NiSM राष्ट्रीय प्रतिभूति बाजार संस्थान
National Institute of Securities Markets
(An Educational Initiative of SEBI)

www.isea.gov.in

Certificate Course on

CYBER SECURITY FOUNDATION

Supported by:

certin
Enhancing Cyber Security in India

Ministry of Electronics and Information Technology,
Government of India

NATIONAL INSTITUTE OF SECURITIES MARKETS

Index

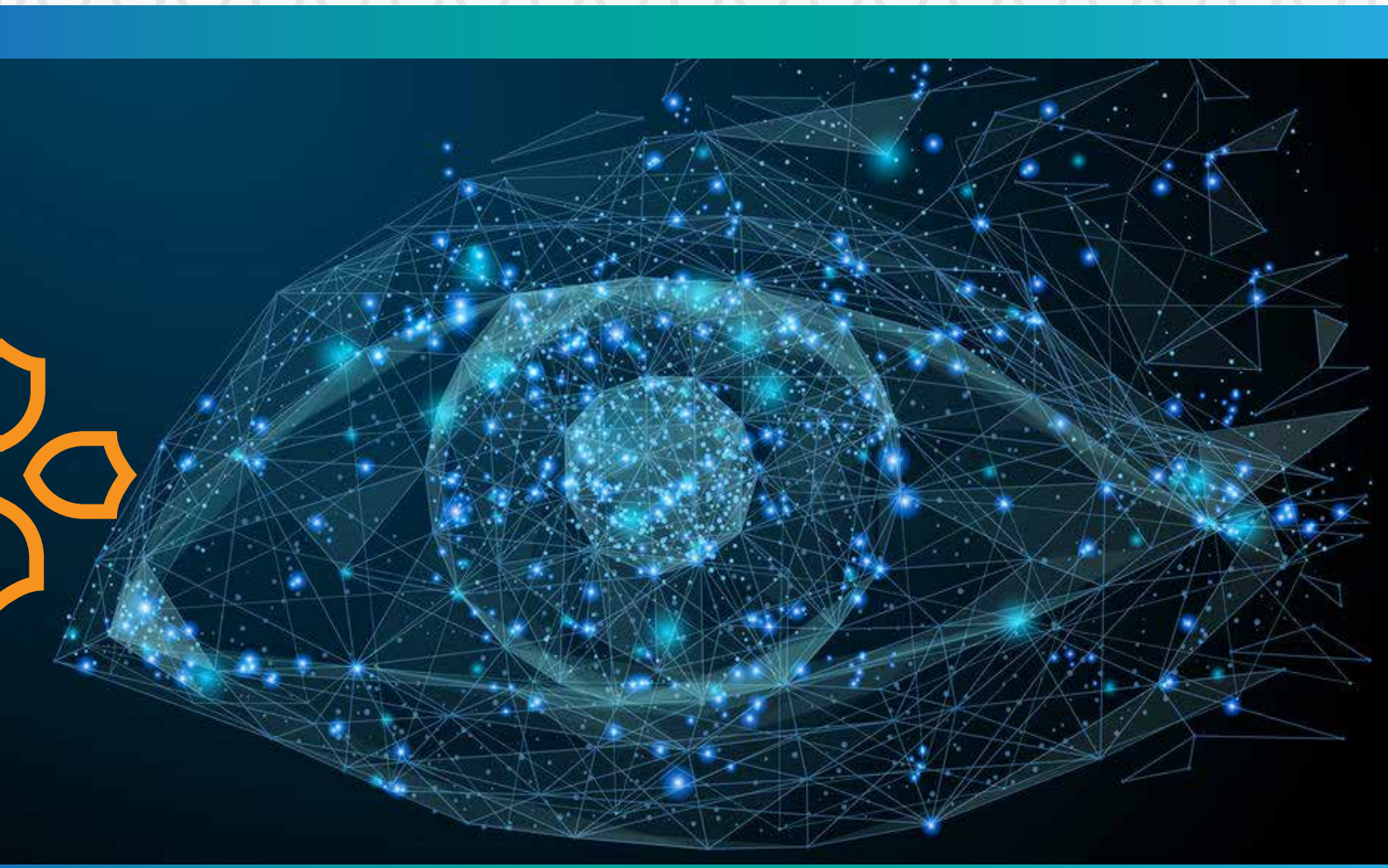
01	About The Course	04
02	Who Should Take This Course?	06
03	Fee Structure	06
04	Learning Mode	06
05	Examination	06
06	Course Content	07
07	Module I: Cyber Security basics for IT/ICT environment	07
08	Module II: Information Security Policies, Procedures and Guidelines	09
09	Module III: System and Network Security Concept	11
10	Module IV: Information Security Audit and Assessments	12
11	About NISM, ISEA, CERT-In / CSIRT-Fin, C-DAC, and MeitY	13

