GUJARAT TECHNOLOGICAL UNIVERSITY

MASTER OF BUSINESS ADMINISTRATION

Year – 2 (Semester – III) (W.E.F. Academic Year 2018-19)

Specialization: Information Technology Management
Subject Name: Cyber Security and IT Governance (CSITG)
Subject Code: 3539254

1. **Learning Outcomes:**
   - Identify and describe the major types of cybercrime.
   - Distinguish between various types of cybercrimes with respect to the motivations and methods of operation of offenders, the types of victims or targets, and the spatial, temporal, and legal domains in which they are carried out.
   - Understand the law with regards to the investigation and prosecution of cyber criminals.
   - Understand the importance of IT Governance in today's scenario

2. **Course Duration:** The course duration is of **36 sessions of 75 minutes** each

3. **Course Contents:**

Module No.	Modules with its Contents/Chapters	No. of Sessions	Marks (out of 70)
I	**Introduction to Cybercrime:** Cyber Crime: Definition and Origin of the Word, Cyber Crime and Information Security, who are Cyber Criminals, Classification of Cybercrimes, E-mail Spoofing, Spamming, Cyber Defamation, Internet Time Theft, Salami Attack, Salami technique Data Diddling, Forgery, Web Jacking, Newsgroup Spam, Industrial Spying, Hacking, Online Frauds, Pornographic Offenders, Software Piracy, Computer Sabotage Email Bombing, Computer Network Intrusions, Password Sniffing, Credit Card Frauds, Identity Theft Cyber Crime: The Legal Perspectives, Indian Perspectives, The Cyber Crime And Indian ITA 2000/2001, Hacking and Indian Laws, Global Perspective on Cyber Crime , Cyber Crime and extended Enterprise, Cyber Crime Era : Survival Mantra for Netizens	10	18
II	Cyber Offenses: How Criminals plan them, Categories of Cyber Crimes, How Criminal Plans the Attack: Active	8	17

	Attacks, Passive Attacks, Social Engineering, Classification of Social Engineering, Cyber Stalking: types of Stalkers, Cyber Cafe and Cyber Crimes, Botnets, Attack Vectors, Cyber Crime and Cloud Computing Cybercrime: Mobile and Wireless Devices, Proliferation of Mobile and Wireless devices, Trends in Mobility, Credit card Frauds in Mobile and wireless devices, Authentication Service Security, Attacks on Mobile/Cellphones, Mobile Devices: Security Implications for Organizations, Organization Security polices and Measures in Mobile Computing Era		
III	Phishing and Identity Theft: Phishing: Methods of Phishing, Phishing Techniques, Types of Phishing Scams, Phishing countermeasures, Identity theft, Types and Techniques of identity thefts and its counter measures Cybercrimes and Cybersecurity: The legal perspectives: Cybercrimes and the legal Landscape around the world, why do we need cyber laws: Challenges to Indian law and cybercrime scenario in India, Digital signatures and the Indian ITA act, Cybercrime and punishment, Cyber law Technology and students: Indian Scenario	8	17
IV	**Cyber Security**- Organizational Implications: Web Threats for Organization, Security and Privacy Implications, Social Media Marketing: Security risk for organizations, Incident handling: An Essential Component of Cyber Security, **IT Governance:** Importance, benefits, what does it cover, Performance Measurement: Why is performance measurement important, what does performance measurement cover, who are the stakeholders and what are their requirements, what should we measure, What's best practice **Implementation Roadmap:** Goals and success criteria, how to get started, who needs to be involved and what are their roles and responsibilities **Communication Strategy & Culture:** Who do we need to influence, What are the key messages, Communication best practices, Developing an influencing strategy	10	18
V	Cybercrime: Examples and Mini cases	---	(30 marks CEC)

4. Teaching Methods:

The following pedagogical tools will be used to teach this course:

- Lectures
- Case Discussions and Role Playing

- Audio-visual Material (Using CDs/Clippings/ online videos)
- Assignments and Presentations

5. Evaluation:

The evaluation of participants will be on continuous basis comprising of the following elements:

A	Continuous Evaluation Component comprising of Projects / Assignments / Quiz / Class Participation / Class test / Presentation on specific topic etc.	(Internal Assessment-50 Marks)
B	Mid-Semester examination	(Internal Assessment-30 Marks)
C	End –Semester Examination	(External Assessment-70 Marks)

6. Reference Books:

Sr. No.	Author	Name of the Book	Publisher	Year of Publication
1	Nina Godbole & Sunit Belapur	Cyber Security : Understanding Cyber Crimes , Computer Forensics and Legal Perspectives	Wiley	Latest Edition
2	National Computing Centre Limited, National Computing Centre Limited Staff	IT Governance: Developing a Successful Governance Strategy: A Best Practice Guide for Decision Makers in IT	John Wiley & Sons, Incorporated, 2005	Latest Edition
3	Prof. Dr. Marco Gercke	Understanding cybercrime: Phenomena and legal challenges Responses	ITU 2012	Latest Edition
4	Nancy R. Mead, Carol Woody	Cyber Security Engineering	Pearson	Latest Edition
5	Vivek Sood	Cyber Law Simplified	McGraw Hill	Latest Edition

Note: Wherever the standard books are not available for the topic appropriate print and online resources, journals and books published by different authors may be prescribed.

7. Online Resource:

https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf