SCHEME OF EXAMINATION

&

DETAILED SYLLABUS

FOR

POST GRADUATE DIPLOMA IN CYBER SECURITY, CYBER DISASTER AND BLOCKCHAIN TECHNOLOGY

Offered in Trimester Mode
from Academic Session 2023-24 onwards

University School of Automation and Robotics

GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY
(**NAAC A++**)
EAST DELHI CAMPUS, SURAJMAL VIHAR-110032

Programme Outcomes

1. ***Engineering Knowledge*** **(PO01):** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of cyber security problems.
2. ***Problem Analysis*** **(PO02**): Identify, formulate and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics and engineering sciences.
3. ***Design/Development of Solutions*** **(PO03):** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the e-security/network security and web security.
4. ***Modern Tool Usage*** **(PO04):** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
5. ***The Engineer and Society*** **(PO05):** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
6. ***Life-long Learning*** **(PO6):** Recognize the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change that are happening on everyday basis in the domain of security.

Course / Paper Group Codes:
BS: Basic Science
HS: Humanities, social science, management
PC: Programme Core, that is course / paper offered in the discipline of the programme as a compulsory paper.
SC: School Core, that is course / paper offered in the discipline of the school as a compulsory paper.

Definitions:
Batch: The batch of the student shall mean the year of the first-time enrolment of the students in the programme of study in the first semester. Lateral entry students admitted in the 3rd semester / 2nd year shall be designated as students admitted in the previous batch as they are admitted one year later. A student re-admitted in a programme of study in a lower / later batch shall be considered as the student of the original batch for the purpose calculation of duration of study.

Programme of study shall mean Post Graduate Diploma

Acronyms:

APC: Academic programme committee comprising all faculty of the school.
BoS : Board of Studies
AC Sub-Committee : Academic Council Sub-Committe
L: Number of Lecture hours per week
T/P: Number of Tutorial / Practical Hours per week
C: Number of credits assigned to a course / paper
COE: Controller of Examinations of the Examinations Division of the University.
SGPA/CGPA: Semester/Cumulative Grade Point Average.
NUES: No term end examination shall be held. The evaluation shall be conducted as per the scheme of examinations as described in the scheme of study.

First Trimester					
Group	**Paper Code**	**Paper**	**L**	**T/P**	**Credits**
Theory Papers					
PC	DCS 101	Fundamental of Computing	4		4
PC	DCS 103	Information Security	4	-	4
PC	DCS 105	BlockChain Technology	4	-	4
Practical / Viva Voce					
PC	DCS 151	Information Security and Fundamental of Computing Lab	-	2	1
PC	DCS 153	BlockChain Technology Lab	-	2	1
PC	DCS 155	Term Paper [NUES]	-		2
Total			**12**	**4**	**16**

Second Trimester					
Group	**Paper Code**	**Paper**	**L**	**T/P**	**Credits**
Theory Papers					
PC	DCS 202	Cyber Security	4	-	4
PC	DCS 204	Cyber Crime and Disaster Management	4	-	4
Practical / Viva Voce					
PC	DCS 252	Cyber Security Lab	-	2	1
PC	DCS 254	Cyber Crime Lab	-	2	1
PC	DCS 256	Project – 1*	-	-	6
Total			**08**	**04**	**16**

*With provision of carrying out the project in collaboration with IBM in Trimester - 3

Third Trimester					
Group	**Paper Code**	**Paper**	**L**	**T/P**	**Credits**
Theory Papers					
PC	DCS 301	Cyber Laws and Cyber Forensics	4	-	4
PC	DCS 303	Cyber Security of Critical Infrastructures	4	-	4
Practical / Viva Voce					
PC	DCS 351	Cyber Forensics Lab	-	2	1
PC	DCS 353	Project - 2	-		9
Total			**08**	**02**	**18**

DETAILED SYLLABUS FOR Ist TRIMESTER

GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY,
EAST DELHI CAMPUS,
SURAJMAL VIHAR-110092

Paper Code : DCS 101	**L**	**T/P**	**C**
Subject : Fundamental of Computing	**4**	**0**	**4**

