



**3-Days Residential Programme on
Integrated Cybersecurity Training for Bank Officers:
A Hands-On Approach to Cyber Threat Mitigation
(February 12 - 14, 2025)**



Administrative Staff College of India
(accredited as उत्कृष्ट by Capacity Building Commission, GoI)



INTRODUCTION

In recent years, the financial sector has faced an alarming increase in cyber incidents, including ransomware attacks, phishing scams, and advanced persistent threats. High-profile breaches have disrupted operations, led to significant financial losses, and damaged customer trust. To mitigate these risks, regulatory bodies like the Reserve Bank of India (RBI), SEBI, and CERT-In have introduced stringent cybersecurity guidelines for banking, fintech, and NBFCs.

This comprehensive 3-day training programme equips financial sector executives with the knowledge and practical skills to navigate the evolving cybersecurity landscape. The programme integrates regulatory requirements, emerging threats, and hands-on activities to provide actionable insights and effective strategies.

OBJECTIVES: By the end of this programme, participants will:

- **Understand Regulatory Compliance:** Gain clarity on RBI, SEBI, and CERT-In cybersecurity mandates for the financial sector in 2024.
- **Identify and Respond to Threats:** Learn to detect, analyze, and mitigate emerging cyber threats such as AI/ML-based phishing attacks and ransomware.
- **Enhance Incident Response Capabilities:** Strengthen organizational resilience with practical incident response strategies, including mapping threats using the Cybersecurity framework.
- **Build a Secure IT Ecosystem:** Explore proactive measures such as vulnerability assessments, application security, and helps in designing robust IT architectures.
- **Foster a Risk-Aware Culture:** Promote cybersecurity awareness among employees and customers to reduce the human factor risks.
- **Master Crisis Management:** Develop a robust cyber crisis management plan through engaging Table Top exercises and cyber drills.
- **Exposure to the latest Cybersecurity Tools & Technologies:** exposure to the latest cybersecurity tools and technologies for effective threat detection, prevention, and response.

These objectives are designed to create a focused and impactful training programme that addresses key aspects of cybersecurity preparedness and leadership within the BFSI and financial sectors, leveraging the unique environment of **Cyber Theme Park (CTmP)**.

How This Programme Will Help You

- Equip you with the latest tools and knowledge to combat modern cyber threats.
- Enhance your organization's cybersecurity posture by aligning with regulatory standards.
- Build confidence in handling cyber incidents through drills and simulations.
- Foster a culture of awareness and vigilance among your employees and customers.
- Prepare your team to respond swiftly and effectively to potential cyber crises.



CONTENT

Day 1:

Topics
<p>RBI Cybersecurity Regulations, Governance and Compliance</p> <ul style="list-style-type: none"> ▪ Overview of Cybersecurity Regulations ▪ ISO 27002-2022 revision and updates ▪ DPDP (Data Protection and Privacy) Act and implications ▪ RBI's cybersecurity guidelines and Governance framework ▪ Regulatory Requirements for Financial Institutions in India ▪ Compliance strategies and reporting mechanisms.
<p>Digital Frauds and Emerging Cyber Threats:</p> <ul style="list-style-type: none"> ▪ Emerging Threats: Analysis of emerging threats, and advanced technological exploits. ▪ Mobile security risks (e.g., mobile malware, phishing, data breaches) ▪ UPI and Aadhaar-based frauds ▪ Case Studies: Real – time scenarios of sophisticated attacks and lessons learned
<p>Phishing Attack Trends</p> <ul style="list-style-type: none"> ▪ Modus Operandi of Business Email Compromise / Account Take Over ▪ Demonstration of BEC attack and it's implications ▪ AI's Role in Evolving cyber security Threats
<p>Mapping the Cyber-Incident with Cybersecurity Framework</p> <ul style="list-style-type: none"> ▪ Understand the attacker tactics, techniques and procedures ▪ Analysing attack trends and patterns
<p>Practical approach: (CTmP)</p> <ul style="list-style-type: none"> ▪ Email Reputation Checking (BEC) ▪ AI/ML based attack demo ▪ Mapping cyber incident with Cybersecurity framework
<p>Activities:</p> <ul style="list-style-type: none"> • Group Discussion on cyber incidents on FinTech. Companies

Day 2:

Topics
<p>Essentials of Network Security and VAPT</p>
<p>Role of Digital Forensics as a Proactive Approach in Detecting Cyber Attacks</p> <ul style="list-style-type: none"> ▪ Importance of forensics in financial institutions ▪ Identify vulnerabilities ▪ Monitoring and early detection of anomalies and strengthen security posture



