RV Educational Institutions ®
RV College of Engineering ®

Autonomous Institution Affiliated to Visvesvaraya Technological University, Belagavi

Approved by AICTE, New Delhi

Go, change the world

SCHEME & SYLLABUS

COMPUTER SCIENCE AND

BACHELOR OF ENGINEERING (B.E.)

2022 SCHEME

Leadership in Quality Technical Education, Interdisciplinary Research & Innovation, with a Focus on Sustainable and Inclusive Technology

MISSION

1. To deliver outcome based Quality education, emphasizing on experiential learning with the state of the art infrastructure.
2. To create a conducive environment for interdisciplinary research and innovation.
3. To develop professionals through holistic education focusing on individual growth, discipline, integrity, ethics and social sensitivity.
4. To nurture industry-institution collaboration leading to competency enhancement and entrepreneurship.
5. To focus on technologies that are sustainable and inclusive, benefiting all sections of the society.

QUALITY POLICY

Achieving Excellence in Technical Education, Research and Consulting through an Outcome Based Curriculum focusing on Continuous Improvement and Innovation by Benchmarking against the global Best Practices.

CORE VALUES

Professionalism, Commitment, Integrity, Team Work, Innovation

DEPARTMENT VISION

To achieve leadership in the field of Computer Science& Engineering by strengthening fundamentalsand facilitating interdisciplinary sustainable research to meet the ever growing needs of the society.

DEPARTMENT MISSION

- To evolve continually as a centre of excellence in quality education in computers and allied fields.
- To develop state-of-the-art infrastructure and create environment capable for interdisciplinary research and skill enhancement.
- To collaborate with industries and institutions at national and international levels to enhance research in emerging areas.
- To develop professionals having social concern to become leaders in top-notch industries and/or become entrepreneurs with good ethics.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

Computer Science &Engineering (Cyber Security)

PEO1: Develop Graduates capable of applying the principles of mathematics, science, core engineering and Computer Science to solve real-world problems in interdisciplinary domains.

PEO2: To develop the ability among graduates to analyze and understand current pedagogical techniques, industry accepted computing practices and state-of-art technology.

PEO3: To develop graduates who will exhibit cultural awareness, teamwork with professional ethics, effective communication skills and appropriately apply knowledge of societal impacts of computing technology.

PEO4: To prepare graduates with a capability to successfully get employed in the right role /become entrepreneurs to achieve higher career goals or takeup higher education in pursuit of lifelong learning.

PROGRAM SPECIFIC OUTCOMES (PSOs)

PSO	Description
PSO1	**System Analysis and Design** The student will be able to: 1. Recognize and appreciate the need of change in computer architecture, data organization and analytical methods in the evolving technology. 2. Learn the applicability of various systems software elements for solving design problems. 3. Identify the various analysis & design methodologies for facilitating development of high quality system software products with focus on performance optimization. 4. Display team participation, good communication, project management and document skills.
PSO2	**Product Development** The student will be able to: 1. Demonstrate the use of knowledge and ability to write programs and integrate them with the hardware/software products in the domains of embedded systems, databases/data analytics, network/web systems and mobile products. 2. Participate in planning and implement solutions to cater to business – specific requirements displaying team dynamics and professional ethics. 3. Employ state-of-art methodologies for product development and testing / validation with focus on optimization and quality related aspects.

Lead Society: Institute of Electrical and Electronics Engineers (IEEE)

ABBREVIATIONS

Sl. No.	Abbreviation	Meaning
1.	VTU	Visvesvaraya Technological University
2.	BS	Basic Sciences
3.	CIE	Continuous Internal Evaluation
4.	SEE	Semester End Examination
5.	PE	Professional Core Elective
6.	GE	Global Elective
7.	HSS	Humanities and Social Sciences
8.	PY	Physics
9.	CY	Chemistry
10.	MA	Mathematics
11.	AS	Aerospace Engineering
12.	AI & ML	Artificial Intelligence & Machine Learning
13.	BT	Biotechnology
14.	CH	Chemical Engineering
15.	CS	Computer Science & Engineering
16.	CV	Civil Engineering
17.	EC	Electronics & Communication Engineering
18.	EE	Electrical & Electronics Engineering
19.	EI	Electronics & Instrumentation Engineering
20.	ET	Electronics & Telecommunication Engineering
21.	IM	Industrial Engineering & Management
22.	IS	Information Science & Engineering
23.	ME	Mechanical Engineering