The Digital world is growing in leaps and bounds and every industry including the Financial Industry is embracing it to create integrated solutions to make smooth customer experience from onboarding to Delivery of Services.

Digital Technology, while is very convenient and efficient, is fraught with cyber security risk. During the Covid affected days, mutual funds, broking firms, Market Infrastructure Institutions (MIIs)(stock and commodity exchanges, depositories and clearing corporations) which together manage countries financial wealth, which is more than our GDP and still growing have adapted digital platforms for their business transactions. While such digital platforms are very convenient to the investing public, intermediaries and MIIs, it is necessary to ensure financial security of investors, integrity of the transaction (ie., value in the transaction reaches the transacting entities and not anyone else) and prevent their identity theft on the web.

In addition to the securities markets (capital market) intermediaries, listed companies, insurance companies, banks – scheduled commercial banks and even new generation banks like urban banks, cooperative banks, payment banks, electronic wallets, etc all use internet platforms regularly for all their transactional needs. As these institutions play critical role in financial wellbeing of our country, they need to protect themselves from cyber-attacks - a new form of 'terrorism' which can come from any part of the world. The increased use of Digital medium also comes with the challenges of preventing and saving organizations from potential cyber threats.

Cyber Security has emerged as an important thread in every organization IT infrastructure management. To understand the various concepts and challenges of Cyber Security management for the firms involved in Financial Domain, NISM is elated to launch an online course in "Cyber Security Foundation" in collaboration with NISM, ISEA, CERT-In / CSIRT-Fin, C-DAC under the aegis of Ministry of Electronics and Information Technology (MeitY), Government of India.



About The Course

Cyber Security management is not a one-time event but a continuous process – it is not a project but a journey. Being aware of cyber security issues, challenges, methods to preserve Data Integrity is the first step and most important step in ensuring cyber security.

To address this important requirement of Cyber Security, NISM, jointly with CERT-In / CSIRT-Fin and C-DAC under the initiative of ISEA (Information Security Education and Awareness) Project by MeitY (Ministry of Electronics and Information Technology), Government of India is offering a self-paced eLearning certification course, which will focus on identifying the gaps in cyber security and develop a robust Cyber Security Framework based on the pillars – Identify, Build Mechanisms, Detect, Respond and Recover.

This course offers approx. 60 hours of learning through video lectures, presentation of case studies and text material for reference (in soft form); candidates who participate in this programme will be issued a joint certificate by NISM, ISEA, CERT-In / CSIRT-Fin, C-DAC, and MeitY once they clear a proctored test after learning the content using the self-paced eLearning material.

In addition to the basic conceptual knowledge about the cyber security pillars stated above, the course also dwells in detail about the cyber security advisory issued by SEBI from time to time. Learning these guidelines will help executives working in SEBI Regulated intermediaries and MII's to learn "what" aspects and "how" aspects of cyber security.

Who Should Take This Course?

This course is ideal for all executives working in any organisation that uses IT platforms for their transactions.

The course would add value to the professionals working in Banking, Stock Exchanges,, Depositories, Clearing Corporations, Stock Brokers (Cash, Commodity, Currency, Derivatives) Mutual Funds and other intermediaries involved in Securities Markets, Fintech firms, and any other organization which heavily rely on IT infrastructure to deliver their services.

The course is also ideal for Management graduates getting specialization in the field of finance to understand the future challenges of Cyber threats in fintech space.

