Course Code CSD4008	Cyber Security Framework	Course Type LT	Credits 3

Course Objectives:

- To provide knowledge of various cyber security frameworks
- To provide knowledge of best practices of risk management to improve security.

Course Outcomes:

At the completion of this course, students should be able to do the following:

- Basics of cyber security framework.
- The Framework core for cyber security activities.
- The framework tier approaches for the implementation principles and practices for risk management to improve the security.

Student Outcomes (SO): b, c, i, k, l

b. An ability to analyze a problem, identify and define the computing requirements appropriate to its solution.

c. An ability to design, implement and evaluate a system / computer-based system, process, component or program to meet desired needs

i. Design and conduct experiment as well as analyze and interpret data.

k. An ability to use current techniques, skills and tools necessary for computing engineering practice.

l. An ability to apply mathematical foundations, algorithmic principles and computer science theory in the modeling and design of computer-based systems (CS)

Unit No	Unit Content	No. of hours	SOs
1	**Basic Fundamentals** Introduction: Types of Cyber Security Framework, Components of Framework, functions of Cyber Security Framework.	08	b,c,i
2	**The Framework Core** Introduction, cyber security activities, outcomes, informative references that are common across critical infrastructure sectors	10	c,i
3	**Framework Profile** Method to Implement organizational Profiles, alignment of cyber security activities with its business requirements, risk tolerances, and resources.	09	c,i
4	**Framework Implementation Tier**	08	c,i

	Mechanism for organizations to view, the characteristics of Cyber Security Risk, Approaches to manage Cyber security risk.		
5	**Principle and Practices** Principles and best practices of risk management to improve the security, organization and structure to today's multiple approaches to cyber security, Implementation of Cyber Security Framework in real time problem.	**08**	**c,i,k,l**
6	**Guest Lecture on Contemporary Topics**	**02**	
	Total Hours:	**45**	

Mode of Teaching and Learning: *Flipped Class Room, Activity Based Teaching/Learning, Digital/Computer based models, wherever possible to augment lecture for practice/tutorial and minimum 2 hours lectures by industry experts on contemporary topics*

Mode of Evaluation and assessment:
The assessment and evaluation components may consist of unannounced open book examinations, quizzes, student's portfolio generation and assessment, and any other innovative assessment practices followed by faculty, in addition to the Continuous Assessment Tests and Final Examinations.

Text Books:

1.	Data Science For Cyber-security: 3 (Security Science and Technology) by Niall M Adams, Nicholas A Heard, Patrick Rubin-delanchy
2.	Cyber Security: An Introduction for Non-Technical Managers Hardcover –by Jeremy Swinfen Green

Reference Books:

1.	Mastering Your Introduction to Cyber Security Paperback – by Dr Michael C Redmond Phd
2.	Cyber Security: A practitioner's guide Paperback – by David Sutton
3.	
4.	

Recommendation by the Board of Studies on	
Approval by Academic council on	
Compiled by	