NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

STANDARD OPERATING PROCEDURE
(SOP)

Identification of PPP (Public-Private-Partnership) entities for partnership with NCIIPC and formulation of training requirements along-with guidelines for conducting training

Mar 2020

NCIIPC, Block-III, Old JNU Campus
New Delhi-10067

Table of Contents

Abbreviations

BFSI	Banking, Financial Services and Insurance
CERT- In	Computer Emergency Response Team - India
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
DeitY	Department of Electronics & Information Technology
DoT	Department of Telecommunication
IB	Intelligence Bureau
ICS	Industrial Control Systems
IDRBT	Institute for Development & Research in Banking Technology
IR	Incident Response
ISGF	India Smart Grid Forum
MoU	Memorandum of Understanding
NCIIPC	National Critical Information Infrastructure Protection Centre
NIIT	National Institute of Information Technology
OEM	Original Equipment Manufacturer
ONGC	Oil and Natural Gas Corporation
PPP	Public-Private-Partnership
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operation Centre
STQC	Standardisation Testing and Quality Control

1. Introduction

1.1. Developing and organising training and awareness programs is an important function assigned to NCIIPC. Keeping in mind the diversity of sectors, organisations and training requirements in Government and also the private & public sector organisations, NCIIPC needs to identify key PPP (Public-Private-Partnership) entities for partnership and formulating training requirements and undertaking training relevant to their area of operations.

1.2. To facilitate the above, a subgroup was constituted during the first NCIIPC Advisory Board Meeting, held on 11th December 2015. The subgroup included members from Ministry of L&J (Law and Justice), DoT (Department of Telecommunication), IB (Intelligence Bureau), MeitY (Ministry of Electronics & Information Technology) and NCIIPC. The subgroup was required to frame a SOP for "Identification of PPP for partnership with NCIIPC and formulation of training requirements along-with guidelines for conducting training".

2. Objective

This document provides standard operating procedure for identification of PPP entities for partnership and formulates training requirements and guidelines for conducting training for all stakeholders.

3. Identifying PPPs for partnership with NCIIPC

3.1. Broad parameters for identification of the partner agency/organisation for entering into a PPP are:

3.1.1. The organisation must be actively engaged in Information Security formulation/ implementations/ management in a CII Sector, and/or must be recognised by the concerned Ministry. Sectoral Institutions such as Institute for Development & Research in Banking Technology (IDRBT) in BFSI (Banking, Financial services and Insurance), India Smart Grid Forum (ISGF) in Power Sector, Forums/ Institutions under Department of Telecommunication (DoT) etc, would be given priority for engaging with PPP partnerships.

3.1.2. The organisation must organically possess the requisite skill set with minimum three years of experience in providing such training course and not perform outsourcing of manpower for conduct of training.

3.1.3. The organisation under consideration must not be blacklisted by any

Government agency or authority.

3.2. Some suggested organisations include:

3.2.1. Government R&D organisations such as Centre for Development of Advanced Computing (C-DAC).

3.2.2. Eminent Government recognised Universities.

3.2.3. Renowned Private Institutions.

3.2.4. Leading ICS/ SCADA OEMs and major public sector organisations such as Powergrid and ONGC.

3.2.5. Selection of private Institutions/ organisation could be made in consultation with IB and CERT-In.

To identify a PPP for partnership with NCIIPC, operating procedures mentioned in subsequent paragraphs shall be followed.

4. PPP Proposals

4.1. To identify suitable PPPs across critical sectors, NCIIPC Sectoral Coordinators, including Incident Response (IR), Security Operation Centre (SOC), and Research and Development units shall submit their PPP engagement proposals to NCIIPC for examination and approval.

