

Course Specifications

M. Tech. / PG Diploma Programme



Faculty of Engineering & Technology
M. S. Ramaiah University of Applied Sciences
University House, New BEL Road, MSR Nagar, Bengaluru – 560 054
www.msruas.ac.in

Course Specifications: Cyber Security and Information Assurance

Faculty	Engineering and Technology
Department	Computer Science and Engineering
Course	Cyber Security and Information Assurance
Dean of Faculty	Prof. H. K. Narahari
HOD	Prof. N. D. Gangadhar

1. Title of the Award

M. Tech. in Cyber Security and Information Assurance

2. Modes of Study

Full-Time Part-Time

3. Awarding Institution/Body

M S Ramaiah University of Applied Sciences-Bangalore, India

4. Joint Award

--

5. Teaching Institution

Faculty of Engineering and Technology (FET)

M S Ramaiah University of Applied Sciences-Bangalore, India

6. Date of Course Specifications

April 2015

7. Date of Course Approval by the Academic Council of MSRUAS

April 2015

8. Next Review Date

April 2017

9. Course Approving Regulatory Body and Date of Approval

--

10. Course Accrediting Body and Date of Accreditation

--

11. Grade Awarded by the Accreditation Body

--

12. Course Accreditation Validity

--

13. Course Benchmark

--

14. Rationale for the Course

The knowledge communities that we live in are built largely on the foundation of information awareness and exchange that span the globe based on seamless connectivity, Internet and Cloud technologies. Enterprises are built on such information assets which are well protected by skilled cyber security professionals and information officers. These qualified professionals are not only well versed in the state-of-the-art but also have the conceptual depth and practical knowledge to quickly master new ideas and techniques to protect valuable information assets and Information Technology (IT) infrastructure.

India is a global leader in computing services & solutions and produces the world's largest pool of engineering graduates. Masters programmes with industry focus are much sought after by fresh graduates as well as working professionals. However, there are a very few Postgraduate programmes which are designed to prepare engineers to meet the requirements and demands of the cyber security and information assurance industry.

M. S. Ramaiah University of Applied Sciences (MSRUAS) is located at Bengaluru, the centre for research, development and service delivery in the field of cyber security and information assurance. MSRUAS has established a strong industry interaction as well as collaborations with foreign Universities. Paladion Networks is a specialised partner for information risk management to leading organisations across industries in Asia, the United States, Europe, the Middle East and Africa. It is rated as the largest 'pure-play' IT security provider in Asia and is also the only Gartner rated managed security provider in the Middle East. This provides a good milieu for MSRUAS and Paladion networks to jointly offer an industry relevant, applied Masters' course in the Cyber Security and Information Assurance (CSIA) domain. The course emphasises design, development, deployment, monitoring and evaluation of cyber security and information assurance features in an enterprise. It includes development of security countermeasures and analytics applications using state-of-the-art computing and networking architectures & technologies.

The M. Tech. (CSIA) course is designed to develop innovative professionals who would demonstrate conceptual depth as well as practical knowledge to meet the demands placed on them. Fresh graduates, as well as working professionals seeking to upgrade their knowledge and qualification, will benefit from the industry relevant focus of the course. In addition, the experience of conducting research enables them to take up a research driven career path.

15. Course Aim

The aim of the Course is to produce postgraduates, with advanced knowledge & understanding of Cyber Security and Information Assurance domain, higher order critical, analytical, problem solving & transferable skills and the ability to think rigorously & independently, to meet the higher level expectations of industry, academia, research or entrepreneurship.

16. Course Objectives

Students will be taught to design, develop, test, deploy, analyse, operate and monitor cyber security and information assurance systems and services with emphasis on adoption of latest technologies.

The objectives of the course are to educate and train the students on the following:

1. Critical understanding of the underlying concepts, principles and processes of cyber security and information assurance
2. Models, protocols and policies employed in the architecture, design and securing of information technology infrastructure for enterprises
3. Design of IT subsystems & applications and their protection mechanisms in enterprise environments
4. Synthesis and securing of computing solutions using state-of-the-art frameworks, technologies and tools
5. Deployment and securing of IT infrastructure in enterprise environments
6. Analysis and auditing of security and information assurance capabilities of the IT infrastructure in enterprises
7. Conceptualisation of new security paradigms and enterprise security solutions for the future
8. General perspective on teamwork, lifelong learning and opportunities for a career in cyber security and information assurance domain
9. Ethics, legalities, economics, social sciences and interpersonal skills relevant to professional practice