INDEX

V SEMESTER								
Sl. No.	**Course Code**	**Course Title**	**Credit Allocation**				**BoS**	**Category**
			L	**T**	**P**	**Total**		
1		HSS Board course	3	0	0	3	HSS	Theory
2	CY Board	Database Management Systems (Common to CS, CY, CD & **IS**)	3	0	1	4	CD	Theory + Lab
3	IS Board	Artificial Intelligence and Machine Learning (Common to CS, CY, CD & **IS**)	3	0	1	4	CS	Theory + Lab
4		Theory of Computation (Common to **CS,** CY & IS)	3	1	0	4	CS	Theory
5		Professional Core Elective-I **(Group-B)**	3	0	0	3	CS	Theory
6		Professional Core Elective-II **(Group C)**	2	0	0	2	CS	**NPTEL**
		Total				**20**		

GROUP-B		
Sl. No.	**Course Code**	**Course Title**
1		Network Programming and Security
2		Computer Vision in surveillance and security
3		IoT Security
4		Vulnerability Assessment & Penetration Testing

Semester: V						
IoT Security **Category: PROFESSIONAL CORE COURSE ELECTIVE-I** **(Group-B)** **(Theory and Lab)**						
Course Code	**:**			**CIE**	**:**	**100 Marks**
Credits: L:T:P	**:**	**3:0:0**		**SEE**	**:**	**100 Marks**
Total Hours	**:**	**45L**		**SEE Duration**	**:**	**3 Hours**

Unit-I	**09 Hrs**
IoT Introduction: Defining the IoT, Why cross-industry collaboration is vital, IoT uses today, The IoT in the enterprise, The IoT of the future and the need to secure. **Vulnerabilities, Attacks, and Countermeasures:** Primer on threats, vulnerability, and risks (TVR), Primer on attacks and countermeasures, Today's IoT attacks, Lessons learned and systematic approaches.	
Unit – II	**09 Hrs**
Security Engineering for IoT Development: Building security in to design and development, Secure design, Technology selection – security products and services. **The IoT Security Lifecycle:** The secure IoT system implementation lifecycle, Operations and maintenance, Dispose.	
Unit –III	**09 Hrs**
Cryptographic Fundamentals for IoT Security Engineering: Cryptography and its role in securing the IoT, Cryptographic module principles, Cryptographic key management fundamentals, Examining cryptographic controls for IoT protocols. **Identity and Access Management Solutions for the IoT:** An introduction to identity and access management for the IoT, The identity lifecycle, Authentication credentials, IoT IAM infrastructure, Authorization and access control.	
Unit –IV	**09 Hrs**
Mitigating IoT Privacy Concerns: Privacy challenges introduced by the IoT, Guide to performing an IoT Privacy Impact Assessment, Privacy by Design principles, Privacy engineering recommendations.	

Setting Up a Compliance Monitoring Program for the IoT: IoT compliance, A complex compliance environment, Examining existing compliance standards support for the IoT		
	Unit –V	**09 Hrs**
Cloud Security for the IoT: Cloud services and the IoT, Exploring cloud service provider IoT offerings, Cloud IoT security controls, Tailoring an enterprise IoT cloud security architecture. **IoT Incident Response:** Threats both to safety and security, Planning and executing an IoT incident response, Incident response planning. IoT incident response team composition, Detection and analysis, Containment, eradication, and recovery, Post-incident activities		

Course Outcomes: After completing the course, the students will be able to: -	
CO 1	Understand and describe the basic concepts, principles, and security requirements in IoT.
CO 2	Identify and describe the variety of IoT systems architectures, essential components, and challenges specific to IoT security systems
CO 3	Apply appropriate security mechanisms for IoT to real-world problems
CO 4	Reflect on the impact of current and future IoT technologies on security and privacy
CO 5	Discuss appropriate security and privacy solutions for real-world applications,

Reference Books	
1	Brian Russell, Drew Van Duren, “Practical Internet of Things Security”, Packt Publishing Ltd, ISBN 978-1-78588-963-9, First published: June 2016
2	Fei HU, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations”, CRC Press,2016
3	The Internet of Things Enabling Technologies, Platforms, and Use Cases by Pethuru Raj, Anupama C. Raman, CRC Press Taylor & Francis Group , 2017, ISBN: 978-1-4987-6128-4

RUBRIC FOR THE CONTINUOUS INTERNAL EVALUATION (THEORY)		
#	**COMPONENTS**	**MARKS**

1.	**QUIZZES:** Quizzes will be conducted in online/offline mode. **TWO QUIZZES** will be conducted & Each Quiz will be evaluated for 10 Marks adding up to 20 Marks. **THE SUM OF TWO QUIZZES WILL BE CONSIDERED AS FINAL QUIZ MARKS.**	**20**
2.	**TESTS:** Students will be evaluated in test consisting of descriptive questions with different complexity levels (Revised Bloom's Taxonomy Levels: Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating). **TWO TESTS** will be conducted. Each test will be evaluated for 50 Marks, adding up to 100 Marks. **FINAL TEST MARKS WILL BE REDUCED TO 40 MARKS.**	**40**
3.	**EXPERIENTIAL LEARNING:** Students will be evaluated for their creativity and practical implementation of the problem. **Phase I (20) & Phase II (20)ADDING UPTO 40 MARKS**.	**40**
	MAXIMUM MARKS FOR THE CIE THEORY	**100**

