M.Sc.I.T. Part-II (SEM III)

S.N.	Learning Objectives	Learning Outcomes
	Technical Writing and Entrepreneurship Development	
1.	This course aims to provide conceptual understanding of developing strong foundation in general writing, including research proposal and reports.	Develop technical documents that meet the requirements with standard guidelines. Understanding the essentials and hands-on learning about effective Website Development.
2.	It covers the technological developing skills for writing Article, Blog, E-Book, Commercial web Page design, Business Listing Press Release, E-Listing and Product Description.	Write Better Quality Content Which Ranks faster at Search Engines. Build effective Social Media Pages..
3.	This course aims to provide conceptual understanding of innovation and entrepreneurship development.	Evaluate the essentials parameters of effective Social Media Pages.
4.		Understand importance of innovation and entrepreneurship.
5.		Analyze research and development projects
Cloud Application Development		
1.	To develop and deploy Microservices for cloud	Develop the Microservices for cloud and deploy them on Microsoft Azure.
2.	To understand Kubernetes and deploy applications on Azure Kubernetes Service	Build and deploy services to Azure Kubernetes service.
3	To understand DevOps for Azure	Understand and build the DevOps way.
4	To follow the DevOps practices for software development	Thoroughly build the applications in the DevOps way.
5	To build APIs for Azure and AWS	Build the APIs for Microsoft Azure and AWS.
Security Breaches and Countermeasures		

1.	To get the insight of the security loopholes in every aspect of computing.	The student should be able to identify the different security breaches that can occur. The student should be able to evaluate the security of an organization and identify the loopholes. The student should be able to perform enumeration and network scanning.
2.	To understand the threats and different types of attacks that can be launched on computing systems.	The student should be able to identify the vulnerability in the systems, breach the security of the system, identify the threats due to malware and sniff the network. The student should be able to do the penetration testing to check the vulnerability of the system towards malware and network sniffing.
3	To know the countermeasures that can be taken to prevent attacks on computing systems.	The student should be able to perform social engineering and educate people to be careful from attacks due to social engineering, understand and launch DoS and DDoS attacks, hijack and active session and evade IDS and Firewalls. This should help the students to make the organization understand the threats in their systems and build robust systems.
4	To test the software against the attacks.	The student should be able to identify the vulnerabilities in the Web Servers, Web Applications, perform SQL injection and get into the wireless networks. The student should be able to help the organization aware about these vulnerabilities in their systems.
5		The student should be able to identify the vulnerabilities in the newer technologies like mobiles, IoT and cloud computing. The student should be able to use different methods of cryptography.
Cloud Management		
1	To Understand the Fundamental Ideas Behind Cloud Computing, The Evolution Of The Paradigm, Its Applicability; Benefits, As Well As Current And Future Challenges;	Understand the concepts of VMM, SDN, NAS , HyperV etc.
2	The Basic ideas And Principles In Data Center Design; Cloud Management Techniques And Cloud Software	Understand and demonstrate the use of Service manager with various deployments that can be performed

	Deployment Considerations;	using it.
3	Different CPU, Memory And I/O Virtualization Techniques That Serve In Offering Software, Computation	Understand SCCM and Demonstrate the use of Configuration Manager
4	And Storage Services On The Cloud; Software Defined Networks (SDN) And Software Defined Storage (SDS);	Understand automation with runbooks and demonstrate the use of Windows Orchestrator
5	Cloud Storage Technologies And Relevant Distributed File Systems, Nosql Databases And Object Storage;	Understand and demonstrate the use of Data Protection Manager
6	The Variety Of Programming Models And Develop Working Experience In Several Of Them.	
Malware Analysis		
1	Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques.	Understand various introductory techniques of malware analysis and creating the testing environment
2	Have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.	Perform advanced dynamic analysis and recognize constructs in assembly code.
3	Extract investigative leads from host and network-based indicators associated with a malicious program.	Perform Reverse Engineering using OLLYDBG and WINDBG and study the behaviours and functions of malware
4	Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples	Understand data encoding, various techniques for anti-disassembly and anti-debugging
5	Achieve proficiency with industry standard tools including IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon etc.	Understand various anti virtual machine techniques and perform shellcode analysis of various languages along with x64 architecture.
Data Centre Technologies		
1	Identify important requirements to design and support a data center.	Understand basic concepts in Virtualization.
2	Determine a data center environment's requirement including systems and network architecture as well as services.	Understand concepts of Load Balancing and Aggregation /virtual switching
3	Evaluate options for server farms, network designs, high availability, load balancing, data center services, and trends that might affect data center designs.	Understand Data center Migration and Fabric Building
4	Assess threats, vulnerabilities and common attacks, and network security devices available to protect data centers.	Understand various Changes in Server Architecture
5	Design a data center infrastructure	

	integrating features that address security, performance, and availability.	
6	Measure data center traffic patterns and performance metrics.	Understand the concepts of Cloud computing and how to move towards a cloud computing technology.
Offensive Security		
1	Understanding of security requirements within an organization	Understand basic security issues in cloud, IoT etc.
2	How to inspect, protect assets from technical and managerial perspectives	Understand different security techniques and policies
3	To Learn various offensive strategies to penetrate the organizations security.	Use Vulnerability assessment and exploitation tool
4	To learn various tools that aid in offensive security testing.	Analyze the network perform reconnaissance and enumerate the target to detect vulnerabilities
		Perform offensive tests using Metasploit on various application, generating payloads etc.