4.2. The PPP proposal shall comprise:

4.2.1. Details of proposed PPPs.

4.2.2. Description of proposed partner such as qualification and experience.

4.2.3. Expertise and skill- set such as certification level of instructors.

4.2.4. Demonstrated experience in delivery of similar trainings.

4.2.5. Demonstrated experience in working with public agencies.

4.2.6. Capacity to deliver the required quantity and quality of training/ services.

4.2.7. Training proposals.

4.2.8. Proposed timelines for the training.

4.2.9. Training requirements of the sector along with desired qualification of the trainees.

4.2.10. Formulation of short term, mid-term and long-term engagements.

4.2.11. Budgetary requirements.

4.2.12. Manpower and Infrastructure Requirements.

4.2.13. Additional resources and capacity (If any).

5. Assessments of PPP Proposals by Competent Authority

NCIIPC shall assess the proposals submitted by the Sectoral Coordinators and other NCIIPC Units for correctness, completeness, and feasibility. Further, in order to optimise, projects redundant or similar in nature may be merged by the Competent Authority.

6. Signing of Memorandum of Understanding (MoU)

A MoU shall be signed between NCIIPC and the PPP. The MoU shall outline the sections as mentioned at **Appendix 'A'**.

7. Steering Committee

NCIIPC shall constitute a Steering Committee for each PPP partnership. The Steering Committee shall be headed by the concerned Sectoral Coordinator and shall provide guidance, direction and control to the project and monitor progress or outcomes. Steering Committee shall have five members in total with members from NCIIPC, CERT-In and STQC along with two co-opted members to be nominated by DG NCIIPC. Secretariat support shall be provided by NCIIPC.

8. Training requirements and guidelines for Critical Sectors

8.1. Training Requirements

8.1.1. NCIIPC Training Curriculum

The training curriculum shall be aimed to train the Middle Level Management, Senior Level Management and Chief Information Security

Officers (CISOs) about Critical Information Infrastructure Protection, Information Security & Policies, Cyber Security, Vulnerability/ Threat/ Risk Analysis, Incident Management & Handling, Cyber Audit etc. The training curriculum is placed at **Appendix 'B'**.

8.1.2. Sector Specific Specialised Training

NCIIPC sectoral coordinators shall submit their sector specific specialised training requirements to Competent Authority. This process may be included in the PPP identification process as explained above.

8.2. Training Guidelines

8.2.1. CISO Training

For conducting the above training critical sector organisations may contact NCIIPC. NCIIPC, in turn may organise training in partnership with PPPs as described in paragraphs above.

However, the critical sector organisation may also organise the NCIIPC CISO Training Curriculum by hiring training entities suitable to their organisational needs. For example, an organisation may include the NCIIPC CISO Training Curriculum in its annual training plan and select a training provider on its own.

8.2.2. NCIIPC Workshops/Trainings

In addition to above, NCIIPC shall also regularly organise workshops/ trainings for critical sector CISOs.

8.2.3. Certifications

The trainings may be followed by an exam or test, subsequent to which NCIIPC may provide certification to the trainees.

9. Review

Present SOP shall be reviewed whenever there is a requirement of an update.

Appendix 'A'

Outline of Memorandum of Understanding (MoU)

1. Preamble of the project
2. Scope
3. Steering Committee
4. Intellectual Property Rights
5. Representations and Warranties
6. Confidentiality and Announcements
7. Term and Termination
8. Governing Law, Arbitration and Jurisdiction
9. Notice
10. Miscellaneous

Appendix ‘B’

NCIIPC Training Curriculum

1. NCIIPC Training Curriculum is aimed at providing awareness to senior, middle-level and operations management personnel and cyber security specialists about Critical Information Infrastructure, Information Security & Policies, Cyber Security, Vulnerability/ Threat/ Risk Analysis, Incident Management & Handling, Cyber Audit etc.

