Frameworks: COSO Framework, IT Infrastructure Library Framework, ISO 27001, COBIT 5, IT Security Controls**,** General Structure and Applications. **(12 hours)**

UNIT III

The Importance of Controls: Goal-Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Control Implementation through Security Architecture Design, **Implementing a Multitiered Governance and Control Framework in a Business :** Constructing Practical Systems of Controls, Building the Security Control System, Initial Setup and Tradeoffs. **(12 hours)**

TextBooks:

(1). "The Complete Guide to Cybersecurity Risks and Controls", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(2)."Securing an IT Organization through Governance, Risk Management, and Audit", Ken Sigler, Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(3). "A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)", Anne Kohnke, Dan Shoemaker, Ken Sigleer, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016

(4). "Cybercrimes: A Multidisciplinary Analysis", Sumit Ghosh, Elliot Turrini, Springer, 2010

Semester III

CSCH 501 : Digital Forensics

CO1 : To train the students to become digital forensics professionals who are required for the law enforcement in the case of cyber incidents.

CO2 : To give the students all possible practical scenarios for the students to perform the digital forensics tasks, with both the technological and legal aspects of the case.

CO3 : To provide the students with the adequate skills required in the form of technical writing skills for the digital forensics.

CO4 : To cultivate the habit of reporting any cyber incidents at the earliest to the law

enforcement agencies.

UNIT I

Introduction To Digital Forensics : Introduction, Evolution Of Computer Forensics, Stages Of Computer Forensics Process, Benefits Of Computer Forensics, Uses Of Computer Forensics, Objectives Of Computer Forensics, Role Of Forensics Investigator, Forensics Readiness, **Computer Forensics Investigation Process** : Introduction To Computer Crime Investigation, Assess The Situation, Acquire The Data, Analyze The Data, Report The Investigation, Digital Evidence And First Responder Procedure, Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types Of Investigation, Techniques Of Digital Forensics

(16 hours)

UNIT II

Understanding Storage Media And File System : Hard Disk Drive, Details Of Internal Structure Of Hdd, The Booting Process, File System, **Windows Forensics** : Introduction, Recovering Deleted Files And Partitions, More About Recovering Lost Files/Data, **Logs & Event Analysis And Password Cracking** : Introduction, Windows Registry, Windows Event Log File, Windows Password Storage, Application Passwords Crackers, **Network Forensics** : Introduction, Network Components And Their Forensics Importance, Osi, Forensics Information From Network, Log Analysis, Forensics Tools, **Wireless Attacks** : Introduction, 4.3wireless Fidelity (Wi-fi)(802.11), Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection Systems

(16 hours)

UNIT III

Investigating Web Attacks : Introduction, Types Of Web Attacks, Web Attack Forensics, Web Application Forensics Tools, **Investigating Email Attacks** : Introduction, Email Attacks And Crimes, Privacy In Emails, Email Forensics, Email Forensic Tools, **Mobile Device Forensics** : Introduction, Challenges In Mobile Forensics, Mobile Communication, Evidences In A Mobile Device, Mobile Forensic Process, Forensic Acquisition Tools, Investigative Reports, **Expert Witness And Cyber Regulations** : Introduction, Report Preparation, Legal Aspects Of Computing

(16 hours)

Text Books:

(1). “Digital Forensics”- Dr.Jeetendra Pande, Dr. Ajay Prasad, Uttarakhand Open University, Haldwani - 2016