



INDIAN INSTITUTE OF BANKING & FINANCE

(An ISO 21001:2018 Certified)

TRAINING PROGRAMME

ON

Cyber Security, Information Security & Digital Banking Risks

(VIRTUAL MODE)

8th to 9th October 2026 (Thursday & Friday)



Coordinated by:

Indian Institute of Banking & Finance,
Professional Development Centre, South Zone,
94, Jawaharlal Nehru Road
Vadapalani, Chennai - 600 026

Website: www.iibf.org.in

For Details & Nomination, please contact:

Individuals can also register for the program at their own cost

Mr. G . Padmanaban Head - PDC, South Zone, Chennai Phone: +91- 44 - 23721429 Mobile: 7397240035 E-mail: head-pdcsz@iibf.org.in	Ms. Priya Maria A Senior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile: +91 9566274128 E-mail: se.pdcsz1@iibf.org.in	Mr Harinadh Nethinti Junior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile : 8317550652 E-mail : je.pdcsz2@iibf.org.in
---	---	--

BACKGROUND

During its 98 years of service, IIBF has emerged as a premier institute in the banking industry. Considering the emerging requirements of the bankers in the dynamic environment, IIBF has been offering certification courses and training programmes to the banking professionals.

The training programs are designed in consultation with the industry experts and human resources personnel with an endeavour to address the skill gaps on a continuous basis. The regular offerings in varied areas prepare the banking professionals ahead of the impending change.

IIBF offers virtual training programmes for its Blended Certification courses and many other programmes to facilitate learning across the country.

IIBF also has state-of-the-art training facilities at its Leadership Centre at Mumbai. It also has seven Professional Development Centres (PDCs) at Chennai, Delhi, & Kolkata, Mumbai, Guwahati, Lucknow & Bangalore conducting training sessions in virtual mode and physical training classes, covering any banking subjects.

ABOUT THE PROGRAMME

- The rapid digital transformation of banking has created significant opportunities as well as new and evolving cybersecurity and information-security risks.
- Banks today operate through interconnected **mobile applications, internet banking platforms, UPI and digital payment systems, APIs, cloud environments, third-party service providers and data-driven technologies**. At the same time, cyber threat actors are increasingly using sophisticated social engineering, malware, ransomware, credential theft, identity compromise and AI-enabled techniques.
- The **CyberShield 360: Securing Digital Banking & Information Assets** programme is a two-day virtual classroom programme designed to provide banking professionals with an updated understanding of the **cyber threat landscape, information security controls, digital banking risks, regulatory expectations, incident response and cyber resilience**.
- The programme incorporates current themes highlighted by RBI, CERT-In and the BFSI cyber-threat landscape, including **AI-assisted attacks, Zero Trust, ransomware, supply-chain risks, API security, real-time monitoring, SOC operations, digital payment frauds and cyber incident response**.

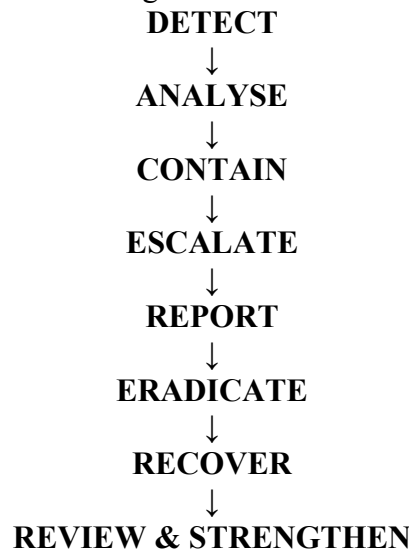
PROGRAMME OBJECTIVES

At the end of the programme, participants will be able to:

- Understand the evolving **cybersecurity threat landscape in banking**.
- Identify key information-security risks affecting banks and financial institutions.
- Understand risks associated with **digital banking and digital payment channels**.
- Recognise phishing, vishing, smishing, malware and social-engineering attacks.
- Understand ransomware and modern attack techniques.
- Identify risks relating to **UPI, mobile banking, internet banking and payment systems**.
- Understand the importance of Identity & Access Management and Multi-Factor Authentication.
- Understand **Zero Trust security principles** and their relevance to banking.
- Identify API, cloud and third-party technology risks.
- Understand information-security governance and risk management.
- Strengthen incident detection, response and recovery capabilities.
- Understand CERT-In cyber-incident reporting and information-security requirements.
- Explore the role of **AI in both cyber attacks and cyber defence**.
- Understand cyber resilience, Business Continuity and Disaster Recovery.
- Develop practical strategies for protecting customer information and critical banking systems.

“CYBER CRISIS RESPONSE CHALLENGE”

Participants will work through a simulated banking cyber incident:



SPECIAL 2026 FOCUS AREAS

The programme will provide focused discussion on:

1. <u>AI-Driven Cyber Threats:</u> AI-assisted attacks, deepfakes, automated reconnaissance and vulnerability exploitation. 2. <u>Zero Trust</u> Identity-centric security, MFA, least privilege and micro-segmentation. 3. <u>BFSI Threat Landscape</u> Current cyber threats affecting banking and financial services 4. <u>Ransomware</u> Attack vectors, prevention, containment and recovery.	5. <u>API & Supply-Chain Security</u> Protecting interconnected digital banking ecosystems. 6. <u>SOC & Real-Time Monitoring</u> Continuous monitoring, threat detection and incident response. 7. <u>Cyber Incident Reporting</u> CERT-In directions and incident-response responsibilities.
--	--

KEY TAKEAWAYS

Participants will learn to:

- **IDENTIFY**
Emerging cyber and information-security risks
- **PROTECT**
Critical systems, information and customer data
- **DETECT**
Suspicious activity and cyber threats
- **RESPOND**
Act effectively during cyber incidents
- **RECOVER**
Restore critical banking operations
- **RESILIENCE**
Build a stronger and more adaptive cyber-security posture

DURATION

8th & 9th October 2026 (Thursday & Friday), from 09.45 AM to 5.30 PM.