2. The training curriculum is divided into three parts as under:

	Course Type	Duration	Remarks
A	**Executive Trg**		Targeted towards Executive, senior and middle level leadership/ management personnel (non-technical/ functional/ generalists) from ministries, regulating bodies, ISSCs and CISOs of CII organisations, who are responsible for Information Security governance and functional oversight on cyber security. Objective of training is to help them understand various dimensions of cyber security, viz, cyber risk assessment, threat modelling, risk management frameworks, ISMS frameworks, incident response, and information governance. May also cover cyber-hygiene aspects for an organisation, infosecurity SOPs & processes, classification and management of digitalised data and documents.
	For CISOs, Middle & Senior level Management	Conducted in 2 parts: Core - 2 working days (4 + 3 hrs) Supplementary - 2 working days (4 + 4 hrs) Training will be done through lectures & case studies, interactions with info & cyber security domain and subject matter experts	
B	**Technical Trg**		Targeted towards Info Security technical & operational management personnel, viz, CISOs & ISMS teams of Govt owned/ Private CII orgs, departmental Info Security administrators, who are responsible for cyber security architecture design & review, ISMS implementation and management, SOC operations (both internal and third-party SOCs/ MSSPs), internal infosec audits, incident response. Objective of training is to help them understand the design, implementation and operation of infosec functions, ISMS frameworks & technologies in an organisation, SOC operations, technical & process oversight on third party SOCs/ MSSPs, audits, incident response functions. Training to also cover tools & techniques for cyber protection, CVE, STIX, TAXII analysis, secure coding, cyber-hygiene aspects, cyber SOPs and processes.
	For Technical & Operational Management personnel, and ISMS teams	Conducted in 2 parts: Core - 3 working days (21 hrs) Supplementary - 3 working days (21 hrs) Training will be done through lectures, demos, hands-on labs, interactions with technical and subject matter experts	

C	**Specialist Trg**		Targeted towards cyber security specialist personnel carrying out deep cyber-technical functions. Objective of training is to help them develop specialized skills in specific areas such as malware analysis, reverse engineering, open source tools and technologies, programming, machine learning, AI, forensics, threat modelling, threat intelligence, threat hunting, cryptography, CVE/ STIX/ TAXII analysis.
	For Cyber Security specialist personnel	Conducted in one part over 5 days Training will be done through lectures, demos, hands-on labs, interactions with technical and subject matter experts on any one of following topics(a) Power (b) Transport (c) Telecom (d) Banking (e) Any other Topic	

3. Criteria for nomination of candidates for the training sessions are as follows:

Executive Training for CISOs, Middle & Senior level Management

Designation: Executive Director, Director, CXO, General Manager, Additional General Manager, Deputy General Manager, CISO, Deputy CISO, Heads of Business and Operations, Director/ Joint Secretary and above from Government organisations.

Experience: At least 15 years management experience.

Technical Training for Technical & Operational Management personnel, and ISMS teams

Designation: Deputy General Manager and below, responsible for technical, operational and information security functions involving IT, OT & IS systems, Director and below from Government organisations.

Experience: At least 5 years in the relevant technical or functional area.

Specialist Training for Cyber Security Specialists

Designation: Not Applicable

Experience: Candidates will be selected through a psychometric capability testing process, in order to assess whether they have the required mindset for the proposed job role. Trg PPP partners will incorporate the same in their candidate selection process.

Course Content

A	Executive Trg (Core)	PPP Course Content		
	Module and Name	**Objectives**	**Duration (hrs)**	**Remarks**
	Module 1 – Overview of Information Security	Understanding Information Security	1 hr	
		Why Care About Security?		
		Understanding techniques to enforce IS in an organization		
	Module 2 – Overview of Security threats	Overview of Information Security Threats	1 hr	
		Types of threats – DDoS, Malicious codes, Espionage, etc		
		Identification of Threats		
		Modus Operandi		
		Sources of Threats		
		Best Practices or Guidelines used to Identify Threats		
		Best Practices or Guidelines used in mitigation of threats		
		Collaborate with peers and experts through different forums to understand contemporary issues and solutions		
	Module 4 – Risk Management	What is Risk?	1 hr	
		Relationship between Threat, Vulnerability& Risk		
		What Is the Value of an Asset?		
		What Is a Threat Source/Agent?		
		What Is a Control?		
		Risk Management		
		Different Approaches to Risk Analysis		
		Best Practices and Guidelines in Assessing and Calculating Risks		
		Develop and implement policies and procedures to mitigate risks arising from ICT supply chain and outsourcing.		
		Best Practices and Guidelines in Mitigating Risks.		
		Governance, Enterprise Risk Management, Proactive Risk identification & Management		
	Module 27 - Identification of Critical Infrastructure	What is “Infrastructure”?	1 hr	
		“Critical” Infrastructure and “Key Resources”		
		Differentiating Critical and Non-Critical “Assets”		
		Challenges Identifying Critical Assets		