RUBRIC FOR SEMESTER END EXAMINATION (THEORY)

Q. NO.	CONTENTS	MARKS
	PART A	
1	Objective type questions covering entire syllabus	20
	PART B (Maximum of TWO Sub-divisions only)	
2	Unit 1 : (Compulsory)	16
3 & 4	Unit 2 : Question 3 or 4	16
5 & 6	Unit 3 : Question 5 or 6	16
7 & 8	Unit 4 : Question 7 or 8	16
9 & 10	Unit 5: Question 9 or 10	16
	TOTAL	**100**

Semester: V						
Vulnerability Assessment & Penetration Testing **Category: PROFESSIONAL CORE COURSE ELECTIVE-I** **(Group-B)** **(Theory)**						
Course Code	**:**			**CIE**	**:**	**100 Marks**
Credits: L:T:P	**:**	**3:0:0**		**SEE**	**:**	**100 Marks**
Total Hours	**:**	**45L**		**SEE Duration**	**:**	**3 Hours**

Unit-I	**09 Hrs**
Introduction to Vulnerability Assessment & Penetration Testing: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.	
Unit – II	**09 Hrs**
Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Clients Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.	
Unit –III	**09 Hrs**
Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista 7 and Server2008), By passing Windows Memory Protections.	
Unit –IV	**09 Hrs**
Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.	
Unit –V	**09 Hrs**
Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client- side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting your self from clients side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.	

Course Outcomes: After completing the course, the students will be able to: -	
CO 1	Recognize and categorize different types of vulnerabilities across software, networks, and human factors.
CO 2	Demonstrate adeptness in employing various penetration testing methodologies and techniques.
CO 3	Evaluate the risk associated with identified vulnerabilities, considering severity, exploitability, and potential impact.
CO 4	Follow a systematic approach encompassing reconnaissance, scanning, exploitation, and post-exploitation phases.
CO 5	Generate detailed reports outlining discovered vulnerabilities, their severity levels, and actionable mitigation recommendations.

Reference Books	
1.	"Gray Hat Hacking: The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom ,3rd Edition, Tata McGraw-Hill. ISBN-10- 9390385296, 2020
2.	"The Web Application Hacker's Handbook, Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 2nd Edition, Wiley Publishing, ISBN-13- 978-1118026472, 2011
3.	"Penetration Testing: Hands on Introduction to Hacking", Georgia Weidman, 1stEdition, No Starch Press, ISBN-10 : 1593275641, 2020.
4.	"The Pen Tester Blueprint Starting a Career as an Ethical Hacker", L. Wylie, Kim Crawly, 1stEdition, Wiley Publications, ISBN-13- 978-1119684305, 2020

RUBRIC FOR THE CONTINUOUS INTERNAL EVALUATION (THEORY)		
#	**COMPONENTS**	**MARKS**
1.	**QUIZZES:** Quizzes will be conducted in online/offline mode. **TWO QUIZZES** will be conducted & Each Quiz will be evaluated for 10 Marks adding up to 20 Marks. **THE SUM OF TWO QUIZZES WILL BE CONSIDERED AS FINAL QUIZ MARKS.**	**20**

2.	**TESTS:** Students will be evaluated in test consisting of descriptive questions with different complexity levels (Revised Bloom's Taxonomy Levels: Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating). **TWO TESTS** will be conducted. Each test will be evaluated for 50 Marks, adding up to 100 Marks. **FINAL TEST MARKS WILL BE REDUCED TO 40 MARKS.**	**40**
3.	**EXPERIENTIAL LEARNING:** Students will be evaluated for their creativity and practical implementation of the problem. **Phase I (20) & Phase II (20)ADDING UPTO 40 MARKS**.	**40**
	MAXIMUM MARKS FOR THE CIE THEORY	**100**

RUBRIC FOR SEMESTER END EXAMINATION (THEORY)

Q. NO.	CONTENTS	MARKS
	PART A	
1	Objective type questions covering entire syllabus	20
	PART B (Maximum of TWO Sub-divisions only)	
2	Unit 1 : (Compulsory)	16
3 & 4	Unit 2 : Question 3 or 4	16
5 & 6	Unit 3 : Question 5 or 6	16
7 & 8	Unit 4 : Question 7 or 8	16
9 & 10	Unit 5: Question 9 or 10	16
	TOTAL	**100**

