Professional Diploma in Cyber Security Management

Regulations, Curriculum and Syllabus

(Applicable to the students admitted from the Jan 2020 onwards)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING SCIENCES

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE

Rajiv Gandhi Salai (OMR), Padur, Chennai – 603 103

1.1 Motto, Vision, Mission and Value Statement Objectives

MOTTO

"TO MAKE EVERY MAN A SUCCESS AND NO MAN A FAILURE"

VISION

To be an International Institute of Excellence, providing a conducive environment for education with a strong emphasis on innovation, quality, research and strategic partnership blended with values and commitment to society.

MISSION OF THE INSTITUTION:

- To create an ecosystem for learning and world class research.
- To instill highest ethical standards and values with a sense of professionalism.
- To take up activities for the development of society.
- To develop national and international collaboration and strategic partnership with industry and institutes of excellence.
- To enable graduates to become future leaders and innovators.

VALUE STATEMENT

Integrity, Innovation, Internationalization

1.2 Further the Institute always strives

- to train our students with the latest and the best in the rapidly changing fields of Engineering, Technology, Management, Science & Humanities.
- to develop the students with a global outlook possessing, state of the art skills, capable of taking up challenging responsibilities in the respective fields.
- to mould our students as citizens with moral, ethical and social values so as to fulfill their obligations to the nation and the society.
- to promote research in the field of Science, Humanities, Engineering, Technology and allied branches.

1.3 Aims and Objectives of the Institute are focused on

- Providing world class education in engineering, technology, applied sciences and management.
- Keeping pace with the ever changing technological scenario to help the students to gain proper direction to emerge as competent professionals fully aware of their commitment to the society and nation.
- To inculcate a flair for research, development and entrepreneurship.

2. Admission

2.1. The admission policy and procedure shall be decided from time to time by Academic Council, the Board of Management (BOM) of the Institute, following guidelines issued by Ministry of Human Resource Development (MHRD), UGC and AICTE.

2.2 Eligibility

Aspirants with Graduation from any stream with knowledge of computers.

OR

Aspirants with higher secondary and two years exposure in computer related work.

OR

Aspirants with higher secondary followed by a diploma and two years exposure in computer related work.

The term related is used in the context of network security, computer security, security administrator, network administrator, system administrator, Desktop administrator, web administrator, domain administrator, cyber investigator, police investigator etc.,

2.3. Enrollment Process

The filled applications shall be scrutinized by the admission committee. All applicable eligibility credentials are validated (Graduation, proof of employment, proof of experience as defined in eligibility criteria). A personal interview by a Panel of professionals will be carried out to evaluate the candidate, his knowledge of computers and understand the submitted credentials to complete the enrollment.

2.4. If at any time after admission, it is found that a candidate has not fulfilled any of the requirements stipulated by the Institute, the Institute may revoke the admission of the candidate with information to the Academic Council.

3. Structure of the programme

3.1. The structure of the programme shall have theory courses, practical course(s) and professional practices including project.

3.2. Duration

The duration of the professional diploma programme will be a minimum of 6 months. However a student may be permitted to complete the programme with additional 24 months as a maximum duration.

3.3 The academic programmes of the Institute follow the credit system.

- One credit for each lecture hour per week per semester;
- One credit for each tutorial hour per week per semester;
- One credit for each laboratory practical of two/three hours per week per semester.
- One credit for 4 weeks of industrial training and
- One credit for 4 hours of project per week per semester

3.4. Award of Professional Diploma

A student has to earn minimum credits specified in the curriculum of the relevant programme of study to award of Professional Diploma.

3.5. Medium of Study

The medium of instruction, examination and the language of the project reports will be English.

3.6 Faculty Advisor

To help the students in planning their courses of study and for getting general advice on the academic programme, the Department will assign a certain number of students to a faculty member who will be called their Faculty Advisor.

4. Discipline

4.1. Every student is required to observe discipline and decorous behaviour both in-side and outside the campus and not to indulge in any activity which will tend to bring down the prestige of the University.

4.2. Any act of indiscipline of a student reported to the Dean (E&T) will be referred to a Discipline Committee so constituted. The Committee will enquire into the charges and decide on a suitable punishment if the charges are substantiated. The committee will also authorize the Dean (E&T) to recommend to the Vice Chancellor the implementation of the decision. The student concerned may appeal to the Vice Chancellor whose decision will be final. The Dean (E&T) will report the action taken at the next meeting of the Council.

5. Attendance

5.1. A student whose attendance is less than 75% is not eligible to appear for the end – semester examinations for that semester. The details of all students who have less than 75% attendance in a course will be announced by the teacher in the class.

