Program	Master of Business Administration (MBA)	**Semester - 4**
Type of Course	Major	
Prerequisite		
Rationale	-	
Effective From A.Y.	2024-25	

Teaching Scheme (Contact Hours)				Examination Scheme				
Lecture	Tutorial	Lab	Credit	Theory Marks		Practical Marks		Total Marks
				T	T	P	P	
4	-	-	4	50	30	-	-	150

***SEE** - Semester End Examination, **T** - Internal Theory, **P** - Internal Practical*

Course Content

T - Teaching Hours | **W** - Weightage

Sr.	Topics	T	W
1	**Module I**	**15**	**25**
	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 **Legal Perspectives of Cyber Crime:** • Indian Perspectives • Need of Cyber Laws • The Cyber Crime and Indian IT Act 2000/2001 • Hacking and Indian Laws • Global Perspective on Cyber Crime • Cyber Crime Era: Survival Mantra for Netizens; • Cybercrime and punishment		
2	**Module II**	**15**	**25**
	Cyber Offenses: • How Criminals plan them, Categories of Cyber Crimes, How Criminal Plans the Attack: • Active 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		
3	**Module III**	**15**	**25**

Course Content

T - Teaching Hours | **W** - Weightage

Sr.	Topics	T	W
	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 **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		
4	**Module IV** **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	**15**	**25**
	Total	**60**	**100**

Suggested Distribution Of Theory Marks Using Bloom's Taxonomy

Level	Remembrance	Application	Evaluate	Create
Weightage	25	25	25	25

NOTE : This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes

At the end of this course, students will be able to:	
CO1	Identify and describe the major types of cybercrimes, their methods of operation, victims, targets, and related legal frameworks.
CO2	Analyse and evaluate the global perspective of cybercrime, including cultural differences, ethical issues, and the balance between security and privacy.
CO3	Develop and implement a framework for classifying information assets, and create an incident response plan to manage information security incidents effectively.
CO4	Demonstrate proficiency in designing, installing, configuring, documenting, and troubleshooting network and system hardware and operating systems, and communicate the importance of IT Governance in addressing cyber issues.

CO PO Mapping

CO	CO - 1	CO - 2	CO - 3	CO - 4
PO - 1	3	2	3	3
PO - 2	2	3	3	3
PO - 3	2	3	0	2
PO - 4	3	3	2	3
PO - 5	0	0	2	3

Reference Books

1.	**Cyber Security - Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (TextBook)** By Nina Godbole and Sunit Belpure | Wiley
2.	**Understanding cybercrime: Phenomena and legal challenges Responses** By Prof. Dr. Marco Gercke | ITU 2012 | Latest