Government Capacity Building

Program Brochure · 2026

CYBERSECURITY FOR BANKING & FINANCE

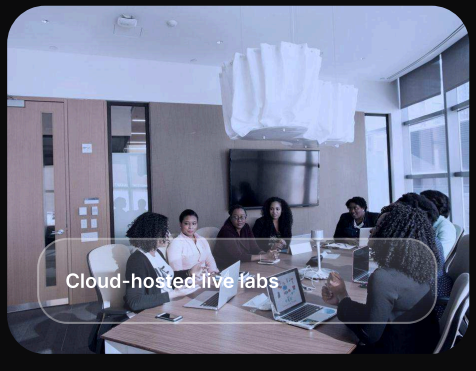
Security for India's financial backbone.

Advanced ↗ | 56 Hours ↗ | SAM-BFSI ↗

Government Capacity Building

Capable institutions. Secure nation.

20 programs in this track



8

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

Tools & frameworks 10

Projects & capstone 11

Certification & method 12

Learning path 13

FAQs 14



AT A GLANCE

Level	**Advanced**
Duration	**56 Hours**
Modules	**8**
Certificate	**SAM-BFSI**

Program overview

Security for India's financial backbone.

Cybersecurity for banks and financial institutions — fraud, compliance, SOC and resilience.

Banks and financial institutions run on digital channels, real-time payments and third-party services, making them a constant target for fraud and cyber attacks. This program equips banking professionals to understand sector threats, apply RBI cybersecurity requirements, strengthen fraud detection and SOC operations, secure digital channels, manage third-party and cloud risk, and build resilience through realistic exercises and governance reporting.

DELIVERY

Instructor-led · Live virtual · Blended



WHAT YOU'LL PRACTISE

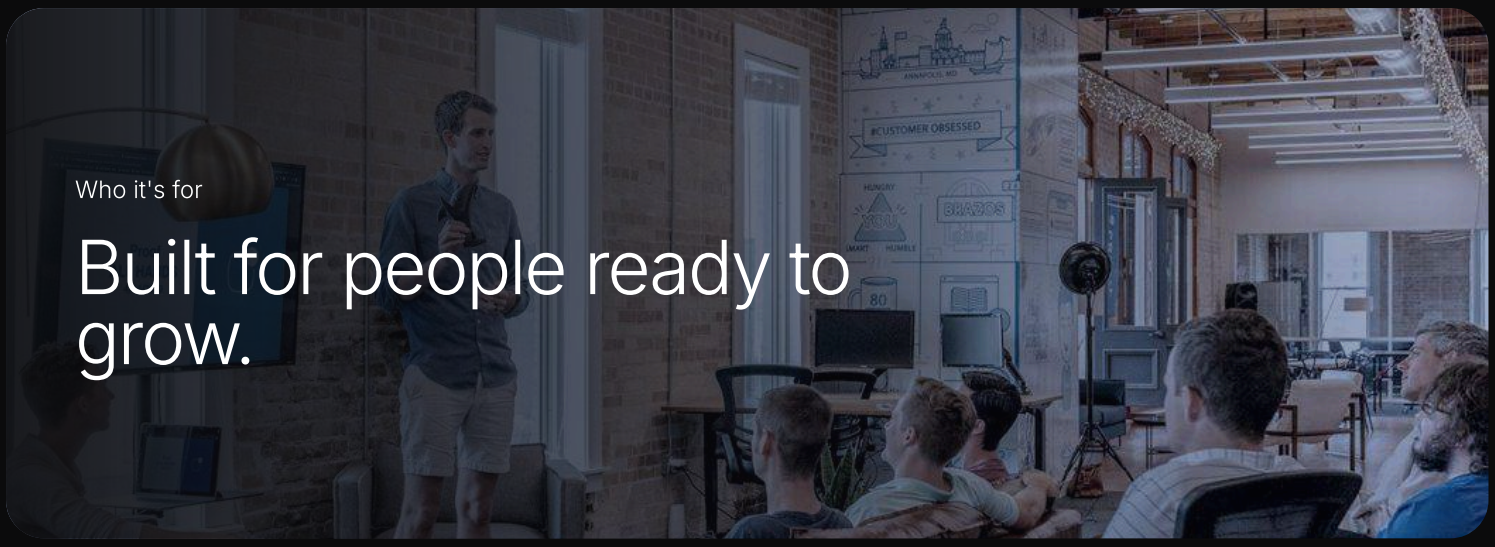
- Understand banking cyber threats
- Apply RBI cyber requirements
- Detect fraud and attacks
- Build resilience and response

LEVEL
Advanced

DURATION
56 Hours

CERTIFICATION
SAM-BFSI

TRACK
Government Capacity Building



Who it's for

Built for people ready to grow.