17. Intended Learning Outcomes of the Course

The Intended Learning Outcomes (ILOs) are listed under four headings:

1. Knowledge and Understanding
2. Cognitive Skills
3. Practical Skills
4. Capability/ Transferable Skills.

17.1 Knowledge and Understanding

After undergoing this course, a student will be able to:

- KU1. Describe existing practices, methods, techniques & technologies underpinning cyber security and information assurance along with their future evolution
- KU2. Explain the concepts, principles and policies used in the development and securing of IT solutions
- KU3. Discuss models, methods, protocols, processes, frameworks and standards of IT infrastructure organisation, development and protection
- KU4. Identify and recommend appropriate strategies, architectures, protocols, mechanisms and techniques for developing and securing IT infrastructure

17.2 Cognitive Skills

After undergoing this course, a student will be able to:

- CS1. Apply appropriate models, approaches, protocols and policies to design and protect IT infrastructure of an enterprise
- CS2. Analyse the performance and quality of IT architectures and subsystems in an enterprise
- CS3. Evaluate and apply appropriate approaches, policies, architectures & systems to implement & secure information technology solutions in an enterprise
- CS4. Analyse and underpin quality of work with reference to supporting literature and case studies

17.3 Practical Skills

After undergoing this course, a student will be able to:

- PS1. Employ industry best practices for development, deployment, analysis, protection and audit of IT solutions
- PS2. Configure, secure and deploy network and computing subsystems of IT infrastructure
- PS3. Manage and audit secure information technology solutions
- PS4. Use appropriate tools for analysis, development and monitoring of IT infrastructure and its subsystems

17.4 Capability/Transferable Skills

After undergoing this course, a student will be able to:

- TS1. Manage information, develop technical reports and make presentations
- TS2. Build, manage and lead a team to successfully complete a task and communicate across teams & organisations for achievement of professional objectives
- TS3. Work under various constraints to meet targets
- TS4. Adopt ethics and practices of chosen profession by continuously upgrading his/her knowledge and understanding through life-long learning

18. Course Structure

A student is required to successfully complete the following modules for the award of the degree. The course is delivered as per the Time-Table for every batch.

Course: Cyber Security & Information Assurance			
Module Code	Modules	Credits	Duration (Weeks)
	Foundation course		2
Department Common Modules			
CSE503	1. Essentials and Practice of Software Engineering	5	5
CSE501	2. Data Structures, Algorithms and Programming Principles	5	5
CSE504	3. Wired and Wireless Networking	5	5
Course Specialisation Modules			
CSN501	1. Discrete Mathematical Methods	5	5
CSN502	2. Real Time Operating Systems and System Programming	5	5
CSN504	3. Distributed and Cloud Computing	5	5
CIP501	4. Network and Application Security	5	5
CIP502	5. Security Intelligence	5	5
CIP503	6. Governance, Risk Compliance	5	5
Faculty-Common Modules			
FET501	1.Principles of Management and Soft Skills Development	3	3
FET502	2.Research Methodology	3	3
Elective Module (Any One)			
FET503	Industry Internship		
FET505	Training		
CIP599	Group Work-Project	10	10
CIP600	Individual Work – Project	30	26
Mandatory Module (Any One)			
FET509	1. Conference Publication		
FET510	2. Journal Publication		
		100	96*

Note:

1. The Vacations and other activities shall be as per the Time-Table for the corresponding batch.
2. * - Excluding Foundation Course

19. Module Delivery Structure-Full-Time

A module is delivered from Monday to Friday of the week. The lecture classes will be normally held from 9.30 PM to 1.00 PM with 30 minutes of break. The laboratory classes will be scheduled during the same days from 2.00 PM to 5.30 PM in the first two weeks of the module.

Week-1	Week-2	Week-3	Week-4	Week-5
Module Delivery	Module Delivery	Study Work	Study Work	Assignment submission & Presentation
			Examination	

20. Teaching and Learning Methods

The module delivery comprises of a combination of few or all of the following:

1. Face to Face Lectures using Audio-Visuals
2. Workshops, Group Discussions, Debates, Presentations
3. Demonstrations
4. Guest Lectures
5. Laboratory/Fieldwork/Workshop
6. Industry Visit
7. Seminars
8. Group Exercises
9. Project Exhibitions
10. Technical Festivals

21. Mandatory Module

FET509 Conference Publication
A student can submit a paper and make a presentation in a conference which is approved by the department. The same paper shall be presented for assessment and the student is required to make a presentation to a team of examiners for assessment.