Semester: VI						
Computer Vision in surveillance and security **Category: PROFESSIONAL CORE ELECTIVE-III** **(Group-D)** **(Theory)**						
Course Code	**:**			**CIE**	**:**	**100**
Credits: L:T:P	**:**	**3:0:0**		**SEE**	**:**	**100**
Total Hours	**:**	**45L**		**SEE Duration**	**:**	**3**

Unit-I	**09 Hrs**
Introduction to Digital Image Fundamentals: What is Digital Image Processing? The origin of Digital Image processing, Fundamental Steps in Digital Image Processing, Components of an Image Processing System, Image Sampling and Quantization, Some Basic Relationships between Pixels. **Histogram Processing**: Histogram Equalization, Histogram Matching (Specification Local Histogram Processing. Fundamentals Of Spatial Filtering the Mechanics of Linear Spatial Filtering, Spatial Correlation and Convolution, Separable Filter Kernels.	
Unit – II	**09 Hrs**
Image Segmentation: Fundamentals, Thresholding: The Basics of Intensity Thresholding, The Role of Noise in Image Thresholding, The Role of Illumination and Reflectance in Image Thresholding. Basic Global Thresholding Optimum Global Thresholding Using Otsu's Method Segmentation by Region Growing and By Region Splitting And Merging Region Growing Region Splitting and Merging.	
Unit –III	**09 Hrs**
Region Segmentation Using Clustering and Super pixels: Region Segmentation Using K-Means Clustering, Region Segmentation Using Superpixels, Slic Superpixel Algorithm. **Object Recognition:** Image Pattern Classification: Priori by A Human Designer, Patterns And Pattern Classes, Pattern Vectors, Structural Patterns, Pattern Classification By Prototype Matching Minimum-Distance Classifier Using Correlation For 2-D Prototype Matching Sift Feature Matching Structural Prototypes	
Unit –IV	**09 Hrs**
Information Hiding, Steganography, and Watermarking: History of Watermarking, History of Steganography, Importance of Digital Watermarking, Importance of Steganography.	

Models of Watermarking: Notation, Communications, Components of Communications Systems, Classes of Transmission Channels, Secure Transmission, Communication-Based Models of Watermarking, Basic Model, Watermarking as Communications with Side Information at the Transmitter, Watermarking as Multiplexed Communications, Geometric Models of Watermarking, Distributions and Regions in Media Space, Marking Spaces

Unit –V	**09 Hrs**
Steganography: Steganographic Communication, The Channel, The Building Blocks, Notation and Terminology, Information-Theoretic Foundations of Steganography, Cachin's Definition of Steganographic Security, Practical Steganographic Methods, Statistics Preserving Steganography, Model-Based Steganography, Masking Embedding as Natural Processing, Minimizing the Embedding Impact, Matrix Embedding, Nonshared Selection Rule	

Course Outcomes: After completing the course, the students will be able to: -	
CO 1	Exploring the basic concepts in image acquisition, pre-processing and post processing operations and fundamentals of Computer Vision.
CO 2	Analyze the difficulties of the pattern recognition problems which include classification techniques, Feature detection and Histogram equalization process.
CO 3	Formulate and solve problems in feature extraction methods, which help identify meaningful patterns and structures in images.
CO 4	Apply and implement basic tracking objects and pattern recognition techniques in images & videos.

Reference Books	
1.	David Forsyth and Jean Ponce, "Computer Vision: A Modern Approach", Prime student, 2nd edition, ISBN-13: 978-0136085928
2.	Rafael C. Gonzalez, Richard E. Woods;" Digital Image Processing"; Pearson Education; 3rd Edition; 2012; ISBN 978-93-325-7032-0.
3.	Milan Sonka, Vaclav Hlavac, Roger Boyle, "Image Processing, Analysis and Machine Vision". 3rd edition, CL Engineering, ISBN-13: 978-0495082521.
4.	Richard Szeliski, "Computer Vision: Algorithms and Applications", Springer Verlag : http://szeliski.org/Book/.

RUBRIC FOR THE CONTINUOUS INTERNAL EVALUATION (THEORY)		
#	**COMPONENTS**	**MARKS**

1.	**QUIZZES:** Quizzes will be conducted in online/offline mode. **TWO QUIZZES** will be conducted & Each Quiz will be evaluated for 10 Marks adding up to 20 Marks. **THE SUM OF TWO QUIZZES WILL BE CONSIDERED AS FINAL QUIZ MARKS.**	**20**
2.	**TESTS:** Students will be evaluated in test consisting of descriptive questions with different complexity levels (Revised Bloom's Taxonomy Levels: Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating). **TWO TESTS** will be conducted. Each test will be evaluated for 50 Marks, adding up to 100 Marks. **FINAL TEST MARKS WILL BE REDUCED TO 40 MARKS.**	**40**
3.	**EXPERIENTIAL LEARNING:** Students will be evaluated for their creativity and practical implementation of the problem. **Phase I (20) & Phase II (20)ADDING UPTO 40 MARKS**.	**40**
	MAXIMUM MARKS FOR THE CIE THEORY	**100**