01

Government officials

Cyber awareness, AI for public service, e-governance

02

Senior IAS / IPS officers

Technology leadership and AI policy

03

PSU workforce

IT security, OT/ICS/SCADA, digital skills

04

Law enforcement & defence

Cyber forensics, CERT ops, defence cyber

PREREQUISITES

- Experience in banking IT, security, risk or operations 01
- Understanding of digital banking channels 02
- Familiarity with regulatory compliance concepts 03

ROLES THIS PREPARES YOU FOR

- Bank information security officers ↗
- Fraud risk analysts ↗
- Banking SOC analysts ↗
- IT risk and compliance managers ↗
- Digital channel security leads ↗

Learning outcomes

What you'll be able to do.



01	Analyse cyber threats across banking channels and payment systems
02	Apply RBI cybersecurity framework and related regulatory directions
03	Detect digital payment fraud patterns using transaction monitoring concepts
04	Design SOC detection use cases for financial sector threats
05	Assess third-party, fintech and cloud risks with structured questionnaires
06	Report cyber risk to boards using meaningful key risk indicators

Program runway

Module by module.

8
modules · 56 hours

01	**Banking Technology and Threats** Core banking and digital channels, UPI, cards and payment systems, Threats to financial institutions	7 hrs
02	**Regulatory Requirements** RBI cybersecurity framework overview, IT governance and risk directions, Outsourcing and cloud guidelines	7 hrs
03	**Fraud Detection and Prevention** Digital payment fraud patterns, Account takeover and mule accounts, Transaction monitoring concepts	7 hrs
04	**Security Operations for Banks** Banking SOC structure, SIEM and log monitoring, Financial threat use cases	7 hrs
05	**Securing Digital Channels** Internet and mobile banking security, API security for open banking, Customer authentication methods	7 hrs
06	**Third-Party and Cloud Risk** Vendor risk assessment, Outsourcing governance, Cloud security responsibilities	7 hrs
07	**Incident Response and Resilience** Cyber crisis management plans, Ransomware response for banks, Regulator and customer communication	7 hrs
08	**Governance and Board Reporting** IT strategy and steering committees, CISO role and reporting, Key risk indicators	7 hrs
★	**Capstone · Bank Cyber Resilience Program** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Banking Technology and Threats

7 hours

Hands-on lab
Map threats across a bank's digital channels and payment flows

TOPICS COVERED

- Core banking and digital channels
- UPI, cards and payment systems
- Threats to financial institutions
- Lessons from public banking incidents
- Third-party and fintech risks

Module 02

Regulatory Requirements

7 hours

Hands-on lab
Perform a gap assessment against RBI cybersecurity framework requirements

TOPICS COVERED

- RBI cybersecurity framework overview
- IT governance and risk directions
- Outsourcing and cloud guidelines
- Incident reporting timelines
- Data protection and localisation