Marking Scheme

1. Teachers Continuous Evaluation: 40 Marks
2. End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2. Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3. The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	Ability of students to apply working knowledge of computers.
CO2:	Ability of students to understand the concept of Operating System
CO3:	Ability of students to understand the concept of networks
CO4:	Ability of students to understand the concept of Open Office

Course Outcomes (CO) to Programme Outcomes (PO)
Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3

Unit 1 **[10 hours]**

Introduction : Five Component Model of a Computer, System and Application software (introduction) storage devices , primary (RAM, ROM, PROM, EPROM, cache) Memory and secondary (magnetic tape, hard disk, Compact disks) memory , peripheral devices , printers.

Unit II **[10 hours]**

Operating Systems: DOS Internal, External commands, Overview of architecture of Windows, tools and system utilities including registry, Overview of Linux architecture , File system , file and permissions , concept of user and group.

Unit III **[10 hours]**

Networking Basics : Uses of a network and Common types of networks , Network topologies and protocols , Network media and hardware , Overview of Database Management System. Basics of programming through flow chart

Unit IV **[10 hours]**

Libre / Open Office Writer : Editing and Reviewing, Drawing, Tables, Graphs, Templates
Libre / Open Office Calc : Worksheet Management , Formulas, Functions, Charts
Libre / Open Office Impress: designing powerful power-point presentation

Text Books

1. Peter Norton, Introduction to computers, Sixth Edition Tata McGraw Hill (2007).
2. Andrews Jean, A+Guide to Managing & Maintaining Your PC, Cengage Publication 6/e

Reference Books

1. Anita Goel, Computer Fundamentals, Pearson Education.
2. Joiner Associates Staff, Flowcharts: Plain & Simple: Learning & Application Guide , Oriel Inc
3. http://www.openoffice.org/why/
4. http://www.libreoffice.org/get-help/documentation/

GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY,
EAST DELHI CAMPUS,
SURAJMAL VIHAR-110092

Paper Code : DCS 103	**L**	**T/P**	**C**
Subject : Information Security	**4**	**0**	**4**

Marking Scheme

1.Teachers Continuous Evaluation: 40 Marks
2.End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2. Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3. The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	Ability of students to understand the concepts of Information Security.
CO2:	Ability of students to understand the Cryptographic Techniques.
CO3:	Ability of students to understand the Cryptographic Algorithms.
CO4:	Ability of students to understand the Cryptographic Protocols

Course Outcomes (CO) to Programme Outcomes (PO)
Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO3	2	3	3	3	3	3
CO4	3	3	3	3	3	3

UnitI **[10 hours]**

Introduction to Information Security: Introduction to Information Security, Critical Characteristics of Information, CIA Triangle, Balancing Security and Access, Security SDLC.

Unit II **[10 hours]**

Cryptography : Shift Cipher, Substitution Cipher, Vigenere Cipher, Confusion and Diffusion Introduction To Symmetric Ciphers, Stream Cipher Basics, RC4. Introduction To Block Ciphers, DES, Rijndael(AES Algorithm). Key Management, Hash Functions, Message Authentication Codes.

Unit III **[10 hours]**

Public Key Encryption and Signatures : Public Key Cryptography, One-way Functions, RSA. Diffie–Hellman Key Exchange, Digital Signature Schemes, Digital Certificates.
Provable Security: Security of Signature Algorithms, Security of Encryption Algorithms.

Unit IV **[10 hours]**

Advanced Protocols: ECC, Access Structures, General Secret Sharing, Zero-Knowledge and NP, Authentication Protocols.

Text Books

1. Smart, N. P. (2003). Cryptography: an introduction (Vol. 3). New York: McGraw-Hill.
2. Forouzan, Behrouz A., and Debdeep Mukhopadhyay. *Cryptography and network security*. Vol. 12. New York, NY, USA:: Mc Graw Hill Education (India) Private Limited, 2015.
3. Stallings, W., & Tahiliani, M. P. (2014). Cryptography and network security: principles and practice, vol. 6. editor: Pearson London.

Reference Books

1. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.

GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY,
EAST DELHI CAMPUS,
SURAJMAL VIHAR-110092

Paper Code : DCS 105	**L**	**T/P**	**C**
Subject : BlockChain Technology	**4**	**0**	**4**

Marking Scheme

1.Teachers Continuous Evaluation: 40 Marks
2.End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1.Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2.Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3.The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	To enable the students to understand the concepts of BlockChain Technology.
CO2:	To enable the students to analyse basics of e-Money and Hashing.
CO3:	To enable the students to understand the concepts of Smart Contract and Hyperledger.
CO4:	To enable the students to understand Consensus Algorithms, BLAST Algorithm.

Course Outcomes (CO) to Programme Outcomes (PO)
Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO3	2	3	3	3	3	3
CO4	3	3	3	3	3	3

Unit–1: **[10 hours]**
Definition of BlockChain. What is BlockChain. How is it used? Data Storage in the Blockchain. Applications of BlockChain; Advantages and Disadvantages of using Blockchains. Public vs. Private Blockchains.

Unit-2: **[10 hours]**
Physical and Digital Money. Notable Cryptocurrencies; Bitcoin: From Bitcoin to Ethereum; Concept of Hashing; Introduction to MD 5 and SHA Algorithm; Generation of the Hash Values using Java Cryptography

Architecture API; Fundamental Pillars of BlockChain Technology;

Unit-3: **[10 hours]**

Creating a Smart Contract; Application of Smart Contract; Smart Contract; BOSCA : BlockChain Oriented Smart Contract Agreement; Blockchain Application Development using REMIX/SOLIDITY; Design, develop and deployment of a smart contract on REMIX IDE.

Unit-4: **[10 hours]**

Consensus Algorithms; conceptualization of Proof of Work and Proof of Stake. Merkle Tree Formation; BLAST : BlockChain Algorithm for Secure Transaction.

Text Books/Online Sources:

1. IBM Smart Contract Platform
2. Lewis, Antony. The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them. Mango Media Inc., 2018.
3. Mahankali, Srinivas. Blockchain: The Untold Story: From birth of Internet to future of Blockchain. BPB Publications, 2019.

DETAILED SYLLABUS FOR 2nd TRIMESTER

GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY,
EAST DELHI CAMPUS,
SURAJMAL VIHAR-110092

Paper Code : DCS 202	L	T/P	C
Subject : Cyber Security	4	0	4

Marking Scheme

1.Teachers Continuous Evaluation: 40 Marks
2.End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1.Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2.Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3.The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	Ability of students to understand Criminal Behavior and Social Engineering.
CO2:	Ability of students to perform network mapping and vulnerability scanning
CO3:	Ability of students to distinguish between various types of firewall
CO4:	Ability of students to demonstrate the application layer security

Course Outcomes (CO) to Programme Outcomes (PO) Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO3	2	3	3	3	3	3
CO4	3	3	3	3	3	3

Unit - I **[10 hours]**

Brief history of the internet, Cyberspace and Criminal Behavior, Cyber psychology, Realms of Cyber world, Attack Vectors, Threats, Harm, Vulnerabilities, Controls,

Authentication, Access Control and Cryptography, viruses and malicious code, Social Engineering.

Unit - II **[10 hours]**

Web attack: Browser Attacks, Web Attacks Targeting Users, Obtaining User or Website Data, Scanning for web vulnerabilities tools: Nikto, W3af Network Vulnerabilities: Overview of vulnerability scanning, Open Port / Service Identification, Banner /Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit.

Unit- III **[10 hours]**

Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, How a Firewall Protects a Network, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, IDS, IPS, VPN: the basic of Virtual Private Networks. Application Inspection tools – Zed Attack Proxy, Sqlmap, DVWA, Webgoat, Password Cracking and Brute-Force Tools: John the Ripper, L0phtcrack, Pwdump, HTC-Hydra.

Unit – IV **[10 hours]**

Email security, web application security, web browser security, ecommerce security, Attack on wireless Networks, Wireless network security, Mobile device security.