		Critical Infrastructure		
		Policy Issues		
	Module 25 - Information Security Policy and Procedures	Understanding Security Frameworks	2 hrs	
		Security Standards		
		Understanding organizational requirements from an information security point of view		
		Security Policy, Procedures, and Practices		
		Develop information security policies and procedures		
		Implement information security policies and procedures		
		Collaborate with other departments within the organization for effective implementation of security provisions.		
		Understand the organization and individual behaviours for information security		
		Update and upgrade Key Performance Indicators for security implementation		
		Best practices and Guidelines in developing information security policies and procedures		
	Module 31 – Senior Management support to Critical Information Infrastructure Protection	Support security within the organization through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities	1 hr	
		Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.		
		Directing and supporting persons to contribute to the effectiveness of the information security management system.		
		Top management shall establish an information security policy.		
		Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.		
	Total Duration		**7 hrs**	
A	**Executive Trg (Supplementary)**	**PPP Course Content**		
	Module and Name	**Objectives**	**Duration (hrs)**	**Remarks**

	Module 17 - Business Continuity Plans	Need of BCP	1 hr	
		BCP standards and frameworks		
		Who Is Ready?		
		Pieces of the BCP		
		BCP Development		
		BCP Risk Analysis		
		Determining backup strategy		
		What Items Need to Be Considered in a Recovery?		
		BCP Plans Creation, Reviews, and Updates		
	Module 18 - Disaster Recovery Planning	Proper Planning	1 hr	
		Backup/Redundancy Options		
		Recovery Strategy		
		Recovery		
		Testing and Drills		
	Module 19 - Incident Management and Handling Process	Seriousness of Computer Incidents	1 hr	
		Incidents Management		
		Triage		
		Incident Notification and Communication		
		Guidelines for handling security Incidents		
		Role of CERT in case of Incident		
	Module 20 - Third Party Management	Need for Third Party Management	1 hr	
		Identification and management of Third Party Risks		
		Categorization of Third Parties Based on Risk Perception		
		Controls for Mitigating Third Parties Risks		
		Security Considerations when Procuring Services and Products from Third Parties		
		Auditing of Third Parties		
		Best Practices and guidelines for managing Third Party Risks		
	Module 21 - Legal Framework	Need for Legal Framework and its enforcement	1 hr	
		Types of Law		
		Historic Examples of Computer Crimes		
		IT (Amendment) Act 2008		
		National Cyber Security Policy Identification Protection & Prosecution		
		Role of Evidence in a Trial		
		Privacy of Sensitive Data		
		Sets of Ethics		

		GAISP- Generally Accepted Information Security Principles		
	Module 22 - Privacy Protection	Understanding Privacy as a Domain	1 hr	
		Relationship between security and privacy		
		Revitalizing security program to enable Privacy Protection		
		Assess privacy implications of security technologies		
		Privacy impact assessment		
		Develop and implement privacy protection measures within the organization		
	Module 23 - Audit and Testing	What is Information Security Audit?	1 hr	
		Importance of Information Security Audit		
		Identifying the Information Security Audit Objectives		
		Audit Planning and preparations		
		Performing Security Audits and Reviews		
		Vulnerability assessment and Penetration testing		
		Code reviews		
		Audit Controls		
		Logical security audit		
		Ethics and codes of conduct for Auditors		
		Security Policies and Procedure Audits and Compliance Audits		
		Conduct and Close internal audits		
		Information Security audit tools		
		Reporting to senior management on defined parameters		
	Module 24 - Computer Forensics	What is Computer Forensics?	1 hr	
		What are the benefits of Computer Forensics?		
		Legal Aspects of Computer Forensics		
		Role of Computer Forensics in collection of evidence in Cyber Crimes		
		Digital Evidences		
		Spoliation and Data Fraud Cases		
		Understanding Digital Forensic Process and Procedures		
		Understanding Computer Forensic investigating and analysis procedures, techniques, and tools		
		Total Duration	**8 hrs**	