Module 03

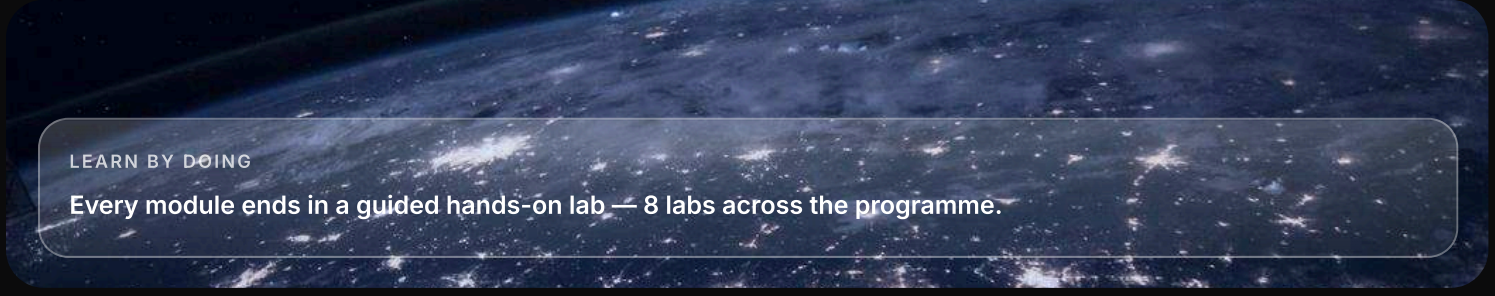
Fraud Detection and Prevention

7 hours

Hands-on lab
Analyse sample transaction data to flag suspicious fraud patterns

TOPICS COVERED

- Digital payment fraud patterns
- Account takeover and mule accounts
- Transaction monitoring concepts
- Customer awareness programs
- Fraud case management



Syllabus, continued.

Modules 04–06

Module 04

Security Operations for Banks

7 hours

Hands-on lab
Develop detection use cases for common threats in a banking SOC

TOPICS COVERED

- Banking SOC structure
- SIEM and log monitoring
- Financial threat use cases
- Threat intelligence sharing
- SOC performance metrics

Module 05

Securing Digital Channels

7 hours

Hands-on lab
Review a mobile banking feature for authentication and API risks

TOPICS COVERED

- Internet and mobile banking security
- API security for open banking
- Customer authentication methods
- Secure software development
- Application security testing governance

Module 06

Third-Party and Cloud Risk

7 hours

Hands-on lab
Assess a payment service provider using a structured vendor risk questionnaire

TOPICS COVERED

- Vendor risk assessment
- Outsourcing governance
- Cloud security responsibilities
- Fintech partnership risks
- Contractual security clauses



Syllabus, continued.

Modules 07–08

Module 07

Incident Response and Resilience

7 hours

Hands-on lab
Run a tabletop exercise on a ransomware incident affecting branch operations

TOPICS COVERED

- Cyber crisis management plans
- Ransomware response for banks
- Regulator and customer communication
- Business continuity and recovery
- Cyber insurance considerations