M.Sc.I.T. Part-II (SEM IV)

S.N.	Learning Objectives	Learning Outcomes
	Blockchain	
1.	To provide conceptual understanding of the function of Blockchain as a method of securing distributed ledgers, how consensus on their contents is achieved, and the new applications that they enable.	The students would understand the structure of a blockchain and why/when it is better than a simple distributed database.
2.	To cover the technological underpinnings of blockchain operations as distributed data structures and decision-making systems, their functionality and different architecture types.	Analyze the incentive structure in a blockchain based system and critically assess its functions, benefits and vulnerabilities
3.	To provide a critical evaluation of existing "smart contract" capabilities and platforms, and examine their future directions, opportunities, risks and challenges.	Evaluate the setting where a blockchain based structure may be applied, its potential and its limitations

4.		Understand what constitutes a "smart" contract, what are its legal implications and what it can and cannot do, now and in the near future
5.		Develop blockchain DApps.
Advanced IoT		
1.	To understand the latest developments in IoT	Build smart IoT applications on Azure.
2.	To build smart IoT applications	Use Microsoft cognitive APIs to build IoT applications.
3	To leverage the applications of IoT in different technologies	Implement Blockchain in IoT.
4	To build own IoT platform	Install and use microservices in IoT.
5		Build own IoT platform and use it in a customised way.
Cyber Forensics		
1.	Explain laws relevant to computer forensics	Investigate the cyber forensics with standard operating procedures.
2.	Seize digital evidence from pc systems	Recover the data from the hard disk with legal procedure.
3	Recover data to be used as evidence	To recover and analyse the data using forensics tool
4	Analyse data and reconstruct events	Acquire the knowledge of network analysis and use it for analysing the internet attacks.
5	Explain how data may be concealed or hidden	Able to investigate internet frauds done through various gadgets like mobile, laptops, tablets and become a forensic investigator.
Server Virtualization on VMWare Platform		
1	Identify the need for Server Virtualization	Understand VMWare VSphere 67, Install ESXi and Configure VSphere Centre
2	Describe the components and features of vSphere 6.7 and ESXi	Demonstrate the use of VSphere Update Manager and Create a VSphere Network
3	Describe how VMware's products help solve business and technical challenges with	Understand VSphere Security, Create and configure storage devices and

	regard to Server Virtualization	Perform configurations to ensure business continuity
4		Demonstrate Resource allocation, Creating and managing virtual machine and the use of templates
5		Understand automation of vSphere and manage resource allocation
Security Operations Centre		
1	The SOC (Security Operations Centre) allows an organization to enforce and test its security policies, processes, procedures and activities through one central platform that monitors and evaluates the effectiveness of the individual elements and the overall security system of the organization.	Understanding basics of SOC, Cryptography and managing and deploying VPNs.
2	This will also allow the learners to configure various use cases and detect various attacks across the network and report them in real time and also take appropriate actions.	Analyse Windows and Linux based logs along with logs generated by endpoints.
3	This course will cover the design, deployment and operation of the SOC.	Understand and analyze various forms of intrusions, threats and perform forensic analysis on them.
4	Once this course is completed, students will have the skills to perform your SOC responsibilities effectively.	Understand the incident response process and handle incidents by adhering to compliance policies and standards set by the organization.
5		Understand the various types of attacks and vulnerabilities, categorize events and perform incident analysis.
Information Security Auditing		
1	Understand various information security policies in place.	Understand various information security policies and process flow, Ethics of an Information security Auditor.
2	Assess an organization based on the needs and suggest the requisite information security policies to be deployed.	Understand various information systems in an organization, their criticality and various governance and management policies associated with them.
3	Audit the organization across relevant policies and assist the organization in implementing such policies along with suggesting improvements.	Critically analyse various operational strategies like asset management, data governance etc. and suggest requisite changes as per organizations requirements with improvements.
4		Understand the information flow across the organization and identify the weak spots, and also suggest improvements to

		strengthen them.
5		Come up with strong strategies to protect information assets and come up with an efficient business continuity plan, disaster recovery strategy etc.
Storage as a Service		
1	Understand the need for Storage Area Network and Data protection to satisfy the information explosion requirements.	Understand different techniques of storage and RAID Technologies
2	Study storage technologies: SAN, NAS, IP storage etc., which will bridge the gap between the emerging trends in industry and academics.	Understand different intelligent storage technologies. Also, understand the benefits of Fibre Channel Storage Networks along with iSCSI.
3	To get an insight of Storage area network architecture, protocols and its infrastructure.	Understand the architecture of NAS and deployment along with Object based and unified storage technologies. Also, the learner will be able to configure the storage devices to maintain highest level of availability
4	To study and discuss the applications of SAN to fulfill the needs of the storage management in the heterogeneous environment.	Understand Replication and Migration techniques and implement them.
5	Study and understand the management of Storage Networks To understand different techniques of managing store.	Understand Different techniques for managing and securing storage infrastructure.