Anatomy of Ransomware attack

- Understand Ransomware attack
- Common Tactics and Techniques Used by Threat Actors
- Ransomware detection using Security Information and Event Management (SIEM) systems

Key SIEM strategies for early ransomware detection and response

Log Source Analysis and Detection Techniques

- Analysing logs from servers, firewalls, and network devices
- Identifying suspicious behaviour from logs
- Introduction to anomaly detection, signature-based detection, and behavioural analysis

Practical Approach (CTmP):

- Ransomware Attack Walkthrough: A Practical Demo of Execution, Impact, and Mitigation
- A Practical Demo on detecting Cyber Incident

Activity:

- Group Activity on Cybersecurity challenges

Day 3:

Topics

Application & API Security Testing

- Demo on Web application testing
- Key vulnerabilities in APIs and how to mitigate them
- Understand the secure API design principles
- Importance of securing APIs in modern applications
- Case studies of real-time API security breaches and lessons learned

Cybersecurity Maturity Models

- Case study on bank's Cybersecurity maturity assessment

Building a Risk-Aware Culture

- The importance of building cybersecurity awareness
- Training and awareness strategies for employees and customers
- Key practices for fostering security awareness in organizations

Practical Approach (CTmP):

- Web application testing
- DaDee web monitoring

Activity:

- Cyber Crisis Management Exercise - Table Top Exercise

Valedictory & Feedback



This programme is not just about learning; it's about empowering financial sector professionals to lead their organizations towards a secure and resilient future.

Target Audience:

This programme is ideal for:

- C-Suite Executives: CISOs, CIOs, and CTOs
- Risk and Compliance Officers
- IT and Security Managers
- Network Administrators and Security Analysts
- Fintech Product Managers
- Banking Operations and Strategy Teams

Organisational sponsorship is essential

VENUE

The programme is fully residential and the participants will be accommodated in air conditioned single occupancy rooms. The college does not provide accommodation for the family. The college is Wi-Fi enabled in a comprehensive way.

DURATION

The programme duration is 3 days starting from **February 12 - 14,2025**. The participants are expected to arrive a day before commencement and may leave after the conclusion of the programme.

PROGRAMME FEE

Residential Fee: Rs. 43,700/- (US \$ 683 for foreigners) plus GST as applicable, presently 18% per participant. The fee covers tuition, board and lodging, courseware (in electronic form), and other facilities of the College including internet usage.

Non-Residential Fee: Rs.37,700/- plus GST as applicable, presently 18% per participant. The fee covers tuition, courseware (in electronic form) working lunch, and other facilities of the College including internet usage.

A discount of 10% on the Programme fee for three or more participants from the same organisation will be given, provided the payment is credited into our Bank account before **February 10, 2025**.



Note: Kindly forward us the details of Bank/Wire transfer of fee payment indicating the Programme Code (**Prg/24 - 25/1/300**) to poffice@asci.org.in for confirmation.

Bank details are given below:

For Indian Participants:

Bank Account Number 62090698675
Beneficiary Name Administrative Staff College of India
IFSC Code SBIN0020063
Bank Name State Bank of India
Branch Address Bellavista Branch, Raj Bhavan Road,
Somajiguda, Hyderabad - 500 082

For Foreign Participants:

Bank Account Number 62090698675
Beneficiary Name Administrative Staff College of India
Swift Code SBININBB327
Bank Name State Bank of India
Branch Address Bellavista Branch, Raj Bhavan Road,
Somajiguda, Hyderabad - 500 082.
Country India

MEDICAL INSURANCE

The nominees are requested to carry with them the proof of Medical Insurance. The sponsoring agency is required to endorse the nominees' medical coverage in the event of hospitalization.

LAST DATE FOR NOMINATION

Please use the prescribed/attached form. Last date for receiving nominations is **January 29, 2025**. Kindly contact Programmes Officer for further details (contact details are given at the end of the nomination form).

LAST DATE FOR WITHDRAWAL

February 05, 2025. Any withdrawals after this date will entail forfeiture of fee paid, if any.

ASCI ALUMNI ASSOCIATION

Participants of the College programmes will automatically become members of the ASCI alumni association.



CERTIFICATE OF PARTICIPATION

The College issues a Certificate of Participation on conclusion of the programme.

Programme Director

Dr. Madhusoodanan PR

Email: mpr@asci.org.in

Administrative Staff College of India (ASCI) is taking all the precautionary measures and following all the norms (in light of COVID 19) to provide a safe environment for the participants who are visiting our Campus to attend the Training Programmes.



ABOUT ASCI

“I need not tell you how important I feel this institution is, not because it is the first in Asia or third in the world, but because obviously, it performs a task which is of high importance in the present state of our country, perhaps of other countries too.”

