_Perspective
2. Kothari, C.R, 2014. *Research Methodology*: Methods and Techniques, New age International, 3rdEdition.
3. Kavadia Gerg, Agarwal & Agarwal, 2002, Introduction to *Research Methodology*, RBSA Publishers.
4. Agarwal, B.L., 2015, Comprehensive *Research Methodology*, New age International, 1st edition.
5. Mukul Gupta, Deepa Gupta, 2011, *Research Methodology*, PHI publisher

| Elective C2 | MOBILE AND DIGITAL FORENSICS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about digital forensic techniques in mobile system.

**UNIT – I**

**INTRODUCTION TO WIRELESS TECHNOLOGIES:** Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft. (10L)

**UNIT - II**

**SECURITY FRAMEWORK FOR MOBILE SYSTEMS :** CIA triad in mobile phones- Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues. (8L)

**UNIT - III**

**MOBILE PHONE FORENSICS :** Crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques. (7L)

**UNIT - IV**

**INTRODUCTION TO DIGITAL FORENSICS :** Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination. (9L)

**UNIT - V**

**ANALYSIS OF DIGITAL FORENSIC TECHNIQUES :** Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context. (11L)

Total (45L)

**REFERENCES**


1. Gregory Kipper, “Wireless Crime and Forensic Investigation”, Auerbach Publications, 2007.
2. Iosif I. Androulidakis, “ Mobile phone security and forensics: A practical approach”, Springer publications, 2012.
3. Andrew Hoog, “Android Forensics: Investigation, Analysis and Mobile Security for Google Android”, Elsevier publications, 2011.
4. Angus M.Marshall, “ Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008.

| Elective C3 | DATA MINING AND WAREHOUSING | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about data mining and data warehousing concepts

**UNIT I**

**Data Mining** : Introduction – Information and production factor – Data mining vs query tools– Data mining in marketing – Self learning computer systems – concept learning – Data mining and Data warehouse. (9L)

**Unit II**

**Knowledge discovery process:** Data selection – Cleaning – Enrichment – Coding – Preliminary analysis of the data set using traditional query tools – Visualization techniques – OLAP tools – Decision trees – Association rules – Neural networks – Genetic Algorithms KDD (Knowledge discover in Database) environment. (10L)

**Unit III**

**Data warehouse Architecture:** System Process – Process architecture – Design – Database scheme – Partitioning strategy – Aggregations – Data mart – Meta data – Systems and data Warehouse process managers. (11L)

**Unit IV**

**Hardware and operational design of data warehouses** – Hardware architecture – Physical layout – security – Backup and recovery – Service level agreement – operating the data warehouse. (8L)

**Unit V**

Planning, Tuning and Testing: Capacity planning – Tuning the data warehouse – Testing the data warehouses – Data warehouse features. (7L)

Total (45L)

**Text Books:**


1. Pieter Adriaans, Dolf Zantinge, Data Mining, Addison Wesley 1996
2. Sam Anahory, Dennis Muray, Data Warehousing in the real world, Addison Wesley 1996
3. Sean Kelly, Data WareHousing in Action, John Wiley 1997.

| Elective C4 | BIG DATA SECURITY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about the hadoop security features.

**Unit I – Big Data Privacy, Ethics and Security Privacy :** Reidentification of Anonymous People – Why Big Data Privacy is self-regulating? – Ethics – Ownership – Ethical Guidelines – Big Data Security – Organizational Security. (9L)

**Unit II - Security, Compliance, Auditing, and Protection** : Steps to secure big data – Classifying Data – Protecting – Big Data Compliance – Intellectual Property Challenge – Research Questions in Cloud Security – Open Problems. (8L)

**Unit III – Hadoop Security Design :** Kerberos – Default Hadoop Model without security - Hadoop Kerberos Security Implementation & Configuration. (7L)

**Unit IV – Hadoop Ecosystem Security :** Configuring Kerberos for Hadoop ecosystem components – Pig, Hive, Oozie, Flume, HBase, Sqoop. (11L)

**Unit V** – **Data Security & Event Logging** : Integrating Hadoop with Enterprise Security Systems - Securing Sensitive Data in Hadoop – SIEM system – Setting up audit logging in hadoop cluster (10L)

Total (45L)

