



3-Days Residential Cybersecurity  
Training Programme on  
**Cyber frauds and Risk  
Management strategies  
for BFSI Sector**  
(December 10-12, 2025)



**Administrative Staff College of India**

(accredited as उत्कृष्ट by Capacity Building Commission, GoI)



## **Preface: Navigating the Cybersecurity Imperative in BFSI - A Call to Action**

In an era defined by rapid technological evolution, the Banking, Financial Services, and Insurance (BFSI) sector stands at the forefront of innovation, playing a pivotal role in the economic landscape. However, with the relentless advancement of technology comes the persistent threat of cyberattacks, targeting institutions for financial gain and operational disruption.

The Reserve Bank of India (RBI), as the regulatory guardian of the financial ecosystem, has consistently emphasized the critical importance of cybersecurity readiness in the BFSI sector. The RBI recognizes that the interconnected nature of financial services place organisations at an elevated risk, demanding proactive and strategic measures to safeguard against cyber threats.

Recent years have witnessed an alarming surge in the sophistication and frequency of cyber threats targeting financial institutions. The evolving landscape encompasses a myriad of risks, from ransomware attacks and data breaches to targeted assaults on critical infrastructure. The RBI, cognizant of this dynamic threat environment, has issued guidelines underscoring the urgency for BFSI entities to fortify their cybersecurity defences.

### **RBI Directives and the Call to Action:**

In alignment with the RBI's directives, it is imperative for BFSI top management to embark on a transformative journey towards cybersecurity resilience. This necessitates a paradigm shift from viewing cybersecurity as a technical concern to recognizing it as an integral aspect of strategic decision-making.

### **The Essence of The Programme:**

This comprehensive cybersecurity program, designed for professionals in the financial and digital sectors, is crafted with a singular purpose – to empower participants with the knowledge, skills, and strategic insights essential to navigate the intricacies of the modern cyber landscape.

Drawing inspiration from RBI guidelines, this program is structured to address key facets of cybersecurity governance, risk mitigation, and compliance, fostering a culture of proactive defence against cyber threats.

### **Objectives:**

These objectives aim to create a comprehensive and impactful training program that not only educates but also empowers team to lead their organizations effectively in the ever-evolving cybersecurity landscape.

- To equip participants with advanced understanding of cyberfraud threats, tactics, and real-world risk management.
- To demonstrate the role of governance, compliance, and digital forensics readiness in strengthening cyber resilience.



- Build crisis management plans, foster a risk-aware culture, and prepare proactive, future-ready response strategies.
- To enable BFSI professionals to confidently handle cyber incidents and make informed, executive-level decisions under crisis.
- To help participants learn by doing—using tools and simulations in the Cyber Theme Park (CTmP) to detect phishing, understand cyber-attacks, and respond to incidents effectively.

These objectives are structured to deliver a comprehensive and results-oriented training program that enhances participants’ ability to manage cyber risks, meet compliance, and apply advanced tools—including AI and LLMs—within the immersive Cyber Theme Park (CTmP) environment.

### Day 1: The Digital Risk Landscape & Governance Imperatives

Topics
<p><b>◆ Cyber at the Core: From IT to Boardroom</b></p> <p><i>Understand why cybersecurity is a strategic business issue and no longer just a tech function.</i></p>
<p><b>◆ Regulations that Matter: Building Trust through Governance</b></p> <p><i>Decode the regulatory expectations from RBI, ISO, NIST, and DPDP in BFSI cybersecurity governance.</i></p>
<p><b>◆ Behind the Mask: Understanding Emerging Threats and Cybercrime-as-a-Service</b></p> <p><i>Explore how deepfakes, phishing, and insider fraud are reshaping digital threat landscapes.</i></p>
<p><b>◆ Ready for Crisis: Building Executive Cyber Resilience</b></p> <p><i>Learn to communicate cyber risk and make real-time decisions during simulated attacks.</i></p>
<p><b>🔗 CTmP Experiences &amp; Activities</b></p> <ul style="list-style-type: none"><li>• Deepfake phishing &amp; BEC simulations</li><li>• AI/ML attack demo</li><li>• Executive cyber crisis drill</li><li>• Case studies on governance failure and phishing impacts</li></ul>