RUBRIC FOR SEMESTER END EXAMINATION (THEORY)

Q. NO.	CONTENTS	MARKS
	PART A	
1	Objective type questions covering entire syllabus	20
	PART B (Maximum of TWO Sub-divisions only)	
2	Unit 1 : (Compulsory)	16
3 & 4	Unit 2 : Question 3 or 4	16
5 & 6	Unit 3 : Question 5 or 6	16
7 & 8	Unit 4 : Question 7 or 8	16
9 & 10	Unit 5: Question 9 or 10	16
	TOTAL	**100**

Semester: VI						
NETWORK PROGRAMMING AND SECURITY **Category: PROFESSIONAL CORE COURSE** **(Theory)**						
Course Code	**:**			**CIE**	**:**	**100 Marks**
Credits: L:T:P	**:**	**3:0:0**		**SEE**	**:**	**100 Marks**
Total Hours	**:**	**45L**		**SEE Duration**	**:**	**3 Hours**

Unit-I	**09 Hrs**
The Transport Layer and introduction to sockets: Introduction to TCP, UDP and SCTP, The big picture, Difference between UDP, TCP, SCTP, TCP connection establishment and termination, TIME_WAIT state, TCP port numbers and concurrent servers, Buffer sizes and limitation. Socket address structure, value result arguments, byte ordering functions, byte manipulation functions, inet_aton, inet_addr and inet_ntoa functions, inet_pton and inet_ntop functions.	
Unit – II	**09 Hrs**
TCP client/server: Socket function, connect function, bind, listen, accept, fork, exec functions, concurrent servers, close function, getsockname and getpeername functions, TCP Echo server – main – str_echo , TCP Echo client - main – str_echo, Normal startup, Normal termination.	

Unit III	09 Hrs
UDP client/server and Name server: Socket options introduction, getsockopt and setsockopt functions. recvfrom and sendto functions, UDP Echo server & UDP Echo client, lost datagrams. DNS, Gethostbyname function, gethostbyaddr function, getservbyname and getservbyport functions, getaddrinfo function, gai_strerror function, freeaddrinfo function, getaddrinfo function: example, host_serv function.	
Unit IV	**09 Hrs**
Traditional Block Cipher and Public Key Cryptosystem: Stream Ciphers and Block Ciphers, Feistel Cipher Structure. The Data Encryption Standard-Encryption and Decryption. Principles of Public Cryptosystems- Public-Key Cryptosystems, Applications for Public-Key Cryptosystems Requirements for Public-Key Cryptosystems, Public-Key Cryptanalysis. The RSA algorithm-Algorithm, Computational Aspects. The security of RSA, Other Public key Cryptosystems: Diffie-Hellman Key Exchange.	
Unit –V	**09 Hrs**
Transport Layer Security and Wireless Network Security: Web Security Considerations, Secure Socket Layer, Transport Layer security, HTTPS. Wireless Network Security: Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN overview, IEEE 802.11i Wireless LAN Security – Services, Phases of operation.	

Course Outcomes: After completing the course, the students will be able to: -	
CO 1	Alalyze the OSI reference model and a variety of network concepts and protocols.
CO 2	Analyze network Protocols interoperability and application.
CO 3	Design and demonstrate client/server programs on Unix platforms to create robust real-world sockets-based applications.
CO 4	Apply appropriate cryptographic algorithms to ensure security of information through wired and wireless medium.