B	**Technical Trg (Core)**	**PPP Course Content**		
	Module and Name	**Objectives**	**Duration (hrs)**	**Remarks**
	Module 1 – Overview of Information Security	Understanding Information Security	1 hr	
		Why Care About Security?		
		Understanding techniques to enforce IS in an organization		
	Module 2 – Overview of Security threats	Overview of Information Security Threats	2 hrs	
		Types of threats – DDoS, Malicious codes, Espionage, etc		
		Identification of Threats		
		Modus Operandi		
		Sources of Threats		
		Best Practices or Guidelines used to Identify Threats		
		Best Practices or Guidelines used in mitigation of threats		
		Collaborate with peers and experts through different forums to understand contemporary issues and solutions		
	Module 3 – Information Security Vulnerabilities	Why do Information Security Vulnerabilities exists	2 hrs	
		Understanding Security Vulnerabilities		
		Understanding Vulnerability Assessment Tools and Techniques		
		Techniques to Exploit Vulnerabilities		
		Techniques to Fix the Vulnerabilities		
		Best Practices and Guidelines to mitigate security Vulnerabilities		
	Module 4 – Risk Management	What is Risk?	2 hrs	
		Relationship between Threat, Vulnerability& Risk		
		What Is the Value of an Asset?		
		What Is a Threat Source/Agent?		
		What Is a Control?		
		Risk Management		
		Different Approaches to Risk Analysis		
		Best Practices and Guidelines in Assessing and Calculating Risks		
		Develop and implement policies and procedures to mitigate risks arising from ICT supply chain and outsourcing.		

		Best Practices and Guidelines in Mitigating Risks.		
		Governance, Enterprise Risk Management, Proactive Risk identification & Management		
	Module 8 - Understanding Security Architecture and Technologies	Access Control Administration	3 hrs	
		Accountability and Access Control		
		Security Features and Implications of technology solutions		
		Security Technologies and Techniques		
		Defense in Depth Security Model		
		Understanding of technology solutions deployed by the organization (servers, applications, databases, OS, routers, switch, etc.)		
		Hardening of IT and security solutions		
		Improving Security		
		Design, implement, and maintain security architecture of the organization		
		Best Practices and Security Guidelines		
		Creation of DMZ Zones for servers		
	Module 11 - Focus on Malware, viruses and how they subvert security	Types of Viruses & Malware	1 hr	
		Potential threats, Emerging class of Malware		
		Means of Propagating		
		Protection Measures		
		Special attention to critical infrastructure systems		
	Module 12 - Operations Security	Operations Issues	3 hrs	
		Specific Operations Tasks		
		Fault-Tolerance Mechanisms		
		Backups		
		Facsimile Security		
		Email Security		
	Module 15 - Cloud Computing and Security	Introduction	3 hrs	
		IAAS		
		PAAS		
		SAAS		
		Public Cloud		
		Private Cloud		
		Hybrid Cloud		
		Components of Cloud Computing		
		Understanding Network and security in Cloud		