FET510 Journal Publication
A student can publish a paper in a technical journal. The proof of submission and a copy of the paper shall be submitted to the department. It will be assessed based on a presentation to a team of examiners.

22. Group Project

CIP599 A group shall have up to 5 students. The purpose of group project is that the group should be able to design a product in their area of specialisation and develop it. The students are required to develop a report for assessment and also need to demonstrate the working of the product. The IPR policy is in line with the University IPR policy. The students are required to sign an agreement before the commencement of the project. The project should be approved by a committee of examiners before the start of the project. Students can choose a project from the database of projects available with the concerned department. The detailed procedure and evaluation procedure will be provided in Operations Manual / Student Handbook.

23. Individual Project

CIP600 A student chooses a topic for the individual project from the database of the projects
Faculty of Engineering and Technology

available with the concerned department. The detailed procedure of executing and assessing individual project is available in the Student Handbook.

24. Assessment and Grading

A module assessment will have two components:

Component-1

Assignment 50% weight

Component-2

Examination 50% weight

(Note: For more details on the break-up, please refer to the Module Specifications)

A student is required to score a minimum of 40% in each of the components and an overall 40% for successful completion of a module and earning the credits.

Note: Final marks awarded in each of the modules will be confirmed only after SAB/PAB as explained in Academic Regulations of M. Tech. Programme.

25. Failure and Re-admissions

If a student fails in a module, he/she is required to re-attend the module when offered next time by re-registering to the module.

26. Attendance

A student is required to have a minimum of 85% attendance to be eligible to write the examination. Less than 85% attendance is considered FAIL; such a student is required to follow the same procedure as that of a failed student

Any condoning of shortfall of the attendance is as per the Academic Regulations for M.Tech. Programme

27. Award of Class

As per the Academic Regulations for M. Tech. Programme.

28. Student Support for Learning

Students are given the following support:

1. Module notes
2. Reference books in the library
3. Magazines and Journals
4. Internet facility
5. Computing facility
6. Laboratory facility
7. Workshop facility
8. Staff support
9. Lounges for discussions
10. Any other support that enhances their learning

29. Quality Control Measures

Following are the Quality Control Measures:

1. Review of module notes
2. Review of question papers and assignment questions
3. Student feedback
4. Moderation of assessed work
5. Opportunities for the students to see their assessed work
6. Review by external examiners and external examiners' reports
7. Staff student consultative committee meetings
8. Student exit feedback
9. Subject Assessment Board
10. Programme Assessment Board

30. Curriculum Map

Module Code	Intended Learning Outcomes											
	Knowledge and Understanding				Cognitive (Thinking) Skills (Critical, Analytical, Problem Solving, Innovation)				Practical Skills			
	KU1	KU2	KU3	KU4	CS1	CS2	CS3	CS4	PS1	PS2	PS3	PS4
CSE503	X	X	X	X	X		X	X	X			X
CSE501	X	X	X	X	X		X	X				
CSE504	X	X	X	X	X	X		X		X		X
CSN501	X		X			X		X				
CSN502	X	X		X	X	X	X	X		X		
CSN504	X	X	X	X	X	X	X	X		X		X
CIP501	X	X	X	X	X	X	X	X	X	X		X
CIP502	X	X	X			X		X	X			X
CIP503	X	X	X	X		X	X	X	X		X	X
FET501								X				
FET502								X				
FET503	X							X				
FET505	X		X					X	X	X	X	X
CIP599	X	X	X	X	X	X	X	X	X	X	X	X
CIP600	X	X	X	X	X	X	X	X	X	X	X	X

31. Capability/Transferable Skills

Module Code	Group work	Self-learning	Research Skills	Written Communication Skills	Verbal Communication Skills	Presentation Skills	Behavioural Skills	Information Management	Personal management/ Leadership Skills
CSE503		X	X	X	X	X		X	
CSE501		X	X	X	X	X		X	
CSE504		X	X	X	X	X		X	
CSN501		X	X	X	X	X		X	
CSN502		X	X	X	X	X		X	
CSN504		X	X	X	X	X		X	
CIP501		X	X	X	X	X		X	
CIP502		X	X	X	X	X		X	
CIP503	X	X	X	X	X	X	X	X	
FET501	X	X	X	X	X	X	X	X	X
FET502		X	X	X	X	X		X	
FET503	X	X		X	X	X	X	X	X
FET505	X	X		X	X	X	X	X	X
CIP599	X	X	X	X	X	X	X	X	X
CIP600		X	X	X	X	X	X	X	X

