Cyber Security: Sem VII								
Course Code	**Course Title**	**Theory**	**Practical**	**Tutorial**	**Theory**	**Practical/Oral**	**Tutorial**	**Total**
HCSC701	**Security Information Management**	**04**	**--**	**--**	**04**	**--**	**--**	**04**

Course Code	**Course Title**	**Examination Scheme**							
		Theory Marks				**Term Work**	**Practical**	**Oral**	**Total**
		Internal assessment			**End Sem. Exam**				
		Test 1	**Test 2**	**Avg.**					
HCSC701	**Security Information Management**	**20**	**20**	**20**	**80**	**--**	**--**	**--**	**100**

Course Objectives:

Sr. No.	**Course Objectives**
The course aims:	
1	The course is aimed to focus on cybercrime and need to protect information.
2	Understand the types of attacks and how to tackle the amount of risk involved.
3	Discuss the role of industry standards and legal requirements with respect to compliance.
4	Distinguish between different types of access control models, techniques and policy.
5	Awareness about Business Continuity and Disaster Recovery.
6	Awareness about Incident Management and its life cycle.

Course Outcomes:

Sr. No.	**Course Outcomes**	**Cognitive levels of attainment as per Bloom's Taxonomy**
On successful completion, of course, learner/student will be able to:		
1	Understand the scope of policies and measures of information security to people.	L1,L2
2	Interpret various standards available for Information security.	L1,L2
3	Apply risk assessment methodology.	L3
4	Apply the role of access control to Identity management.	L3
5	Understand the concept of incident management**,** disaster recovery and business continuity.	L1,L2
6	Identify common issues in web application and server security.	L3

DETAILED SYLLABUS:

Sr. No.	**Module**	**Detailed Content**	**Hours**	**CO Mapping**
0	**Prerequisite**	Vulnerability Assessment for Operating Systems, Network (Wired and Wireless). Tools for conducting Reconnaissance.	**2**	--

I	**Basics of Information Security**	**1.1** What is Information Security & Why do you need it? – **1.2** Basics Principles of Confidentiality, Integrity **1.3** Availability Concepts, Policies, procedures, Guidelines, Standards **1.4** Administrative Measures and Technical Measures, People, Process, Technology, IT ACT 2000, IT ACT 2008 **Self-learning Topics:** Impact of IT on organizations, Importance of IS to Society	**6**	CO1, CO2
II	**Current Trends in Information Security**	**2.1** Cloud Computing: benefits and Issues related to information Security. **2.2** Standards available for InfoSec: Cobit, Cadbury, ISO 27001, OWASP, OSSTMM. **2.3** An Overview, Certifiable Standards: How, What, When, Who. **Self-learning Topics:** Cloud Threats, Impact of cloud computing on users, examples of cloud service providers: Amazon, Google, Microsoft, Salesforce etc.	**8**	CO2
III	**Threat & Risk Management**	**3.1** Threat Modelling**:** Threat, Threat-Source, Vulnerability, Attacks. **3.2** Risk Assessment Frameworks**:** ISO 31010, NIST-SP-800-30, OCTAVE **3.3** Risk Assessment and Analysis: Risk Team Formation, Information and Asset Value, Identifying Threat and Vulnerability, Risk Assessment Methodologies **3.4** Quantification of Risk, Identification of Monitoring mechanism, Calculating Total Risk and Residual Risk. **Self-learning Topics:** Risk management trends today and tomorrow.	**8**	CO3
IV	**Identity and Access Management**	**4.1** Concepts of Identification, Authentication, Authorization and Accountability. **4.2** Access Control Models: Discretionary, Mandatory, Role based and Rule-based. **4.3** Access Control Techniques: Constrained User, Access control Matrix, Content-dependent, Context – dependent **4.4** Access Control Methods: Administrative, Physical, Technical, Layering of Access control **4.5** Access Control Monitoring: IDS and IPS and anomaly detection. **4.6** Accountability: Event-Monitoring and log reviews. Log Protection **4.7** Threats to Access Control: Various Attacks on the Authentication systems. **Self-learning Topics:** challenges and solutions in identity and access management	**10**	CO4
V	**Operational Security**	**5.1** Concept of Availability, High Availability, Redundancy and Backup. **5.2** Calculating Availability, Mean Time Between Failure (MTBF), Mean Time to Repair (MTTR)	**10**	CO5

		5.3 Incident Management**:** Detection, Response, Mitigation, Reporting, Recovery and Remediation **5.4** Disaster Recovery: Metric for Disaster Recovery, Recovery Time Objective (RTO), Recovery Point Objective (RPO), Work Recovery Time (WRT), Maximum Tolerable Downtime (MTD), Business Process Recovery, Facility Recovery (Hot site, Warm site, Cold site, Redundant site), Backup & Restoration **Self-learning Topics:** Challenges and Opportunities of Having an IT Disaster Recovery Plan		
VI	**Web Application, Windows, and Linux security**	**6.1** Types of Audits in Windows Environment **6.2** Server Security, Active Directory (Group Policy), Anti-Virus, Mails, Malware **6.3** Endpoint protection, Shadow Passwords, SUDO users, etc. **6.4** Web Application Security: OWASP, Common Issues in Web Apps, what is XSS, SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues, etc. **Self-learning Topics:**, Network firewall protection,Choosing the Right Web Vulnerability Scanner	**8**	CO6

Textbooks:

1. Shon Harris, Fernando Maymi, CISSP All-in-One Exam Guide, McGraw Hill Education, 7th Edition, 2016.
2. Andrei Miroshnikov, Introduction to Information Security - I, Wiley, 2018
3. Ron Lepofsky, The Manager's Guide to Web Application Security, Apress; 1st ed. edition, 2014

References:

1. Rich-Schiesser, IT Systems Management: Designing, Implementing and Managing World - Class Infrastructures, Prentice Hall; 2 edition, January 2010.
2. NPTEL Course: - Introduction to Information Security – I (URL: https://nptel.ac.in/noc/courses/noc15/SEM1/noc15-cs03/)
3. Dr. David Lanter – ISACA COBIT – 2019 Framework - Introduction and Methodology
4. Pete Herzog, OSSTMM 3, ISECOM
5. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, September 2012

Online References:

Sr. No.	Website Name
1.	https://www.ultimatewindowssecurity.com/securitylog/book/Default.aspx
2.	http://www.ala.org/acrl/resources/policies/chapter14
3.	https://advisera.com/27001academy/what-is-iso-27001/

4.	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf
5.	http://www.diva-portal.org/smash/get/diva2:1117263/FULLTEXT01.pdf

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

➢ **Question paper format**

- Question Paper will comprise of a total of **six questions each carrying 20 marks Q.1** will be **compulsory** and should **cover maximum contents of the syllabus**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** need to be answered