Module 08

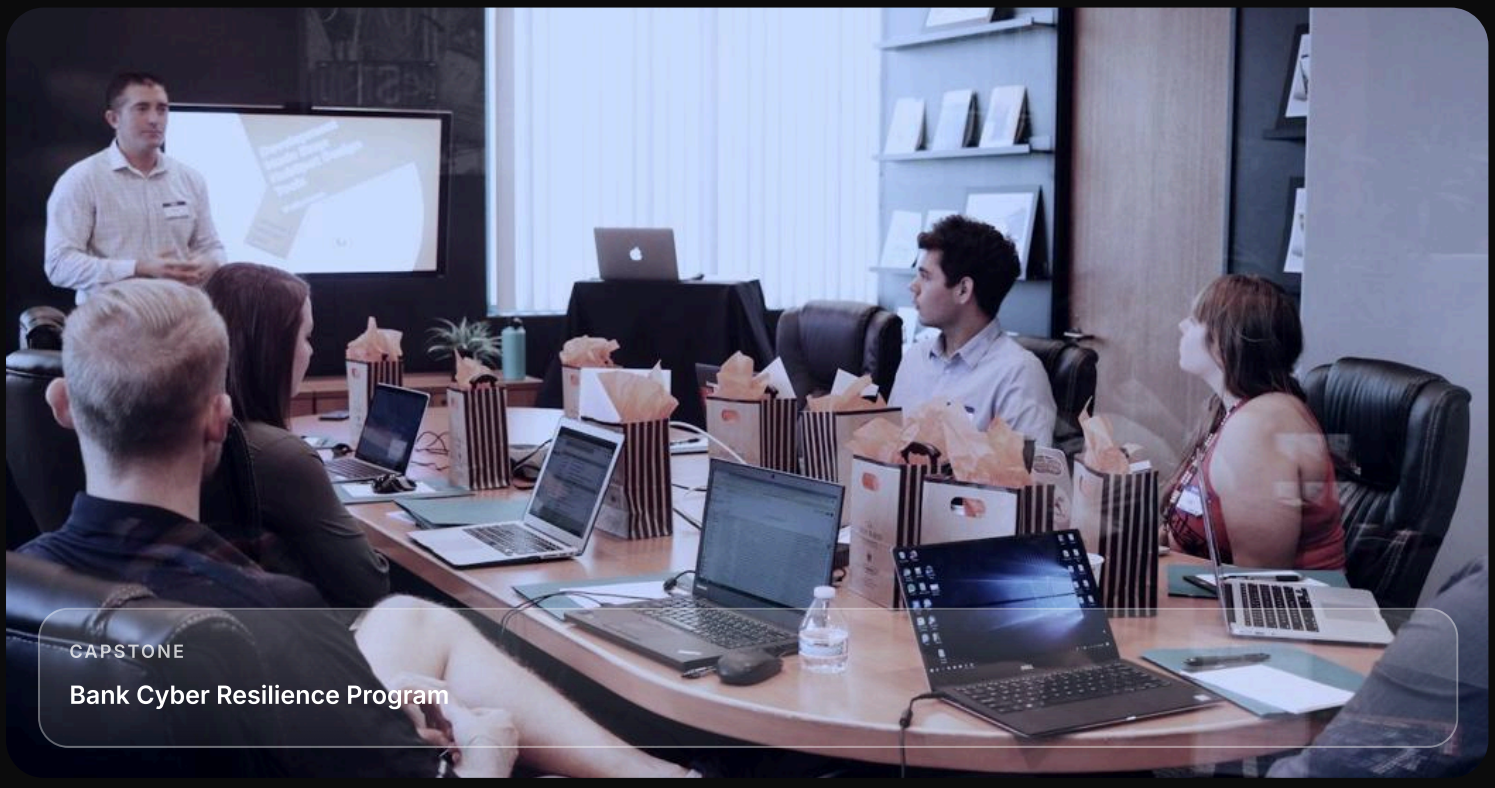
Governance and Board Reporting

7 hours

Hands-on lab
Prepare a board-level cyber risk report with key risk indicators

TOPICS COVERED

- IT strategy and steering committees
- CISO role and reporting
- Key risk indicators
- Audit and inspection readiness
- Security culture in banks