		Understanding Data, Application, and Service Control and Ownership in Cloud		
		Security issues for Clouds		
		Legal and jurisdictional challenges		
		Evaluating security of cloud service providers		
		Standards and frameworks for security and privacy in the cloud		
		Resource scheduling		
		Third party secure data publication applied to cloud		
		Data and information Control Issues and Vulnerabilities		
		Security Compliance for Cloud Computing		
		Encrypted data storage for cloud		
	Module 19 - Incident Management and Handling Process	Seriousness of Computer Incidents	2 hrs	
		Incidents Management: Determine the IRP of your organisation, gather the right stakeholders to create a program, the six phases of IRP, how to remain creative during the IRP process, write an IRP for (part of) your organisation		
		Triage		
		Incident Notification and Communication		
		Guidelines for handling security Incidents		
		Role of CERT in case of Incident Coverage includes: Why is an Incident Response Plan (IRP) essential for your organisation? How do you write an IRP? Which phases are included in the plan? Why is it important to connect the different stages of security maturity? How can you increase the effectiveness of an IRP? How do you ensure an adequate and efficient workflow of reported weaknesses? Developed competencies and learning outcomes: • Participant understands how response teams should deal with reports sent in by ethical hackers under Responsible Disclosure • Participant knows how to act as a consultant Operational Risk Control • Participant can set up specific elements of the IRP for the application team • Participant knows how to test an IRP (procedure and implementation)		
	Module 25 - Information Security	Understanding Security Frameworks	2 hrs	
		Security Standards		

	Policy and Procedures	Understanding organizational requirements from an information security point of view		
		Security Policy, Procedures, and Practices		
		Develop information security policies and procedures		
		Implement information security policies and procedures		
		Collaborate with other departments within the organization for effective implementation of security provisions.		
		Understand the organization and individual behaviours for information security		
		Update and upgrade Key Performance Indicators for security implementation		
		Best practices and Guidelines in developing information security policies and procedures		
	Total Duration		**21 hrs**	
B	**Technical Trg (Supplementary)**	**PPP Course Content**		
	Module and Name	**Objectives**	**Duration (hrs)**	**Remarks**
	Module 5 - Network Protocols and Devices	OSI Model	4 hrs	
		Data Encapsulation		
		OSI Layers		
		Protocols at Each Layer		
		Devices Work at Different Layers		
		Networking Devices		
		Firewall – First line of defense		
		Firewall Types		
		Firewall Placement		
		Firewall Architecture Types		
		IDS – Second line of defense		
		IPS – Last line of defense?		
		Host-based Intrusion Protection System		
		Network Service		
		VLAN concept in switch		
		Static and Dynamic Routing		
		Securing Internetworks using ACLs		
	Module 6 -	Introduction to Directory Services	4 hrs	

	Understanding Directory Services	Benefits of DS in a network		
		DS implementations in different Operating Systems		
		Introduction to Active Directory		
		Logical structure of Active Directory		
		Physical structure of Active Directory		
		Creating Domain		
		Creating Additional DC and Read Only DC		
		Understanding trees and forest		
		Creating and managing Global Catalog Servers		
		Understanding Sites and Securing domain/ network through sites		
		Organizing resources in OU		
		Understanding Users and Groups concepts		
		Groups and their rights		
		Assigning permissions to users using group membership		
		Securing environment using Local and Domain Group policies		
		Group policies object and Group policy templates		
		Inheritance of group policies		
		Execution of Group Policies		
		Backup and Restoration of AD		
	Module 7 - Access Control	Access Control Administration	4 hrs	
		Accountability and Access Control		
		Trusted Path		
		Who Are You?		
		Authentication Mechanisms		
		Strong Authentication		
		Authorization		
		Access Criteria		
		Role of Access Control		
		Control Combinations		
		Accountability		
		Types of Classification Levels		
		Models for Access		
		MAC Enforcement Mechanism – Labels		
		Rule-Based Access Control		
		Remote Centralized Administration		