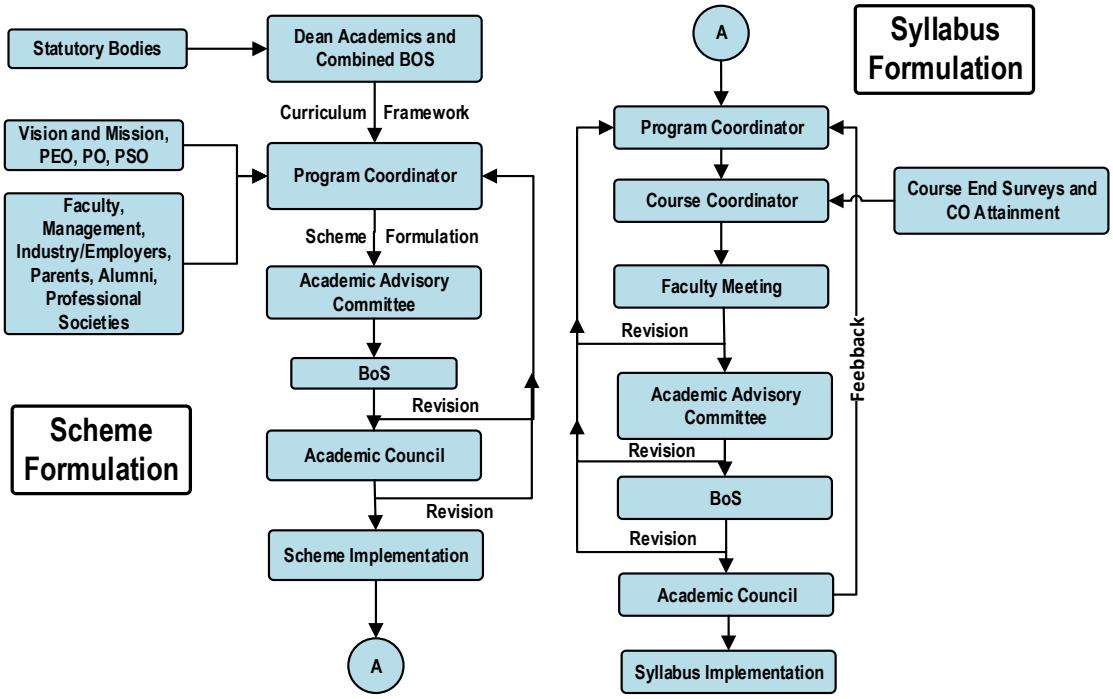
Reference Books

1.	W. Richard Stevens, Bill Fenner, Andrew M. Rudoff, UNIX Network Programming – Thesockets networking API, Vol.I , Third edition, PHI. ISBN-13: 978-0131411555 ISBN-10:9780131411555.
2.	William Stallings, "Cryptography and Network Security", 6th Edition, ISBN-13: 978-0-13-335469-0.
3.	Comer, Stevens, Internetworking with TCP/IP, Vol. III, Second Edition, PHI, ISBN-13: 978- 0132609692 ISBN-10: 013260969X.
4.	Richard M Reese, Learning Network Programming with Java, First Published: December2015, Packet Publishing Ltd., ISBN-13: 978-0123742551, ISBN-10: 0123742552.

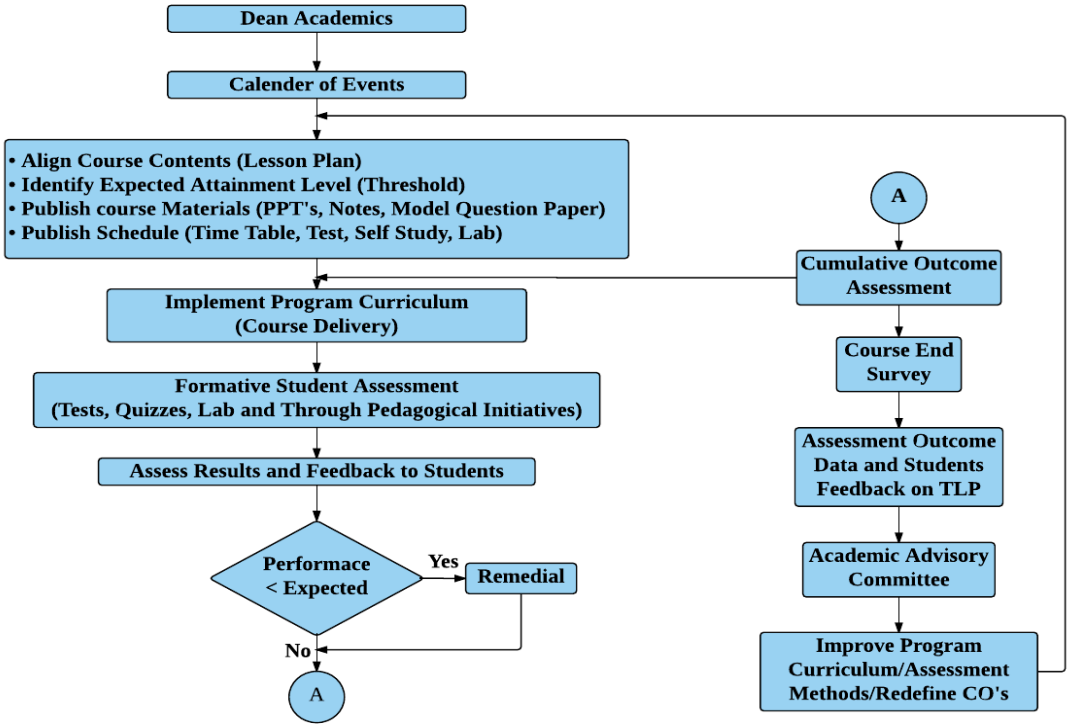
RUBRIC FOR THE CONTINUOUS INTERNAL EVALUATION (THEORY)		
#	**COMPONENTS**	**MARKS**
1.	**QUIZZES:** Quizzes will be conducted in online/offline mode. **TWO QUIZZES** will be conducted & Each Quiz will be evaluated for 10 Marks adding up to 20 Marks. **THE SUM OF TWO QUIZZES WILL BE CONSIDERED AS FINAL QUIZ MARKS.**	**20**
2.	**TESTS:** Students will be evaluated in test consisting of descriptive questions with different complexity levels (Revised Bloom's Taxonomy Levels: Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating). **TWO TESTS** will be conducted. Each test will be evaluated for 50 Marks, adding up to 100 Marks. **FINAL TEST MARKS WILL BE REDUCED TO 40 MARKS.**	**40**
3.	**EXPERIENTIAL LEARNING:** Students will be evaluated for their creativity and practical implementation of the problem. **Phase I (20) & Phase II (20)ADDING UPTO 40 MARKS**.	**40**
	MAXIMUM MARKS FOR THE CIE THEORY	**100**