CAPSTONE

Bank Cyber Resilience Program

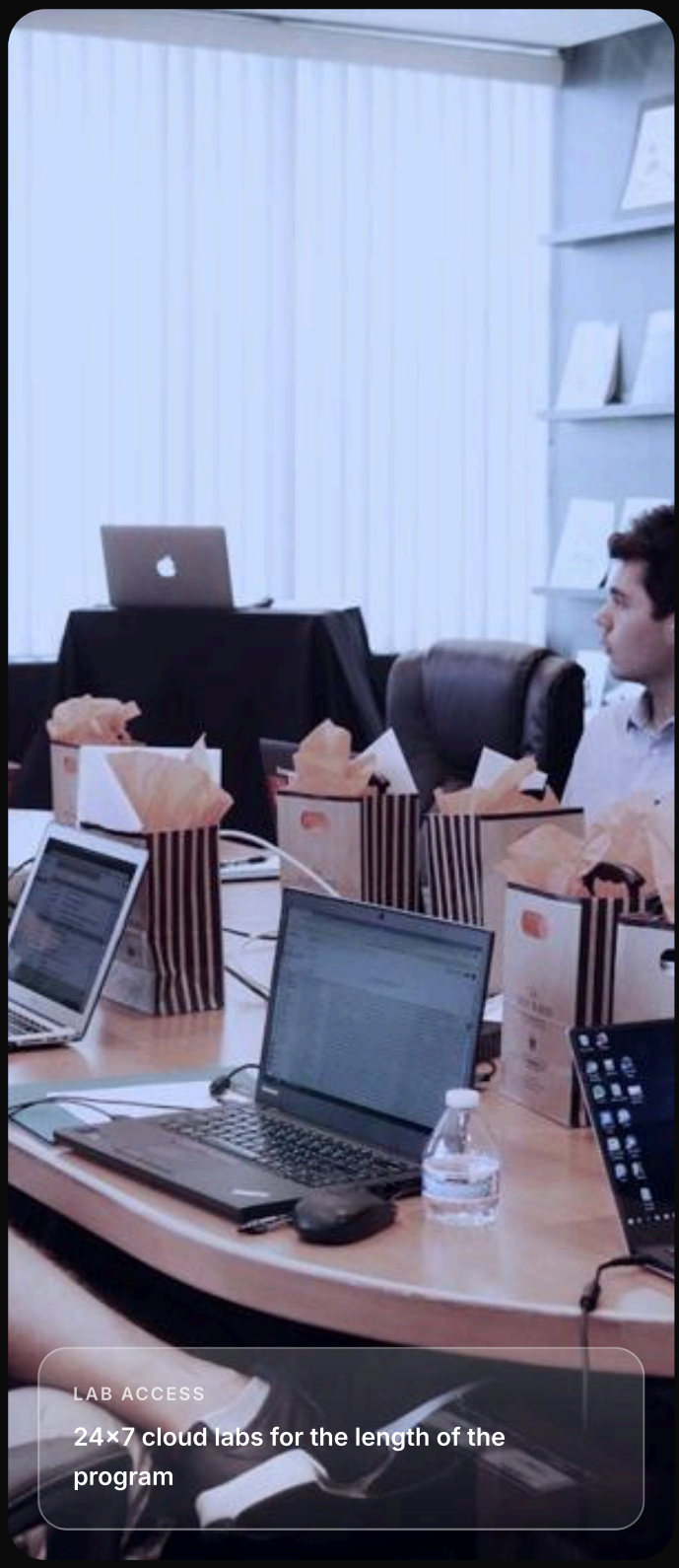


Frameworks & standards

RBI

FOCUS AREAS

Understand banking cyber threats	01
Apply RBI cyber requirements	02
Detect fraud and attacks	03
Build resilience and response	04



01

RBI Framework Gap Assessment

Assess a sample bank's controls against RBI cybersecurity requirements and prioritise remediation actions with owners and timelines.

02

Fraud Pattern Analysis

Analyse a sample transaction dataset to identify mule account and account takeover patterns, recommending monitoring rules and customer measures.

03

Vendor Risk Review

Evaluate a fintech or payment partner using a vendor risk questionnaire and recommend contractual and monitoring safeguards.



Capstone project

Certification

SAM-BFSI

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

Real-world attack and use-case scenarios open every module.

Phase 02

Apply

Hands-on lab work, CTF challenges and live projects.

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive

Learning path · Government Capacity Building

Where this program fits.