Fee Structure

In order to encourage all targeted persons to take this test, the fee for this program is kept at very affordable price of ₹ **2,500/-** plus GST per person.

Candidates who have failed to score a minimum of 60% marks in their examination will have to pay ₹ **1000/-** plus GST as applicable, as re-examination fee for their second attempt. A candidate will be given a maximum of 2 attempts to complete the course.

Learning Mode

The Course is designed in an e-Learning mode and the working executives can complete the same at their own pace. Access to course content will be valid for a period of 12 months from the date of registration.

Examination

The Candidate needs to appear for a remote proctored examination after the completion of the course and successful candidates will receive a joint certification from NISM, ISEA, CERT-In / CSIRT-Fin, C-DAC, and MeitY.

Course Content

Module I: Cyber Security basics for IT/ICT environment

Chapter 1: Introduction to Information Security

01	Understand basic cyber security concepts, definitions and its importance
02	Key Information Security Concepts
03	Critical Characteristics of Information
04	Components of Cyber Information Systems
05	Approaches of Information Security
06	Balancing Cyber Security and access
07	Understand basic security architecture principles such as identifying critical assets, CIA, AAA for organization etc., with examples • What is confidentiality and what are threats to it? • What is integrity and what are the two basic principles of integrity? • What are the goals of information security and what is CIA? • Why do we need information security (IS) and what are the three roles in IS? • What are the components of an information system and how do we secure them? • Authentication, Authorization and Accountancy (AAA)
08	Information Assurance (IA) principles - Examples, Case Studies, Assignments and Module Assessment

Chapter 2: Need of Security

01	Business Needs Vs. Cyber Security Implementation • Protecting the Functionality of Organization • Enabling the safe operation of Applications • Protecting the data and information about the data • Safeguarding Technology Assets of an organization
02	Understanding Threats towards organization • Compromises of Intellectual property • Espionage or Trespass • Human errors / failures • Information Extortion • Internal Threats • External Threats etc.
03	Understanding Attacks towards organization • Malicious Activities • Hoaxes • Backdoors • Password Cracks • Man-in- Middle Attacks • Spam • Mail Bombing • Pharming • Timing attacks etc.

Chapter 3: Legal and Ethics of Information Security

01	Law and Ethics of Cyber Security • Organizational Liability and Need for Counsel • Policies Vs. Laws
02	Relevant Indian Laws • IT ACT 2000/2008 amendments • Relevant IPC • Other Laws
03	Ethics and Information Security
04	SEBI Regulatory framework for cyber security.
05	SEBI circulars on Cyber Security and compliance thereof.
06	Systems Audit and audit of cyber security arrangements.
07	Case Studies

Chapter 4: Introduction to Information Security Controls, Models, Standards, Practices and Management Goals.

01	Information Security Management Goals
02	Information Security Models
03	Information Security Standards
04	Information Security Practices
05	Information Security Controls and Implementation Issues • About Information Security Controls and it's their importance • What are Internal Controls and why is costs benefit consideration important? • Why do we need Segregation of information security duties within the systems function? • Access Controls • Why do we need Access control (Physical control)? • What are technical controls or Logical control? • What are identification and authentication and why access control is important? • Why Access Control is important and what are the problems with passwords / options for authentication? • Multi Factor Authentications

Chapter 5: Introduction to Security Systems Development Life Cycle

01	System Vs. Security Systems Development Life Cycle • Introduction to Systems Development Cycle • Introduction to Security Systems Development Life Cycle
02	Application Level Control and Information Security Planning • What are the security controls that can be applied at an application level (at input, processing and output)? • What are the 3 important plans for Information Security? (Security Plan, Backup and Recovery Plan and Disaster Recovery Plan)
03	Security Professionals and Organization
04	Define types of incidents and identify elements of an incident response plan

Module II: Information Security Policies, Procedures and Guidelines

Chapter 6: Information Security Policies, Procedures and Guidelines for Technical, Administrative and Management Staff