## Day 2: Attack Vectors, Defense Strategies & SIEM Integration

Topics
<p>◆ <b>The Digital Battlefield: Securing Networks &amp; Systems</b></p> <p><i>Identify vulnerabilities and proactively defend systems against evolving threats.</i></p>
<p>◆ <b>Invisible Threats: Third-Party &amp; API Risk Exposure</b></p> <p><i>Understand how attackers exploit supply chains, APIs, and vendors to compromise financial systems.</i></p>
<p>◆ <b>Know Your Logs: Detecting Anomalies with SIEM &amp; UEBA</b></p> <p><i>Learn to read between the lines—log analysis, user device activity, and behavioral detection.</i></p>
<p>◆ <b>Ransomware in Action: Lessons from Real Attacks</b></p> <p><i>Dissect the lifecycle of a ransomware attack and the role of SIEM in early detection.</i></p>
<p>🔗 <b>CTmP Experiences &amp; Activities</b></p> <ul style="list-style-type: none"><li>• Live ransomware infection &amp; detection</li><li>• SIEM log simulation</li><li>• Supply chain breach case walkthrough</li></ul>

## Day 3: Building Resilience and Future Readiness

Topics
<p>◆ <b>Code to Control: Securing Applications &amp; APIs</b></p> <p><i>Find and fix security flaws in BFSI web and mobile applications through guided exploration.</i></p>
<p>◆ <b>The Human Firewall: Culture, Awareness &amp; Response Readiness</b></p> <p><i>Strengthen security culture and design customer and employee awareness programs.</i></p>
<p>◆ <b>Digital Clues: Forensics &amp; Evidence in Cyber Fraud</b></p>



*Discover how digital evidence is collected, preserved, and analyzed—including AI's role in forensics.*

#### ◆ **Future Frontlines: AI & Crisis Simulation**

*Experience the future of cyber warfare through AI-led breach simulations and executive war games.*

#### 🔧 **CTmP Experiences & Activities**

- App & API testing
- Digital forensics demo
- Simulated ransomware/phishing breach
- Executive War Game Simulation

#### **Valedictory & Feedback**

### **Participant Profile:**

This program is tailored for mid-to-senior-level professionals in the banking, financial services, and insurance (BFSI) sector, including:

- **Executives** (CEOs, CIOs, CISOs) leading cybersecurity strategies.
- **Compliance Officers** handling regulatory requirements.
- **Risk Managers** addressing cyber risks.
- **IT Security Teams** managing threat detection and response.
- **App & Vendor Managers** securing digital platforms.
- **Operations & Customer Service Managers** preventing fraud.
- **Fraud Prevention Teams** tackling cybercrime.

Perfect for those focused on fraud prevention, cybersecurity, and risk management, equipping them with tools to protect against cyber threats.

***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 WiFi enabled in a comprehensive way

### **DURATION**

The programme duration is from December 10 - 12, 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, course ware (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 **December 08, 2025**.

**Note: Kindly forward us the details of the Bank/ Wire transfer of the programme fee through email to: [poffice@asci.org.in](mailto: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 hospitalisation.

## LAST DATE FOR NOMINATION

Please use the prescribed/attached form. Last date for receiving nominations is **December 03, 2025**. Kindly contact Programmes Officer for further details (contact details are given at the end of the nomination form).



## **LAST DATE FOR WITHDRAWAL**

**December 06, 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 P R**  
e-mail: [mpr@asci.org.in](mailto: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 Cybersecurity Training Programme on Cyber frauds and Risk Management Strategies for BFSI Sector (December 10 - 12, 2025)

#### Nominee's Contact Information

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

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

#### Sponsors Details

#### 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:

#### 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**