5.2. Those who have less than 75% attendance will be considered for condonation of shortage of attendance. However, a condonation of 10% in attendance will be given on medical reasons.

5.3 Application for condonation recommended by the Faculty Advisor, HOD, Dean is to be submitted to the attendance grievance committee, the committee, depending on the merits of the case, may permit the student to appear for the end semester examinations. Application for medical leave, supported by medical certificate with endorsement by a Registered Medical Officer, should reach the HOD within seven days after returning from leave or, on or before the last instructional day of the semester, whichever is earlier.

6. Assessment Procedure

6.1. The assessment for the theory course shall be assessed through the continuous basis as follows:

Test / Exam	Weightage	Duration of Test / Exam
First Periodical Test	10%	2 hours
Second Periodical Test	10%	2 hours
Third Periodical Test/ Model	20%	3 hours
Seminar/ Assignments/ Quiz	10%	
Attendance	10%	
End – semester Exam	50%	3 hours

6.2 The assessment for the practical courses shall be
(i) Weekly assignment/Observation note book / lab records – weightage 60%.
(ii) End semester examination of 3 hours duration including viva – weightage 40%.

6.3 Project Evaluation

The periodic review shall be conducted to assess the students' performance on the project work.

The Internal Continuous Assessment = 50%

End Semester Assessment = 50%

The end – semester examination will be conducted by a panel of examiners constituted by the Controller of Examination.

7. Declaration of results

7.1 A candidate who secures not less than 50% of total marks prescribed for a course with a minimum of 50% of the marks prescribed for the end semester examination and 50% marks in the continuous internal assessment shall be declared to have passed the course and earned the specified credits for the course.

7.2 If a candidate fails to secure a pass in a course due to not satisfying the minimum requirement in the end semester examination, he/she shall register and re-appear for the end semester examination during the following semester. However, the continuous internal marks secured by the candidate will be retained for all such attempts.

7.3 A candidate can apply for the revaluation of his/her end semester examination answer paper in a theory course within stipulated time from the declaration of the results, on payment of a prescribed fee through proper application to the Registrar/Controller of Examinations through the Head of the Department. The Registrar/ Controller of Examination will arrange for the revaluation and the results will be intimated to the candidate concerned through the Head of the Department. Revaluation is not permitted for practical courses and for project work.

8. Grading

8.1 A Grading system as below will be adhered to.

Range of Marks	Letter Grade	GP
100-95	S	10
85 - 94	A	09
75- 84	B	08
65-74	C	07
55-64	D	06
50-54	E	05
< 50	U	00

8.2 Grade Point Average

GPA is the ratio of the sum of the product of the number of credits C_i of course "i " and the grade points P_i earned for that course taken over all courses "i" registered by the student to the sum of C_i for all "i ". That is,

$$GPA = \frac{\sum_i C_i P_i}{\sum_i C_i}$$

8.3 Class/ Division

8.3.1 The Classification is based on CGPA and is as follows:

CGPA $\geq$ 8.0 : **First Class with distinction**

6.5 $\leq$ CGPA < 8.0: **First Class**

5.0 $\leq$ CGPA < 6.5 : **Second Class.**

8.3.2 Further, the award of 'First class with distinction' is subject to the candidate becoming eligible for the award of the degree having passed the examination in all the courses in his/her first appearance within the minimum duration of the programme.

9 Eligibility for the award of Professional Diploma

9.1 A student will be declared to be eligible for the award of the **Professional Diploma** if he/she has

i) registered and successfully acquired the credits for the courses;

ii) successfully acquired the credits in the different categories as specified in the curriculum corresponding to the discipline (branch) of his/her study within the stipulated time;

iii) has no dues to all sections of the Institute including Hostels, and

iv) has no disciplinary action pending against him/her.

The award of the degree must be recommended by the Academic Council and approved by the Board of Management of the University.

10. Power to modify

Notwithstanding all that has been stated above, the Academic Council shall modify any of the above regulations from time to time subject to approval by the Board of Management.

PROGRAMME EDUCATIONAL OBJECTIVES

1. To develop highly competent Professionals in Cyber Investigation and Laws and Engineering who are able to spearhead related ICT industries.
2. To encourage the Graduates to go for higher studies leading to excellent research contributions to the Society.
3. To train the Graduates to practice lifelong learning for continuing professional development.

PROGRAMME OUTCOME

1. Ability to acquire and apply fundamental principles of Cyber Security and Laws
2. Capability to communicate effectively.
3. Acquisition of technical competence in specialised areas of computing discipline.
4. Ability to identify, formulate and model problems and find engineering solutions based on a systematic approach.
5. Ability to conduct investigation and research on engineering problems in a chosen field of specialisation.

