Professional Diploma in Cyber Security Management

Curriculum and Syllabus
2020

(Applicable to the students admitted from the Academic year 2020 onwards)

INSTITUTE OF TECHNOLOGY MANAGEMENT & RESEARCH

(Division of Mamta Trust)

2/850, Mugalivakkam Main Road, Mugalivakkam, Chennai – 600 125

Eligibility Criteria for this program

TO be filled up

Enrollment process:

1. Filled up applications are received for scrutiny
2. All applicable eligibility credentials are validated (Graduation, proof of employment , proof of experience as defined in eligibility criteria)
3. 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.

Codification:

The codification of the courses of this program will be in consonance with the existing codes for similar subjects and for all other courses, they will be defined de novo.

INSTITUTE OF TECHNOLOGY MANAGEMENT & RESEARCH

Diploma in Cyber Investigations & Laws

CURRICULUM 2013-2014

Sl. No	Course Code	Course Title	L	T	P	C	TCH
SEMESTER I							
Theory							
1.		Cyber Risk Management	3	0	0	3	3 45
2.		Information System Audit Management	3	0	0	3	3
3		Infrastructure Penetration Testing Management	3	0	0	3	
4.		Remote Infrastructure Management	3	0	0	3	4
5.		SIEM & log trails	3	0	0	3	3
Practical							
6.		Forensics lab	0	0	4	2	2
7.		Project	0	0	7	4	4
		Total Credits					23

	Cyber RISK Management	L T P C 3 0 0 3
Goal	To introduce the principles of Cyber Risk management and expose the 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 locations of electronic 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 cyber crime, tools 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

	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

	FORENSICS LAB	L T P C 0 0 4 2
Goal	To understand the use of tools to manage forensics and system and application level vulnerability	

Objective:	**Outcome :**
1. Understand the technique of collecting live forensic information 2. Understand the use of disk forensic tools 3. Understand the use of mobile forensic tools 4. Understand the use of Network forensic tools	1.Exhibit live forensic data collection 2.Exhibit the use of disk forensic tool to collect and manage evidence 3.Exhibit SIM data collection techniques 4. Use network tools to collect VA and exploits data

1. Use NMAP as your tool and try out the various scan types with different flag combinations. With a single IP address and multiple IP address combinations.

2. Load a single IP address in Nessus and carry out a light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Extend the exercise for a range of addresses in Nessus and repeat the light scan, and intensive scan of the identified machines. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Also list out the block range of Filters available for SCAN as a part of your report

3. Load a single IP address in OPENVAS and carry out a light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Extend the exercise for a range of IP addresses in OPENVAS and repeat the light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Also list out the block range of Filters available for SCAN as a part of your report.

4. Use the password cracker tool (**SALT** or equivalent) and with a given encrypted / or shadowed password file, try to identify the username and the respective passwords.

5. Using Wireshark as a tool capture the network traffic and reconstruct the data flowing through the network for an Identified HTTP traffic.

6. Using Wireshark as a tool, load an captured pcap file and analyse the same with respect to given problem. Isolate the evidences from the captured traffic file, construct a forensic report describing the incidents in a time line view.

7. Live Forensics: Identify the following details from the target machine using live analysis tool. List loaded programs, List current network connections, List running processes, List open share files, list of routing table entries, list of ARP entries.

8. Using Nikto as a web application analysis tool, scan a given website for web vulnerabilities at the web server level and the application level

9. Using Wapiti as a web application analysis tool scan a given website for web vulnerabilities at the web server level and the application level

10. For a given email header, carry out the header analysis, identify the domains, and reconstruct the mail traffic flow from the sender to the receiver. Differentiate between internal and external IP addresses if available in the header and try to reconstruct the network.

11. In a given machine Identifiy the list of visited websites with respect to Internet explorer and Firefox. Generate the output as a timeline entry. Mark observed deviations in browsing based on the timeline and describe the person's activity at that point in time.

12. Take a USB stick which has a few jpeg images. Delete a few JPEG images. and create an disk image of USB. Mount the disk image and using Scalpel tool retrieve the deleted images.

13. With a sample apache attack log, analyse the shared log and try to identify the attacker along with the steps in identifying the method of entry.

14. For the given Asset inventory, identify the threat and risk matrix and hence calculate the exposure risk for the shared assets. Propose a risk mitigation plan.

15. With the given windows system, use a suitable disk explorer tool and identify the directory structure and windows specific hidden file locations especially, the event and security log entry locations and system32 locations with file size entries,

16. With the given windows system, identify the various registry entries and generate a report on the current configuration and current user permissions. With the given configuration and the permissions, try to reconstruct the users, and their privileges.

17. **Demonstration only**: Load a SIM card and analyze the various folders available as a part of the SIM.

DCE 207 Project

As per university Guidelines