**References:**


1. Mark Van Rijmenam, “Think Bigger: Developing a Successful Big Data Strategy for Your Business”, Amazon, 1 edition, 2014.
2. Frank Ohlhorst John Wiley & Sons, “Big Data Analytics: Turning Big Data into Big Money”, John Wiley & Sons, 2013.
3. Sherif Sakr, “Large Scale and Big Data: Processing and Management”, CRC Press, 2014.
4. Sudeesh Narayanan, “Securing Hadoop”, Packt Publishing, 2013.
5. Ben Spivey, Joey Echeverria, “Hadoop Security Protecting Your Big Data Problem”, O’Reilly Media, 2015.
6. Top Tips for Securing Big Data Environments: e-book (http://www.ibmbigdatahub.com/ whitepaper/top-tips-securing-big-data- environments-ebook)
7. http://www.dataguise.com/?q=securing-hadoop-discovering-and-securing-sensitive-Datahadoop-data-stores
8. Gazzang for Hadoophttp: // www.cloudera.com/ content/cloudera/ en/ solutions/ Enterprise solutions / security-for-hadoop.html
9. eCryptfs for Hadoop https://launchpad.net/ecryptfs.
10. Project Rhino - https://github.com/intel-hadoop/project-rhino/

## Electives - Group D

| Elective D1 | Detecting and Investigating Cyber Frauds | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To learn about detecting and investigating various cyber frauds

**Unit-1: Concepts of fraud in the cyber space**

Definition of frauds – fraud relationship with opportunities and motives in cyber space – Fraud triangle – Firefly syndrome – Corruption and fraud – Distinguishing features of cyber fraud – shaming theory and impact on fraud – easy availability of cyber fraud tools and opportunities (11L)

**Unit-2: Fraud risk assessment**

Threats – Vulnerabilities – Exploit path – asset under attack – cost of committing fraud – risk of being apprehended – risk of prosecuting and sentencing – transnational nature of cyber frauds – protection under international jurisdictional disputes (10L)

**Unit-3: Fraud management**

Five myths about cyber fraud – Cyber fraudster profile – Red flags: personality of the suspect, IS Organization, IS fraud taxonomy – IS architecture driven frauds – frauds on data – policy driven frauds – CVE as a fraud management tool (8L)

**Unit-4: Fraud types**

Brute force attack – masquerading – packet replay – phishing – trojans – e-value modification – destroying AAA features – unauthorized web access – DoS and DDoS – dial-in penetration – e-mail spoofing – ID theft and alteration (7L)

**Unit-5: Data Analytics**

Data analytics as a fraud management tool – CAAT – Benford law – Lhun's algorithm – data mining and data warehousing – digital signature and artifacts – ACFE fraud prevent checklist (9L)

Total (45L)

References:


1. Managing the risk of fraud and misconduct by Richard H Girgenti, and Timothy P Hedley, first edition, Mc Graw Hill Education Publication, 09 Mar 2011
2. Detecting Accounting Fraud: Analysis and Ethics by Cecil W Jackson, 1st Edition, Pearson Education Publication, 26 Jan 2014
3. Anatomy of a fraud investigation by Stephen Pedeault, 1st Edition, John Wiley & Sons Publication, 2010
4. Telecom and Network Security: Toll Fraud and Telabuse update by Jan Wilson, 2nd Edition, Telecommunications reports International Publication, 22 April 2010

| Elective D2 | IT Governance, Risk and Compliance | L | T | P | C |
|---|---|---|---|---|---|
| | | | | | |

**Preamble:** To know the Information Security Governance Practices. Effective GRC implementation helps the organization to reduce risk and improve control effectiveness, security and compliance through an integrated and unified approach that reduces the ill effects of organizational silos and redundancies.

**Unit 1: GRC Basics :** Governance, Risk & Compliance definition, Scope and Preamble - IT Governance Metrics & Framework – BASEL – OECD – NIST – ITGI (7L)

**Unit 2: Best Practices for IT Governance :** ITIL - ISO/IEC 27001 - Control Preamble of Information and Related Technology (COBIT) - The Information Security Management Maturity Model - Capability Maturity Model – Other emerging standards (9L)

**Unit 3: Information Security Governance concepts :** 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 (8L)

**Unit 4: Information Security Governance Practices :** 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 - COSO – NIST Risk Assessment & Risk Mitigation model - Evaluation & Assessment (10L)

**Unit 5: Compliance :** Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - 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 - 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. (11L)

Total (45L)

References:


1. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby, 1st Edition, Wiley Publication, 13 April 2009
2. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition by W. KragBrotby, 2nd Edition, ISACA Publication, 01 Mar 2006
3. Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture by Fred Cohen, Large Print Edition, Fred Cohen & Assosciates Publication, 2005

4. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
5. IT Compliance and Controls: Best Practices for Implementation by James J., IV DeLuccia, Illustrated Edition, Wiley Publication, 2008
6. The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments by Craig S. Wright, Brian Freedman, Dale Liu, 1st Edition, Syngress Publication, 2008
7. Auditor's Guide to Information Systems Auditing by Richard E. Cascarino, 2nd Edition, Wiley Publication, 03 Apr 2012

| Elective D3 | Business Continuity & Disaster Recovery Management Systems | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble**: To learn Business Continuity & Disaster Recovery Management Systems. CDR professionals can help an organization and its employees achieve resiliency. Developing a strategy is a complex process that requires research and analysis, including conducting a business impact analysis (BIA) and a risk analysis, and developing BCDR plans, tests, exercises and training.