01	Information Security Policies, Procedures and Guidelines • Defining about Security Policies, Procedures and Guidelines • Importance of people as a critical asset and roles of HR, Legal, administrative staff in cyber security • Defining and How to establish Cyber Security Organization / Organogram • How do we handle changes to Information security Policy and what is clean desk policy? • Importance of defending incidents by Security Patch management: Policies Procedures and Guidelines • Importance of Cyber Security Practices in establishing Policy • What is SETA and why is it required? • Exercise: Establishing IS Governance structure • Case Study/ Studies: - Design and Development of Cyber Security Policy, - Implementing Process of Policies, Procedures, Guidelines with respect to standards - Introduction to ISMS/ISO 27000, COBIT standards etc. • Introduction to various compliances

Chapter 7: Cyber Security Architecture and Respective Principles

01	Cyber security architecture and respective principles • Identify the key components of cyber security network architecture • What is the overall Framework for management, operational and technical controls? • Introduction about IS Standards and Compliances • How does Defence in Depth and Security Perimeter help with security standards and key components? • What is security analysis? • What is security SDLC, IS Blueprints and some sample policies? • Case Study: Mapping SDLC with organization

Chapter 8: Understanding about Risks, Threats and Vulnerabilities towards Organization

01	An Overview of Risk Management • Know yourself • Know your Enemy

Chapter 9: Describe Risk Management Processes and Practices

01	Risk Identification • Identify the key components of cyber security network architecture • What is the overall Framework for management, operational and technical controls?
02	Risk Assessment
03	Risk Control Strategies
04	Selecting a Risk Control Strategy and Discussion Points
05	Quantitative, Qualitative Risk Control Practices
06	Case Studies: Recommended Risk Control Practices

Chapter 10: Identify the Key Components of Cyber Security Network Architecture

01	Business Impact Analysis for organizations
02	Identifying Critical Assets
03	Continuity Strategies - BCP and DR Concepts • What is a BCP (Business Continuity Plan)? • What is business impact analysis (BIA) / event damage classification and disasters and impact / recovery time? • How do you determine the criticality of business processes and what are RPO and RTO and summary, disruption vs. Recovery Costs and conclusion? • What are high availability solutions and network disaster recovery? • What are the alternative recovery strategies? • What is business continuity process (BCP) and data storage protection? • What is disaster recovery testing and what are the contents of DRP (Disaster Recovery Plan)? • What are the major concerns for a BCP/DR plan and what are the different disaster recovery responsibilities? • What is BCP documents and business continuity overview? • How is MTBF = MTTF + MTTR and what is disaster recovery test execution? • What are the disaster recovery test types, testing objectives, testing procedures, test stages and gap analysis? • Backup Management Concepts - Exercises - Case Studies

Chapter 11: Defining and implementing Policies, Procedures, Guidelines

01	Information Security Planning and Governance • CISO and other Staff • Information Security Organogram / Organization • Information Security Governance
02	Information Security Blue Print - Overview

Chapter 12: Importance of Cyber Hygiene Program

01	Information Security Education
02	Information Security Training
03	Information Security Awareness and Hygiene

Module III: System and Network Security Concepts

Chapter 13: Understanding about security of networks, systems, applications and data

01	Physical Security • Physical Access Controls • Fire Security and Safety • Failure of Supporting utilities and structural Collapse • Interception of Data • Portable, BYOD Security • Other Physical Considerations

Chapter 14: Understanding Hardware and Software Used for Organization for Networking and Cyber Security

01	Security Technology: Introduction to Firewalls, VPNs • Access Controls • Firewalls • Protecting Remote Connections such as VPN, Remote connections etc.
02	Security Technology: IDS, IPS and Other Tools • Introduction and Prevention Systems • Understanding Honey Pots, Honey nets etc. • Auditing and Assessment Tools etc.
03	Security Technology: Cryptography Tools • Foundations of Cryptography • Cipher Methods • Cryptographic Algorithms • Cryptographic Tools • Digital Certificates and Digital Signatures • Understanding Steganography

Chapter 15: Understanding about Various Security Tools and Hardening Techniques of Systems and Network Devices