METHODOLOGY	TARGET GROUP	TRAINING PERIOD
➤ Lectures, ➤ Case Studies, Discussions & interactions ➤ Sharing of experience on Virtual Platform (ZOOM)	Bankers in PSU/RRB & Co-op Banks and Private sector & Foreign banks, working in Branches/Controlling Offices overseeing Operations including Deposits/Credits/Remittances, Risk Management, Delivery channels and other areas	08.10.2026 & 09.10.2026 (Thursday & Friday) Timings: 09.45 AM to 5.30 PM

FEES

Rs.5,000/- plus GST @18% aggregating to **Rs.5,900/-** per participant

(In case of TDS deduction, please send us TDS certificate)

Programme fees may be remitted to the Institute's bank account as per the details given below:

Account Name	: Indian Institute of Banking & Finance
VAN FOR SOUTH ZONE, CHENNAI - TRAINING FEES	: IIBF28TRGSOUTHZONE
IFSC code	: SBIN0004266
BANK	: STATE BANK OF INDIA
PAN No: AAATT3309D and GSTIN No: 33AAATT3309D2ZY	

(Kindly provide your GST Number in the nomination letter to facilitate raising of invoice)

For further details and nomination please contact:

Mr. G . Padmanaban Head – PDC, South Zone, Chennai Phone: +91- 44 – 23721429 Mobile: 7397240035 E-mail: head-pdcsz@iibf.org.in	Ms. Priya Maria A Senior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile: +91 9566274128 E-mail: se.pdcsz1@iibf.org.in	Mr Harinadh Nethinti Junior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile : 8317550652 E-mail : je.pdcsz2@iibf.org.in
--	--	---



INDIAN INSTITUTE OF BANKING & FINANCE
(ISO 21001:2018 Certified Institute)

Nomination Form (for Banks/FIs & Other Organisations)

Programme Title: Cyber Security, Information Security & Digital Banking Risks

Date: 8th & 9th October 2026 (Thursday & Friday)

Programme Type: Virtual Mode

Details of participant(s):

Sl. No	Name (Mr./Ms./Mrs.)	Designation	Branch /Office	Mobile No. and Land Line No.	E-mail
1					
2					

Name of the Bank/FI	:
Address	:
GST No	:
PAN No	:
Phone/Mobile Number of Nominating Official :	
E-Mail ID of Nominating Official	:

FEES

Rs.5,000/- plus GST @18% aggregating to **Rs.5,900/-** per participant

(In case of TDS deduction, please send us TDS certificate)

Programme fees may be remitted to the Institute's bank account as per the details given below:

Account Name	: Indian Institute of Banking & Finance
VAN FOR SOUTH ZONE, CHENNAI - TRAINING FEES	: IIBF28TRGSOUTHZONE
IFSC code	: SBIN0004266
BANK	: STATE BANK OF INDIA
PAN No: AAATT3309D and GSTIN No: 33AAATT3309D2ZY	

(Kindly provide your GST Number in the nomination letter to facilitate raising of invoice)

Please send your nominations at the earliest to:

Mr. G . Padmanaban Head – PDC, South Zone, Chennai Phone: +91- 44 – 23721429 Mobile: 7397240035 E-mail: head-pdcsz@iibf.org.in	Ms. Priya Maria A Senior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile: +91 9566274128 E-mail: se.pdcsz1@iibf.org.in	Mr Harinadh Nethinti Junior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile : 8317550652 E-mail : je.pdcsz2@iibf.org.in
--	--	---



INDIAN INSTITUTE OF BANKING & FINANCE
(ISO 21001:2018 Certified Institute)

Nomination Form (for Self-Sponsored Candidates)

Programme Title: Cyber Security, Information Security & Digital Banking Risks

Date: 8th & 9th October 2026 (Thursday & Friday)

Programme Type: Virtual Mode

Details of the nominee:

Sl. No	Name (Mr./Ms./Mrs.)	Designation	Branch /Office	Mobile No. and Land Line No.	E-mail
1					

FEES

Rs.5,000/- plus GST @18% aggregating to **Rs.5,900/-** per participant

(In case of TDS deduction, please send us TDS certificate)

Programme fees may be remitted to the Institute's bank account as per the details given below:

Account Name	: Indian Institute of Banking & Finance
VAN FOR SOUTH ZONE, CHENNAI - TRAINING FEES	: IIBF28TRGSOUTHZONE
IFSC code	: SBIN0004266
BANK	: STATE BANK OF INDIA
PAN No: AAATT3309D and GSTIN No: 33AAATT3309D2ZY	

(Kindly provide your GST Number in the nomination letter to facilitate raising of invoice)

Please send your nominations at the earliest to:

Mr. G . Padmanaban Head – PDC, South Zone, Chennai Phone: +91- 44 – 23721429 Mobile: 7397240035 E-mail: head-pdc sz@iibf.org.in	Ms. Priya Maria A Senior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile: +91 9566274128 E-mail: se.pdc sz1@iibf.org.in	Mr Harinadh Nethinti Junior Executive, PDC-South Zone, Chennai Phone: +91- 44 -24722990 Mobile : 8317550652 E-mail : je.pdc sz2@iibf.org.in
---	--	---