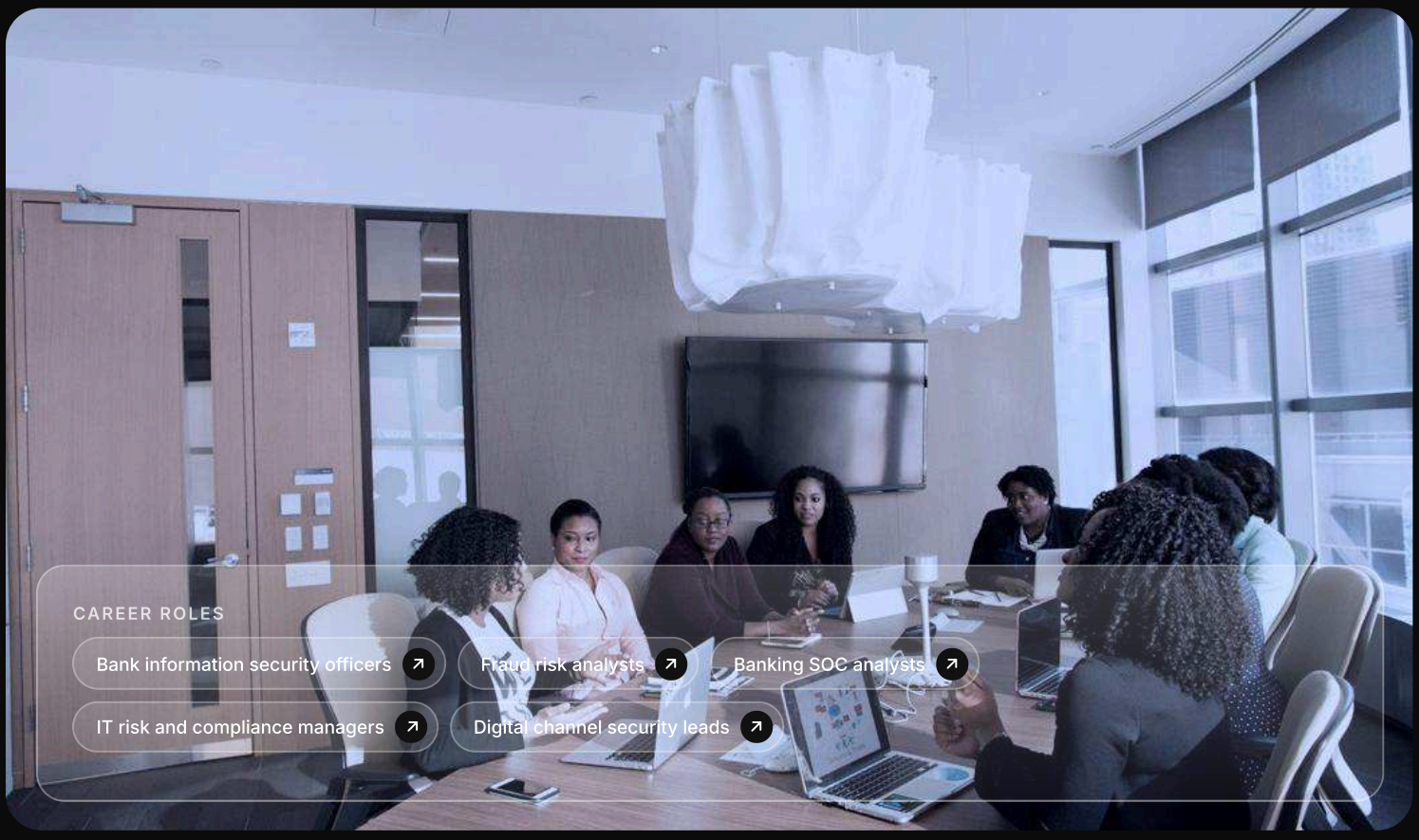
Foundation	Intermediate	Advanced	Expert	Executive
4 programs	5 programs	You are here	1 programs	2 programs

Before this

- **Digital Governance & e-Governance Platforms** — 32 Hours
- **Cybersecurity for Critical Infrastructure** — 40 Hours
- **AI Policy & Technology Regulation Workshop** — 24 Hours
- **OT/ICS/SCADA Security for Industrial PSUs** — 48 Hours

Up next

- **PSU Digital Transformation Advisory** — Custom



Questions, answered.

Q01

Do I need prior experience to join?

Yes. This is an advanced-level program that assumes prior experience in banking IT, security, risk or operations. It moves quickly into frameworks, case studies and hands-on work, so participants should meet the listed prerequisites before enrolling.

Q02

How is the program delivered and scheduled?

The 56 hours program is instructor-led and can be delivered live virtual, in person at your institution, or in a blended format. Session timings and batch sizes are planned with the sponsoring organisation to fit official working schedules.

Q03

Will I receive a certificate?

Yes. Participants who meet attendance requirements and successfully complete the assessments receive the Samcommunity Academy SAM-BFSI certificate. Assessments may include quizzes, practical exercises and a final capstone review, depending on the program format.

Q04

What do the hands-on exercises involve?

Exercises use case studies, templates, tabletop scenarios and guided demonstrations rather than live production systems. Any required materials or sandbox access are shared before the program, and no special software installation is usually needed.

Q05

Is career or post-program support included?

The program is designed for capacity building of working professionals rather than placement. Participants receive learning resources, templates and guidance on further learning paths. Samcommunity Academy does not guarantee promotions, postings, jobs or salary outcomes.



Let's talk

START CYBERSECURITY FOR BANKING & FINANCE.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India