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Professional Diploma in Cyber Security Management

CURRICULUM

Sl. No	Course Code	Course Title	L	T	P	C	TCH
SEMESTER I							
Theory							
1.	CSP201	Cyber Risk Management	3	0	0	3	3
2	CSP211	Information System Audit Management	3	0	0	3	3
3.	CSP212	Infrastructure Penetration Testing Management	3	0	0	3	3
4.	CSP213	Remote Infrastructure Management	3	0	0	3	3
5.	CSP205	SIEM & Log trails	3	0	0	3	3
Practical							
6.	CSP233	Case Studies	0	2	0	2	2
7.	CSP232	Project Work	0	0	6	3	6
		Total Credits	**20 Credits**				

CSP201	Cyber RISK Management	L T P C 3 0 0 3
Goal	To introduce the principles of Cyber Risk management and expose the various techniques of Risk evaluation	

Objective:	Outcome :
• Understand the components of IT Systems • Understand the IT assets and Asset evaluation techniques • Understand the Threat modeling methods • Understand the elements of Risk assessment • Understand Business Continuity	• Differentiate the IT components • Apply Asset evaluation methods • Apply threat modelling methods • Apply the elements of Risk Assessment techniques • Apply business continuity components

Unit 1: IT Systems: Information Systems - System components - network components - Risk management - What is Risk - profile - identification -assessment -Analysis -Response - Tolerance - Risk types - inherent risk - control risk - audit risk. -Security risk analysis - Advantages

Unit 2: IT Assets: Assets management - Identify Assets - Asset classification - Asset valuation - Binary Asset Valuation -Rank-Based Asset Valuation - Consensus Asset Valuation - Classification-Based Asset Valuation - others

Unit 3: Cyber Threat: Threat management - Identifying Threats -Threat model - Threat attributes - Attack tree - STRIDE - DREAD - OCTAVE - CAPEC- Threat Statements- Technical Threats and Safeguards - Physical Threats and Safeguard - Human Threats to Physical Security - The RIIOT Method: Physical Data Gathering - Test Physical Security Safeguard.

Unit 4: Risk Assessment: Security Risk Assessment - Quantitative vs. Qualitative Analysis - Determining Risk - Creating Risk Statement - Security Risk Mitigation - Selecting Safeguard - Security Risk Assessment Reports - Report Structure.

Unit 5: Business Continuity: Principles of Business continuity - Business Interruption Events – Business impact assessment – fire exposure analysis – functional analysis –compliance issues – Pre-Planning - Initial Response - Recovery - Identification of Recovery environment - Identification of Recovery Point - site and structures – Equipment and technology – documents and records electronic equipment and process equipment - Business continuity plans – crisis management plans –function restoration plans – disaster recovery plans – Incident Response Plan

Text Book

1. Thomas L Norman., Risk analysis and Security counter measure selection , CRC press, 2010
2. Ariel Evans, Managing Cyber Risk, Routledge, 2019
3. Lee T Ostrom, Risk Assessment: Tools, Techniques, and Their Applications, Wiley 2019
4. Christopher Hodson,, Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls, Kogan, 2019
5. Richard.E Cascarino., Auditors guide to information system auditing, John Wiley and Sons, 2007.

DCE202	**Information System Audit Management**	L T P C 3 0 0 3
Goal	To introduce the relevance of IS audit and expose the various audit methodologies for the different audit profiles	

Objective:	**Outcome :**
• Understand Audit as a profession • Understand the relevance of governance frameworks • Understand the security Frameworks like NIST, OWASP and ISO27001 • Understand the methods of generating Audit reports	• Evaluate COBIT controls • Differentiate NIST and ISO27001 requirements • List the relevance of OWASP controls • Design Audit plan and schedule

Unit 1: Auditing Profession - Audit function - Internal - External -Need for IT Audit -Role of the IT Auditor - counsellor - partner - investigator - Common body of knowledge - Institute of internal auditors - Ethics and code of practice - ISACA - Ethics and code of practice.

Unit 2: IT Governance Frameworks - COBIT - Why Controls? - Internal controls - Control Framework - Control Models - IT Performance Metrics -The External Audit

Unit 3: NIST Security audit - assessment techniques - Testing viewpoints - Review techniques - Target analysis techniques - Assessment planning - Execution - Cloud Audit Standards - IT security Audit standard - ISO/IEC 27001 - Controls - Internal Audit - External Audit - Compliance Audit

Unit 4: IS Audit - Management process - needs - performance objectives - The Audit Charter - IT Audit process - Audit plan - Audit schedule - Audit team - Audit Tasks - Audit procedures - Audit Findings - Other Types of IT Audits.

