SEMSETER-II

GANPAT UNIVERSITY									
FACULTY OF MANAGEMENT STUDIES									
Program	MBA		Branch/Spec.		Tech MBA (MBA Technology Management)				
Semester	II				Version	1.0.0.0			
Effective from Academic Year		2025-26			Effective for the batch Admitted in		January 2025		
Subject code	**IIA07CRE**		Subject Name		**Cybersecurity, Risk Analytics and Ethical Hacking**				
Teaching scheme					Examination scheme (Marks)				
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	4	0	0		4	Theory	60	40	100
Hours	4	0	0		4	Practical			

Objective:
To equip future business leaders with a strategic framework to manage cybersecurity as a critical business function, enabling them to lead risk-informed decisions, govern security investments, and navigate the complexities of the digital threat landscape.

Course Outcome:
CO 1: The students will be able to articulate the role of cybersecurity as a core business function and explain how governance frameworks (e.g., NIST) and regulatory requirements guide enterprise security strategy.
CO 2: The students will be able to apply financial and quantitative risk analysis concepts (e.g., ALE, ROSI) to build a business case and justify cybersecurity investments.
CO 3: The students will be able to analyze common cyber-attack methodologies and explain the strategic business value of ethical hacking techniques like penetration testing.
CO 4: The students will be able to evaluate key strategic controls for building a defensible enterprise and formulate a business-focused incident response plan to manage a cyber crisis.

Theory syllabus

Unit	Content	Hrs
1	Foundations of Cybersecurity for Business, Cybersecurity as a Business Risk, Not an IT Problem, The CIA Triad (Confidentiality, Integrity, Availability), Financial & Reputational Impact of Cyber Incidents, Corporate Security Roles (CISO, Board, Executives), Governance Frameworks (NIST, ISO 27001), Legal & Regulatory Environment (GDPR, HIPAA), Differentiating Compliance vs. Security, Crown Jewel Analysis: Identifying Critical Business Assets.	12
2	Cyber Risk Analytics & Financial Management, Cyber Risk Quantification (CRQ) vs. Qualitative Analysis, Risk Treatment Strategies (Accept, Mitigate, Transfer, Avoid), Financial Metrics: Annualized Loss Expectancy (ALE), Economics of Security: Cost-Benefit Analysis, ROSI, Building the Business Case for Security Initiatives, Cyber Insurance as a Risk Transfer Mechanism, The FAIR Model for Risk Analysis (Conceptual Overview), Communicating Risk Effectively to the Board.	12

Note: Version 1.0.0.0 (First Digit= New syllabus/Revision in Full Syllabus, Second Digit=Revision in Teaching Scheme, Third Digit=Revision in Exam Scheme, Forth Digit= Content Revision)
L=Lecture, TU=Tutorial, P= Practical/Lab., TW= Term work, DT= Direct Teaching, Lab.= Laboratory work
CE= Continuous Evaluation, SEE= Semester End Examination

3	Understanding the Adversary: Ethical Hacking for Managers, The Hacker Mindset & Attacker Motivations, The Cyber Kill Chain® Methodology, Key Attack Vectors: Phishing, Ransomware, Social Engineering, BEC, The Insider Threat: Malicious vs. Accidental, Vulnerability Management from a Business Perspective, Penetration Testing (Pen-Testing): Purpose and Value, Interpreting a Pen-Test Executive Summary, Strategic Use of Threat Intelligence.	12
4	Building a Defensible Enterprise: Strategic Controls, The Human Firewall: Security Awareness & Culture, Identity & Access Management (IAM), Core Principles: Least Privilege & Zero Trust Architecture, The Role of Multi-Factor Authentication (MFA), Third-Party & Supply Chain Risk Management, Cloud Security: The Shared Responsibility Model, Data Loss Prevention (DLP) Strategy, The Role of a Security Operations Center (SOC).	12
5	Crisis Management, Response & Future Frontiers, The Incident Response Lifecycle & Plan, Business Continuity vs. Disaster Recovery (BCDR), Managing a Cyber Crisis: PR, Legal, and Communications, Developing a Crisis Communication Playbook, Regulatory Disclosures & Reporting, Post-Incident Review: Root Cause Analysis & Lessons Learned, Future Threats: AI in Attacks, IoT Risks, Quantum Computing, Building Enterprise Cyber Resilience.	12
Practical content		
Reference Books		
1.	Frei, S., and Fire, A. The Known Unknowns: The Unsolved Mysteries of Modern Anomaly Detection. No Starch Press, 2022.	
2.	Hubbard, Douglas W., and Seiersen, Richard. How to Measure Anything in Cybersecurity Risk. Wiley, 2016.	
3.	Clinton, Larry. Cybersecurity for Business. Routledge, 2018.	
4.	Kissel, Richard (Ed.). NIST Cybersecurity Framework: A Quick Start Guide. National Institute of Standards and Technology (NIST), 2018.	
5.	Fasano, P. J. Agile CISO: A De-Stressed and Pragmatic Guide to Leading a Highly-Effective Cybersecurity Program. Independently published, 2021.	
6.	Harvard Business Review. HBR's 10 Must Reads on Managing Risk. Harvard Business Review Press, 2020.	
7.	Singer, P.W., and Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.	
8.	Krebs, Brian. Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door. Sourcebooks, 2015.	
9.	Shostack, Adam. Threat Modeling: Designing for Security. Wiley, 2014.	
10.	Oltsik, Jon. The CISO's Guide to Cloud Security. Information Systems Security Association (ISSA), 2020.	
11.	Tidy, J. Cybersecurity: The Beginner's Guide. Kogan Page, 2021.	
12.	Freund, J., and Jones, J. Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, 2014.	
13.	Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown, 2014.	

Note: Version 1.0.0.0 (First Digit= New syllabus/Revision in Full Syllabus, Second Digit=Revision in Teaching Scheme, Third Digit=Revision in Exam Scheme, Forth Digit= Content Revision)

L=Lecture, TU=Tutorial, P= Practical/Lab., TW= Term work, DT= Direct Teaching, Lab.= Laboratory work

CE= Continuous Evaluation, SEE= Semester End Examination