-- Pandit Jawaharlal Nehru, the First Prime Minister of India during his visit to the College on 23 Oct. 1958

Established in 1956, it is the first and foremost institution of its kind in the country. Set up as an institution with a difference at the joint initiative of both the Government of India and the industry, it is an autonomous, self-supporting, public-purpose institution with the objectives of being a think- tank for policy inputs and to build the capacities of practicing professionals in the management of government and business enterprises.

ASCI is an institution of excellence and national importance, and a registered society by constitution. At the apex of its governance structure is a policy-setting, oversight body, the Court of Governors (CoG). It is a virtual who's who of eminent professionals, public figures and industry leaders who have distinguished themselves in their respective fields of specialization in education, enterprise, administration, management and governance spanning a wide variety of sectors like agriculture, banking, engineering, economics, judiciary, law, manufacturing, science and technology and public administration.

Capacity building and applied research assignments constitute the bedrock of the activities of ASCI. They have larger societal benefit and public good as the key cornerstones. ASCI integrates economic, social, cultural, financial, technological, regulatory, human, organizational, and environmental aspects into its management training and action-research initiatives for addressing issues of topical interest and current concern to the government and the industry. With its focus on policy, strategy, management, governance, regulation and socio-economic impact evaluation, ASCI brings knowledge inputs, informed advice, best practice and innovative ideas to bear on its training, policy advocacy, advisory and implementation-assistance services. In the process, it provides opportunities to State and Central Government Departments and Ministries in India and abroad as well as the industry, to develop sustainable policies, devise inclusive strategies and deploying robust plans towards improved economic performance, human development and social progress.

As a result, ASCI enjoys the trust and confidence of the government and industry and is relied upon and entrusted with assignments of varied scale, scope, sweep, spread and specialization.



About ESF Labs Limited

“ESF Labs Limited brings cyber resilience with innovation and excellence.”

ESF Labs is a recognized Cyber Security and Digital Forensics Research Centre with over a decade of experience, focusing on delivering effective and innovative solutions and capacity building to clients. As a CERT-INDIA empanelled entity, ESF Labs, aims at assisting its customers to combat the various cyber threats they face through training/capacity building and solutioning. As a trusted partner, ESF Labs, works closely with corporations, law enforcement agencies, and governments to provide consultation services that enhance the client's cybersecurity and digital forensic capabilities. The solutions delivered are designed to minimize the risk exposure of organizations and also providing a strong foundation in cybersecurity and digital forensic posture.

ABOUT CYBER THEME PARK (CTmP) AN EXPERIENCE CENTRE



Cyber Theme Park is an experience center that transforms theoretical knowledge into practical wisdom. It is a dynamic environment where individuals come together to engage in meaningful interactions, exchange ideas, and challenge their existing perspectives. We believe that true learning occurs when theoretical knowledge is applied and tested in real-life scenarios & situations. Our aim is to bridge the gap between theory and practice by creating an immersive experience with 4 distinct mindsets Attacker, Protector, Defender, and Overseer that transforms abstract concepts into tangible outcomes. The programme seamlessly blends theory with practical, immersing you in the world of attacker and defender techniques.



Nomination Form
 3-Days Residential Programme on
Integrated Cybersecurity Training for Bank Officers:
A Hands-On Approach to Cyber Threat Mitigation
 (February 12 - 14, 2025)

Nominee's Contact Information

Name (Mr/Ms)	_____ :	Date of Birth:	_____
Designation	: _____	Qualification:	_____
Organisation	: _____		
Address	: _____		
Phone(s)	: Office: _____	Mobile: _____	Home: _____
e-mail	: _____	Fax:	_____

Sponsors Details

Name of the Sponsoring Authority:	_____ :	Designation:	_____
Organisation	: _____		
GSTIN Number:	_____		
Address	: _____		
	_____	Pincode:	_____
Phone(s)	: Office: _____	Mobile:	_____
e-mail	: _____	Fax:	_____

Fee particulars

Amount Payable :	Mode of Payment (DD/Ch/NEFT):
Name of the Bank :	Date of Instrument/Transfer:
Instrument Number:	UTR Number for NEFT

Medical Insurance:

Name of the Insurance Agency	Policy Number	Validity upto
Note: Coverage should be available in Hyderabad, India.		

Signature and Official Seal of the Sponsoring Authority:

NOTE: Forward nomination form to: **Mr. G. Sreenivasa Reddy, Programmes Officer,** Administrative Staff College of India, Bella Vista, Hyderabad-500 082. Phone: 0091-40-66534247, 66533000, Mobile: 9246203535, Fax: 0091-40-66534356, e-mail: poffice@asci.org.in