Textbooks:

1. Stallings, William. *Cryptography and network security, 4/E*. Pearson Education India, 2006.

2. Stallings, William, et al. *Computer security: principles and practice*. Vol. 3. Upper Saddle River: Pearson, 2012.

	GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, EAST DELHI CAMPUS, SURAJMAL VIHAR-110092

Paper Code : DCS 204	**L**	**T/P**	**C**
Subject : Cyber Crime and Disaster Management	**4**	**0**	**4**

Marking Scheme

1.Teachers Continuous Evaluation: 40 Marks
2.End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1.Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2.Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3.The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	Ability of students to understand the concepts of Cyber-attacks and cyber security
CO2:	Ability of students to understand the Phishing and Social Frauds
CO3:	Ability of students to understand the concepts of cyber stalking and Disaster Planning.
CO4:	Ability of students to understand the concepts of Risk Analysis

Course Outcomes (CO) to Programme Outcomes (PO)
Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO3	2	3	3	3	3	3
CO4	3	3	3	3	3	3

Unit 1 **[10 hours]**

Introduction to Cyber World, Cyber Crime and Digital Fraud, Cyber-attacks and cyber security, Information warfare and cyber terrorism, Cybercrimes targeting Computer systems and Mobiles.

Unit 2 **[10 hours]**

Online scams and frauds- email scams, Phishing, Vishing, Smishing, Online payment fraud, Cyberbullying, website defacement, Cyber espionage, Cryptojacking, Darknet- illegal trades, drug trafficking, human trafficking, Social Media Scams & Frauds- impersonation, identity theft, fake news.

Unit 3 **[10 hours]**

Cyber-crime against persons - cyber grooming, child pornography, cyber stalking., Social Engineering attacks, Cyber Police stations, Crime reporting procedure, Case studies. Cyber disaster, disaster planning, Company Wide disaster planning, Business Impact analysis. Cyber security Plan- cyber security policy, cyber crisis management plan., Business continuity

Unit 4 **[10 hours]**

Threat, Vulnerability and Risk, Risk Analysis: An ongoing process, how to minimize Risk, Important of ongoing risk analysis and define incident handling procedure. Cyber security audit and compliance, National cyber security policy and strategy.

Text Books:

1. Godbole, Nina, and Sunit Belapure. "Cyber Security: Understanding Cyber Crimes." Computer forensics and legal perspectives (2015): 14.
2. Agrawal, Manish, Alex Campoe, and Eric Pierce. Information security and IT risk management. John Wiley & Sons, 2014.

GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY,
EAST DELHI CAMPUS,
SURAJMAL VIHAR-110092

Paper Code : DCS 301	**L**	**T/P**	**C**
Subject : Cyber Law and Cyber Forensics	**4**	**0**	**4**

Marking Scheme

1.Teachers Continuous Evaluation: 40 Marks
2.End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1.Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2.Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3.The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	Ability of students to understand different Acts.
CO2:	Ability of students to understand the IPR and CyberLaws
CO3:	Ability of students to understand the concepts of Cyber Forensics and Steganography
CO4:	Ability of students to understand the concepts of Mobile Forensics.

Course Outcomes (CO) to Programme Outcomes (PO)
Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO3	2	3	3	3	3	3
CO4	3	3	3	3	3	3

Unit - I **[10 hours]**

Basics of Law and Technology, Scope and Jurisprudence, defamation, privacy concerns, censorship, cyber fraud, e-commerce law, information security legal liabilities, insurance law Indian Laws, Information Technology Act 2000 and its amendments, Indian Evidence Act, Computer Security Act 1987, National Information Infrastructure Protection Act 1996, Fraud Act 1997, Children Online Protection Act 1998, Computer Fraud and Abuse Act 2001, The Role of

Electronic Evidence and the Miscellaneous Provisions of the IT Act, Legal Aspects of Electronic Records/Digital Signatures, The Rules and Regulations of Certifying Authorities in India.

Unit -II **[10 hours]**

Intellectual Property, IP Theft, Copyright, Trademark, Privacy and Censorship, Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Personal Information Protection and Electronic Documents Act (PIPEDA). Introduction to International Cyber Laws, US Cyber laws, European Union Cyber Laws. Cyber Laws and Legal and ethical aspects related to new technologies- AI/ML, IoT, Blockchain, Darknet and Social media etc.