Unit 5: Audit Productivity Tools - Flow charting as an Audit Analysis Tool - Computer-Assisted Audit Techniques - Audit working papers - Audit presentation -

Text books

1. Angel R Otero., Information technology control and audit, CRC Press, 5th Ed, 2019
2. K.H.Spencer Pickett., The essential handbook of internal auditing, John Wiley, 2005
3. Handbook on Professional Opportunities in Internal Audit, Sahitya Bhawan Publications, 2011
4. Ana Cecilia Delgado, COBIT 5 Foundation – reference and study guide, Createspace Independent Pub, 2016,
5. Weber, Information Systems: Control & Audit, Pearson, 2016

DCE203	**Infrastructure Penetration Testing Management**	L T P C 4 0 0 4
Goal	To understand the internals of the operating systems leading to locati evidences and mapping the same to judiciary requirements in terms of FIR and associated IPC requirements.	

Objective:	**Outcome :**
• Understand the elements of cyber security • Understand Cloud APIs • Understand the concept of Vulnerability and tools • Understand the Various security standards • Understand the various types of compliance reports • Understand service Delivery	• Apply and Manage the Vulnerability Tools • Apply and manage the pen test tools • Design Pen Test reports • Design compliance reports • Design Service delivery reports

Unit 1: Confidentiality Integrity and privacy - availability - access control - access control techniques - authorization -authentication tokens - Key Management - Kerberos - Hashes - APIs - API Gateway - API Life cycle management -API documentation standards - API management patterns - API security patterns - API authentication - protection against cyber threats

Unit 2: Vulnerability Management - Vulnerability Framework - The Vulnerability Creation Process - General Architecture - Charter Development - Business Case - Asset Valuation Guide - VM Policies - Deployment Strategies - Basic Strategy - Risk-Based Strategy - Controlling Internal Vulnerabilities - Principles of Mitigation - vulnerability assessment - Nessus - NMAP - Pen testing - Tools.

Unit 3: Standards - Common Vulnerabilities and Exposure, Common Vulnerability Scoring System, - National Vulnerability Database(NVD) - Common Platform Enumeration - Security Content Automation Protocol - Trusted Automated exchange of indicator information - OWASP Application security verification standard - Payment Card Industry - PCI compliance - HIPAA - HIPAA compliance

Unit 4: Discovery Reports - Scheduling - Evaluation Reports - Profile Reports -Audit Reports -Audit Trend Analysis -Vulnerability Trend Report -Network Risk Trend Report - Compliance reports

Unit 5: IT Systems - System components - ITIL / ITSM process- Components/Elements of a Service - Service definition - configuration management - Infrastructure as code - versions - patch management - tools like Ansible - Chef - IT Service catalog - Self service - Request management - Incident management - knowledge management - problem management - Service level agreement management - Vendor management - Change management.

Text Books

1. Park Foreman, Vulnerability Management, CRC press, 2010
2. Georgia Weidman, Penetration Testing – A Hands–On Introduction to Hacking, No Starch Press, 2014
3. William Chuck Easttom II, Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, Pearson, 2018
4. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, Auerbach, 2017
5. Brajesh De, API management, APress, 2017
6. Gerardus Blokdyk , Payment Card Industry Security Standards Council A Complete Guide,5STARCooks 2019

DCE204	Remote Infrastructure Management	L T P C 4 0 0 4
Goal	To enable a prospective student to understand the various types of cybe and associated legal implications.	

Objective:	**Outcome :**
• Understand the concept of cyber crime • Understand & differentiate types of cyber crime • Understand network crime and techniques • Understand IT ACT and role • Correlate IT ACT with related acts	• Differentiate the various types of cyber crime • Differentiate the various types of virus and BOTS and their crime ware capabilities • Differentiate the various elements of IT act and related amendments • IT acts influence on Related acts

Unit 1**:** Installation: Installation - Capacity Planning Redundancy and Backup - Installing the Nagios Software- Nagios Server - Nagios Plug-ins - Configuring Web Server for Nagios - Report Triggers - Scheduling - Report templates

Unit 2: Nagios roles: How Does Nagios Work? - How Is Nagios Configured- Getting Started - Configuration -Specifying Configuration Files - Nagios objects - Defining Nagios Configuration Objects - defining host –Services – templates – contact objects – group objects – time periods – commands

Unit 3 Security and administration: General security guidelines – Web console security –Nagios administration – using the web console - Monitoring hosts and services – tactical monitoring – reporting – Remote monitoring – NRPE – SSH

Unit 4: Advanced commands: Macros – event handlers – notifications – External commands – host and services dependencies – Notification escalations – Distributed monitoring, redundancy and failover – Integrating Nagios - MRTG, Zabbix, Cacti, and other tools

Unit 5 OpenNMS: Installation, configuration, types of files, Add, modify, delete, nodes, RRD, RRD xml templates - report generations – Dashboards.