**Unit 1: Introduction**

Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR) - Terms and definitions - BCM principles - BCM lifecycle - BCM in business: Benefits and consequence - Contemporary landscape: Trends and directions (7L)

**Unit 2: Risk Management & BIA**

BCM and DR – The relationship with Risk Management - Risk Management concepts and framework - 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 (9L)

**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 (11L)

**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 (8L)

**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 (10L)

Total (45L)

**References:**


1. ISO22301 (ISO)
2. Business Continuity Planning: A Step-by-Step Guide With Planning Forms on CD-ROM by Kenneth L. Flumer, 3rd edition, Rothstein Associates Publication, 04 Oct 2004

3. A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance by Julia Graham, David Kaye and Philip Jan Rothstein, Illustrated edition, Rothstein Associates Publication, 31 Jan2006
4. Business Continuity Planning – Protecting Your Organization's Life by Ken Doughty, Illustrated edition, Taylor & Francis Publication, 2000
5. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
6. The Definitive Handbook of Business Continuity Management by Andrew Hiles, 3rd Edition, John Wiley & Sons Publication, 22 Oct 2010
7. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
8. Certified Information Systems Security Professional, Study Guide by Ed Tittel, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012

| Elective D4 | Incident Response | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | | | 3 |

**Preamble:** To collect various evidences using incident Response

**Unit 1: Incident Management** - Introduction to incident management - Incident management - ITIL – perspective - Incident management - COBIT perspective - Incident management - NIST SP 800- 61 perspectives - Stages in Incident management - Initial preparation required for incident response - Need for incident response team - CERT (Computer Emergency Response Team) - CSIRT (Computer Security Incident Response Team) - Roles and responsibilities of Incident response team - Need for User awareness for better incident response. (11L)

**Unit 2: Handling incidents** - Types of incidents and their categorization - Incident prioritization -Sources of incidents – Precursor - Indicators - End Users - Methods of identifying incidents - User reporting procedures - Incident containment eradication and recovery (7L)

**Unit 3: Collecting Digital evidence – 1** - Forensic analysis methodology - Introduction to Digital Evidence - Investigative process - Incident reconstruction - Identifying the methodology involved for carrying out attacks - Identifying the motive behind the attacks - Identifying the technology used for carrying out the attacks - Preparing evidence for courtroom - Guidelines for Digital evidence handling and examination. (11L)

**Unit 4: Collecting Digital evidence – 2** - Collecting evidence from windows system - Collecting evidence from non windows system - Collecting digital evidence from the internet - Investigating routers and network topology - Investigating servers and end user PCs (8L)

**Unit 5 Learning from incidents and Pro active incident detection** - Improving security policies after learning from an incident - Honeypots – Introduction - Types of honeypots - Tools used for setting up honeypots - Collecting evidence from honeypots - Looking out for attack signatures (9L)

Total (45L)

**Reference Books:**

1. Incident Response: Investigating computer crime by Kevin Mandia and Chris Prossie

2. Incident Response and Computer Forensics (Second Edition) by Kevin Mandia and Chris Prossie
3. Digital Evidence and Computer Crime: Forensic Science, Computer and the internet, Second Edition by Eoghan Casey
4. 4.NIST SP 800- 61 – Computer Security Incident Handling Guide
5. Honeypots – Tracking Hacker by Lance Spitzner Addison Wesley

| **Major Project** | **Dissertation and Viva Voce** | **12** |
|---|---|---|

Preamble of this course is to facilitate transfer of knowledge acquired by a student to a field of his chosen specialization for application to solving a problem. The Co-ordinator of Students' Project works from the department shall coordinate this course. Student is expected to collect and study relevant material under mentorship of a Project Supervisor, identify a suitable problem and propose methodology towards its solution. Alternately a student can explore hardware / software implementation of existing solution(s).

The student will be tested for his understanding of basic principles of the core Specializations. The internal assessment will be made by Project Supervisor. The Project Supervisor will conduct three reviews in each level of progress. On completion of the work, a thesis report should be prepared in the prescribed format and submitted to the department. The end-semester university examination, will have a thesis presentation and Viva-Voce examination conducted by a committee of one external examiner and one internal examiner appointed by the HOD/Professor/ Co-ordinator of Students' Project works.