Unit – III **[10 hours]**

Overview of Types of computer forensics i.e., Media Forensics, Network forensics (internet forensics), Machine forensic, Email forensic (e-mail tracing and investigations). Processing Crime and Incident Response: Identifying Digital evidences, collecting evidence, preparing for a search, Seizing and Storing Digital evidences, Digital Hashing, Reporting and chain of custody. Windows and DOS systems-based Investigations: File Systems, Examining File systems, Disk Encryption, Windows registry, startup tasks, Linux Boot processes and File systems, Digital signature and time stamping, cryptography, Steganography, Password encryption analyzer. [10 hours]

Unit - IV **[10 hours]**

Mobile Forensic- identification, collection and preservation of mobile evidence, social media analysis, data retrieval, Email analysis from mobile phones. Email investigation, email tracking, IP tracking, email recovery, search and seizure of computer systems, password cracking Network Forensics, SQL Injections, Port scanning and vulnerability assessment tools like *Nmap, Netscan* etc.

* Note: The teacher may use propriety/open-source/freeware tools (as per availability) to teach Unit – III and Unit - IV

Textbooks:

1. CYBER LAW - The Indian Perspective, Pawan Duggal

2. C. Altheide& H. Carvey Digital Forensics with Open-Source Tools, Syngress, 2011. ISBN: 9781597495868

3. Computer Forensics and Investigations, 2nd edition, Nelson, Phillips, Enfinger, Steuart, Cengage Learning 2008

	GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, EAST DELHI CAMPUS, SURAJMAL VIHAR-110092

Subject : Cyber Security of Critical Infrastructures	**4**	**0**	**4**

Marking Scheme

1. Teachers Continuous Evaluation: 40 Marks
2. End Term Theory Examination: 60 Marks

INSTRUCTIONS TO PAPER SETTERS: **Maximum Marks : 60**

1. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks
2. Apart from Question No. 1, rest of the paper shall consist of 4 units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks.
3. The requirement of (scientific) calculators/ log-tables/ data-tables may be specified if required

Course Outcomes:

CO1:	Ability of students to understand the Cyber Physical System and UAV
CO2:	Ability of students to understand the Hardware level Security
CO3:	Ability of students to understand the Security Threats and Vulnerabilities in Wireless Network
C04:	Ability of students to understand the Risk Assessment Software

Course Outcomes (CO) to Programme Outcomes (PO) Mapping (Scale 1: Low, 2: Medium, 3: High)

CO/PO	PO01	PO02	PO03	PO04	PO05	PO06
CO1	3	3	3	3	3	2
CO2	2	3	3	3	2	3
CO3	3	3	3	3	2	3
CO4	3	3	3	2	3	3

Unit I **[10 hours]**

Cyber Physical System : Concept, Issues and Applications. Software As a Service, Platform As a Service, Infrastructure As a Service in CPS, Security Threats and Vulnerabilities in CPS.
UAS : Security Threats and Vulnerabilities in UnManned Aerial Vehicle(UAV).

Unit II **[10 hours]**

IT Infrastructure and Network hardening: Application hardening, Operating system hardening, Server hardening, Endpoint hardening, Database hardening

Unit III **[10 hours]**

Wireless Network : Vulnerabilities and Security Issues in Wireless Network, MANET(Mobile Adhoc Network), DTN(Delay Tolerant Network)

Unit IV **[10 hours]**

Risk assessment software: Gap analysis tools, Vulnerability assessment tools, Penetration testing, Risk assessment tools, Information security policy and scoping: Information security policy, Scope of the ISMS. The ISO 27001 risk assessment: Overview of the risk assessment process.

Text Books

1. Newsome, Bruce. A practical introduction to security and risk management. Sage Publications, 2013.

2. Handbook on Securing Cyber-Physical Critical Infrastructure, Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann (Elsevier), ISBN 978-0-12-415815-3, 2012 Ed

Reference Books :

1. Newsome, Bruce. A practical introduction to security and risk management. Sage Publications, 2013.