	Module 9 - Understanding Cryptography, Tunnelling, and Wireless Security	Cryptography	3 hrs	
		Use of certificates in authentication, encryption, and e- commerce		
		What Is a Tunnelling Protocol?		
		Wireless Technologies – WAP		
		Software Engineering and System Survivability		
	Module 10 - Securing your Database	Database Security Issues	2 hrs	
		Redundancy and availability of Database		
		Types of attacks		
	Module 13 - Software Development Security	How Did We Get Here?	2 hrs	
		Issues in application security (SQL injection, cross scripting, etc.)		
		Security in SDLC		
		Modularity of Objects and Security		
		Security of Embedded Systems		
		Common Gateway Interface		
		Virtualization		
		How to develop secure applications; Application security design, architecture and design software, quality assurance techniques, secure coding standards, Threat risk modelling		
	Module 14 - Physical Security	Physical Security – Threats	2 hrs	
		Different Types of Threats & Planning		
		Entrance Protection		
		Perimeter Protection		
		Surveillance/Monitoring		
		Types of Physical IDS		
		Facility Attributes		
		Fire Prevention		
		Physical Security Compliance and Auditing		
		Convergence of physical and logical security		
	Total Duration		**21 hrs**	
	Module 16 – Securing Industrial Control Systems Additional Module for CII Organisations and Personnel handling OT	ICS Characteristics, Threats and Vulnerabilities.	4 hrs	
		ICS Security Program Development and Deployment.		
		Network Architecture.		
		ICS Security Controls.		

C	Cyber Security Specialist Trg	PPP Course Content		
	Module and Name	**Objectives**	**Duration (hrs)**	**Remarks**
	Module – Introduction to Ethical Hacking	Definitions of hacking	7 hrs	
		Hacker tools		
		Process hacker		
		'Do it yourself' (using hacker tools)		
		Methods for intrusion detection		
		Dealing with ethical hackers and Responsible Disclosure Coverage includes: What is ethical hacking? How to communicate with hackers and how do they communicate amongst themselves? What is the Darknet? What software can be used? How do you recognize a hack? How do you hack and what tools are available? Developed competencies and learning outcomes: • Participant can create a penetration testing application • Participant can give advice in outsourcing penetration tests • Participant can indicate the stack deployment of an application on all levels • Participant can perform hacks on the internal environment and to test the conditions on how to implement a robust and secure application • Participant can test the mitigation of applications from technical software specialists against hackers		
	Module 11 - Deep Malware analysis		14 hrs	
	Module 28 - Vulnerability/ Threat/ Risk Analysis	**Vulnerabilities**	14 hrs	
		o Technology weaknesses		
		o Configuration weaknesses		
		o Security policy weaknesses		
		Threats		
		o Unstructured threats		
		o Structured threats		
		o External threats		
		o Internal threats		
		Attacks		
		o Reconnaissance		

		o Access		
		o Denial of service		
		o Worms, viruses, and Trojan horses		
		Vulnerability Analysis		
		o Policy identification		
		o Network analysis		
		o Host analysis		
		Vulnerability-Threats Assessment for Enterprise Network		
		Threat and risk assessment/ analysis		
		Risk Assessment/ Analysis		
		o Identifying Potential Risks to Network Security		
		o Asset Identification		
		o Vulnerability Assessment		
		o Threat Identification		
		o Open Versus Closed Security Models		
		Risk evaluation - relationships - most critical assets, and threats - assets and the vulnerability impacts		
		Threat and risk assessment/ analysis		
		o Identify the safeguards to be adapted to maintain confidentiality		
		Network security integrity strategy		
		o Identifying the areas of greatest risk and concentrate on those triggers like Trojan horses, viruses, and malwares		
		Risk Assessment Framework		
		o The Concepts of Return on Investment		
		o Botnets Propagation Mechanism		
		o Vulnerability Access Control		
		o Estimating Risk and Return on Investment		
		The Emergence of Threats on Enterprise Network Information Systems		
		o Threats and the Vulnerabilities		
		o Network Exploitation		
		o Client – Side and Client to Client Exploitation		
		o Governance, Enterprise Risk Management, Proactive Risk identification & Management		
		Analysis Tools		
		Total Duration	**35 hrs**	