Text

1. Wojciech Kocjan, Learning Nagios, 3rd Ed, PACKT, 2016.
2. Tom Ryder, Nagios Core Administration Cookbook, Packt, 2013
3. James turnbull Pro Nagious 2, Apress, 2006
4. Williams Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1&2, Pearson 2002
5. Douglas R. Mauro, Essential SNMP: Help for System and Network Administrators, Orielly, 2005
6. Ghislain Hachey, Instant OpenNMS Starter, Packt, 2013
7. Chris Sanders , Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2014

CSP205	SIEM AND LOG TRAILS	L T P C 3 0 0 3
Goal	To expose the learner on the relevance of various types of Logs generated from different systems and expose the concept of SIEM which is used for Log correlation and alerts	

Objective:	**Outcome :**
• Understand the relevance of MIB and RMON • Understand the Concept of Log formats and log correlation • Understand the relevance and working of Syslog server • Understand the relevance and working of SNORT	• Differentiate the MIBs, OIDs and RMON capabilities • Differentiate the Log formats • Understand the configurations of Syslog server • Understand SNORT configuration and SNORT rules.

Unit 1: Introduction: Concepts of Log, What Should the Logs Log? Everything - The 5 Ws (Who, What, When, Where, and Why) - Unix Logs – Windows Logs - Events and Event Lifecycle - Linux Logs - Types of logs - Security logs - Application logs – System Logs – WMI – WMI Architecture

Unit 2: SNMP: Simple Network Management Protocol – Structure – Basic commands – get get next,…Management Information Base (MIB) – V1, V2 and V3, RMON - OID notation - OID Trees - SNMP Tools, Case Studies

Unit 3: Log Formats And Log Collection: Log files – Log formats – application specific Log Formats -Apache Logs - Mail logs - Firewall Logs – vendor Specific Logs - Event Correlation - Event Normalization, Correlation Rules Log Collection - Push Log Collection - Pull Log Collection - Prebuilt Log Collection - Custom Log - Parsing/Normalization of Logs - Rule Engine/Correlation Engine - Correlation Engine, Case Studies

Unit 4: Managing Log Files: Log tools – SYSLOG – Open source Log analyzers - Log File Conversion -Standardizing Log Formats - Using XML for Reporting -Correlating Log File Data -Log Rotation and Archival -Determining an Archiving Methodology -Separating Logs, Case Studies

Unit 5: Investigating Intrusions: Intrusion detection system - NIDS, HIDS - Locating Intrusions - Monitoring Logons - Monitoring IIS - Reconstructing Intrusions – concepts of SNORT - Rules - Rule headers - Rule options - Pre- processors - Stream4 - Frag2 - Frag3 - HTTP inspect - plugins - Alerts Detail Report, Case Studies.

TEXT BOOKS

1. David Miller, Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2010
2. Client P Garrison, Digital forensics for network internet and cloud computing, , Elsevier, 2010
3. Jacob Babbin et al, Security Log Management-Identifying patterns in chaos, Syngress, 2006
4. Vivek Chopra, et al, Professional Apache Tomcat, Wrox, 2004

5. Gabriele Giuseppini, et al, Microsoft Log Parser Toolkit, Syngress, 2004
6. Toby Kohlenberg, Snort IDS and IPS toolkit, Syngress, 2007
7. Al-Sakib Khan Pathan, The State of the Art in Intrusion Prevention and Detection, CRC 2014
8. John R.Vacca, Scott Ellis, Firewalls Jumpstart for Network and Systems Administrators, Elsevier,2005.

CSP232	Project	L T P C 0 0 6 3
Goal	Develop the mini project by using Cyber Forensics Techniques	

Objective:	**Outcome :**
• Develop a mini project using Cyber Security Management Techniques	• Ability to Manage Cyber Security Challenges

CSP233	Case Studies	L T P C 0 2 0 2
Goal	Do a Case Studies on Cyber Security Management	

Objective:	**Outcome :**
• Do a Case Study on Cyber Security Mangement	• Ability to Analyze the Cyber Security Cases.