RUBRIC FOR SEMESTER END EXAMINATION (THEORY)		
Q. NO.	**CONTENTS**	**MARKS**
	PART A	
1	Objective type questions covering entire syllabus	20
	PART B (Maximum of TWO Sub-divisions only)	
2	Unit 1 : (Compulsory)	16
3 & 4	Unit 2 : Question 3 or 4	16
5 & 6	Unit 3 : Question 5 or 6	16
7 & 8	Unit 4 : Question 7 or 8	16
9 & 10	Unit 5: Question 9 or 10	16
	TOTAL	**100**

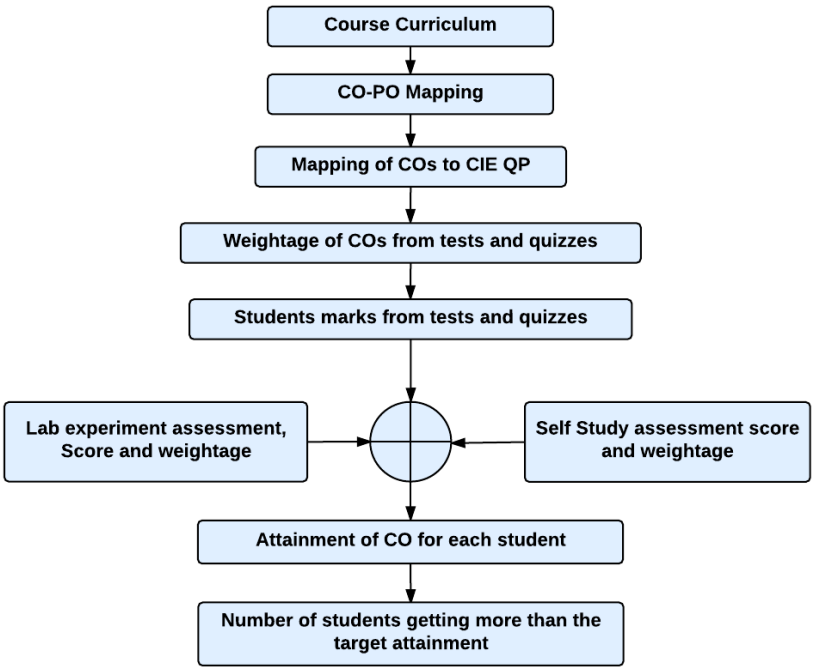
Curriculum Design Process



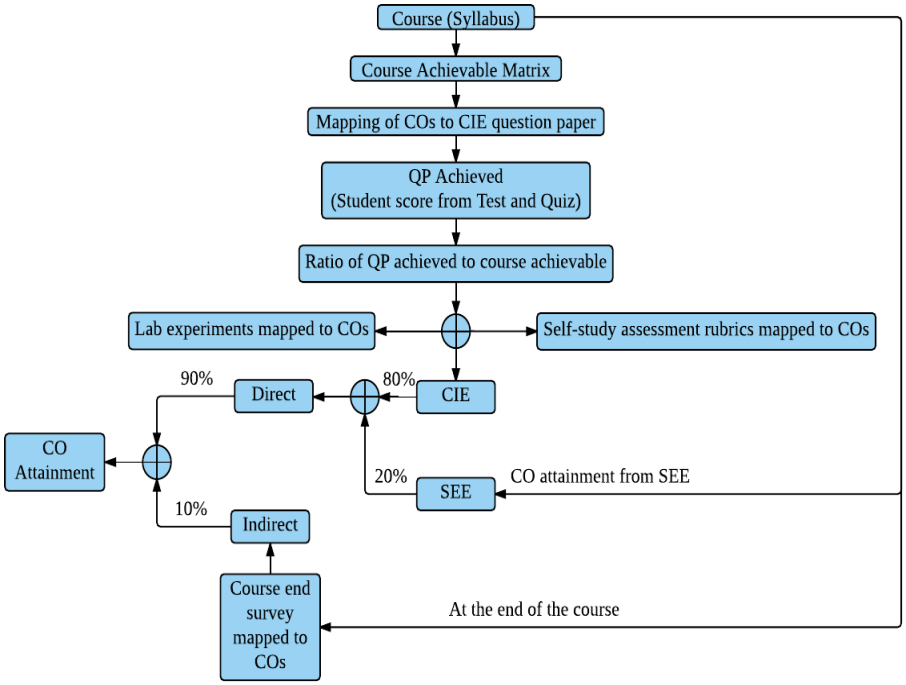
Academic Planning And Implementation



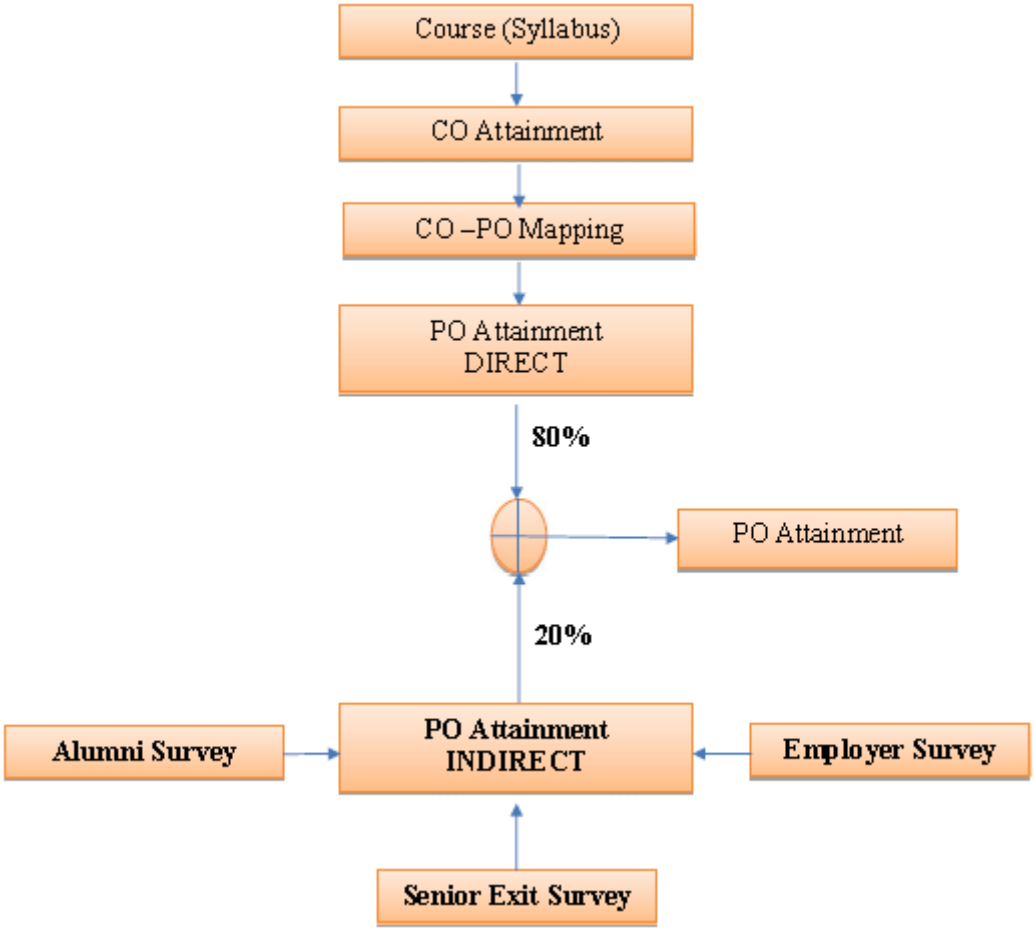
Process For Course Outcome Attainment



Final CO Attainment Process



Program Outcome Attainment Process



INNER BACK COVER PAGE

PROGRAM OUTCOMES (POs)

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialisation for the solution of complex engineering problems.

2. **Problem analysis:** Identify, formulate, research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modelling to complex engineering activities, with an understanding of the limitations.

6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with the society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning:** Recognise the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

RV College of Engineering®

Autonomous Institution Affiliated toVisvesvaraya Technological University, Belagavi

Approved by AICTE, Accredated by NBA

Department of Computer Science and Engineering

Phone: 080-68188199, 8200 : e-mail: hod.cse@rvce.edu.in