01	Securing e-mail, Internet Browsers, Instant Messaging and other applications used Department/ Ministry
02	Understanding about proactive, reactive and predictive security devices
03	Importance of Proactive Security
04	Importance of Incident and Forensic Analysis

Module IV: Information Security Audit and Assessments

Chapter 16: Importance of Auditing and Assessing Organization Systems, Networks and Users

01	Understanding Known/Unknown Vulnerabilities and mapping with assets
02	Understanding to analyse threats and risks within the context of the cyber security architecture
03	Importance of assessing systems, networks and users in respective Organizations
04	Understanding critical functions and mapping respective security standards and compliances
05	Defining and understanding concepts of Penetration Testing, Vulnerability Assessment, Auditing and Forensic Auditing

Chapter 17: Distinguish / Understanding about System and Application Security Threats and Vulnerabilities

01	Distinguish / Understanding about system and application security threats and vulnerabilities
02	Application Security Assessment Guidelines

Chapter 18: Types of incidents including Categories, Responses and Timelines for Response

01	Introduction of Incident response and Analysis
02	Types of incidents including categories, responses and timelines for response
03	Incident Reporting Mechanisms
04	Tools used for Incident and Forensic Analysis

Chapter 19: New and Emerging IT and Information Security (IS) Technologies

01	AI/ ML importance
02	Importance of Security over IoT devices
03	Introduction to Dark Web

About NISM, ISEA, CERT-In / CSIRT-Fin, C-DAC, and MeitY

NISM

The National Institute of Securities Markets (NISM) is an educational initiative of the Securities and Exchange Board of India (SEBI). A comprehensive understanding of activities of NISM can be formed by visiting **www.nism.ac.in**. NISM carries out a wide range of capacity building activities at various levels aimed at enhancing the quality standards of and increasing the participation in the securities markets.

ISEA Project, Phase-II

Ministry of Electronics and Information Technology(MeitY), Government India is implementing a project entitled 'Information Security Education and Awareness (ISEA) Project Phase-II' which aims at capacity building and promoting formal/non-formal courses in the area of Information Security, training of Government officials and creation of mass Information Security awareness targeting various user segments.

The project is implemented by 52 premier institutions, more details about the programme including the awareness content for children, students, government official, Law Enforcement Agencies (LEAs), system administration, general users and women etc., is available at **www.isea.gov.in / www.infosecawareness.in**.

CERT-In

The Indian Computer Emergency Response Team (CERT-In) under Ministry of Electronics and Information Technology of the Government of India is the nodal agency for incident response. It performs various functions in the area of cyber security ranging from emergency measures for handling cyber security incidents to response coordination, analysis, alerts, forecasts and advisories.

CSIRT-Fin

CERT-In is providing the requisite leadership for the CSIRT-Fin (Computer Security Incident Response Team-Finance Sector) operations under its umbrella. CSIRT-Fin provides response, containment and mitigation of cyber security incidents reported from the financial sector.

C-DAC

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Ministry of Electronics and Information Technology (MeitY) for carrying out R&D in IT, Electronics and associated areas. As an institution for high-end Research and Development (R&D), C-DAC has been at the forefront of the Information Technology (IT) revolution, constantly building capacities in emerging/enabling technologies and innovating and leveraging its expertise, caliber, skill sets to develop and deploy IT products and solutions for different sectors of the economy.

MeitY

The Ministry of Electronics and Information Technology (MeitY) aims to promote e-Governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITeS industries, enhancing India's role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and innovation, enhancing efficiency through digital services and ensuring a secure cyber space. It envisions e-Development of India as the engine for transition into a developed nation and an empowered society.

NATIONAL INSTITUTE OF SECURITIES MARKETS

NISM Vashi Office
NISM Bhavan, Plot No. 82, Sector - 17,
Vashi, Navi Mumbai, Maharashtra - 400703
Tele: 022-66735100-02
Fax: 022-66735110

NISM Campus
Plot No. IS -1 & 2, Patalganga Industrial Area,
Mohopada Tal. Khalapur, Dist. Raigad,
Maharashtra - 410222
Tele: 02192-668300

www.nism.ac.in