

EXECUTIVE EDUCATION PROGRAMS · EXECUTIVE

Cybersecurity Risk for Non-Technical Leaders

Cyber risk without the jargon.

Contents

Why this program 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

Frameworks & tools 08

Projects & capstone 09

Certification & method 10

Learning path 11

FAQs 12



LEVEL	Executive
DURATION	12 Hours
MODULES	3
CERTIFICATE	SAM-CSRNTL

Why this program

Understand, question and govern cyber risk without a technical background.

Cyber incidents are business events that affect customers, finances, regulators and reputation, so leaders cannot leave cybersecurity solely to technical teams. Many executives, however, find security reports full of jargon. This short program explains common threats in plain language and helps leaders read cyber risk reports, ask the right questions and make sound decisions during incidents.



12 hours of compact, practical sessions

3 focused modules, built around real work

3 projects plus a capstone presentation



Who this program is for



01

Board members & directors

AI and technology risk governance

02

CXOs

AI strategy, data-driven leadership

03

CISOs & CIOs

CISO leadership program

04

Senior government officials

National security & cyber policy

PREREQUISITES

- Leadership or management role
- No technical background required
- Interest in organisational risk and resilience

DESIGNED FOR

- Business Unit Head
- Senior Executive
- Founder or Managing Director
- Finance, Legal or HR Leader
- Operations Manager

What you'll be able to do.

01 Describe common cyber threats such as phishing and ransomware

02 Understand how attacks affect business operations and customers

03 Read and interpret cyber risk reports and metrics

04 Ask security teams focused, practical questions about protection

05 Understand key Indian obligations under DPDP and CERT-In

06 Make informed leadership decisions during cyber incidents

How the program works

Cyber Threats in Plain Language

Phishing and social engineering, Ransomware and extortion, Business email compromise, Insider and third-party threats.

Reading Cyber Risk and Controls

Cyber risk in business terms, Key security controls explained, Reading security reports and metrics, DPDP Act and CERT-In basics.

Leading Through Cyber Incidents

Incident response roles, Decisions during ransomware events, Communicating with customers and regulators, Building a security-aware culture.

01 · Cyber Threats in Plain Language	4 hrs
02 · Reading Cyber Risk and Controls	4 hrs
03 · Leading Through Cyber Incidents	4 hrs
★ Capstone · Cyber Readiness Leadership Review	



The curriculum

MODULES 01–03

01 Cyber Threats in Plain Language

4 HOURS

Practical: Walk through a real-style phishing attack and identify where it could be stopped.

- Phishing and social engineering
- Ransomware and extortion
- Business email compromise
- Insider and third-party threats
- AI-enabled scams and deepfakes

02 Reading Cyber Risk and Controls

4 HOURS

Practical: Interpret a sample cyber risk report and list questions for the security team.

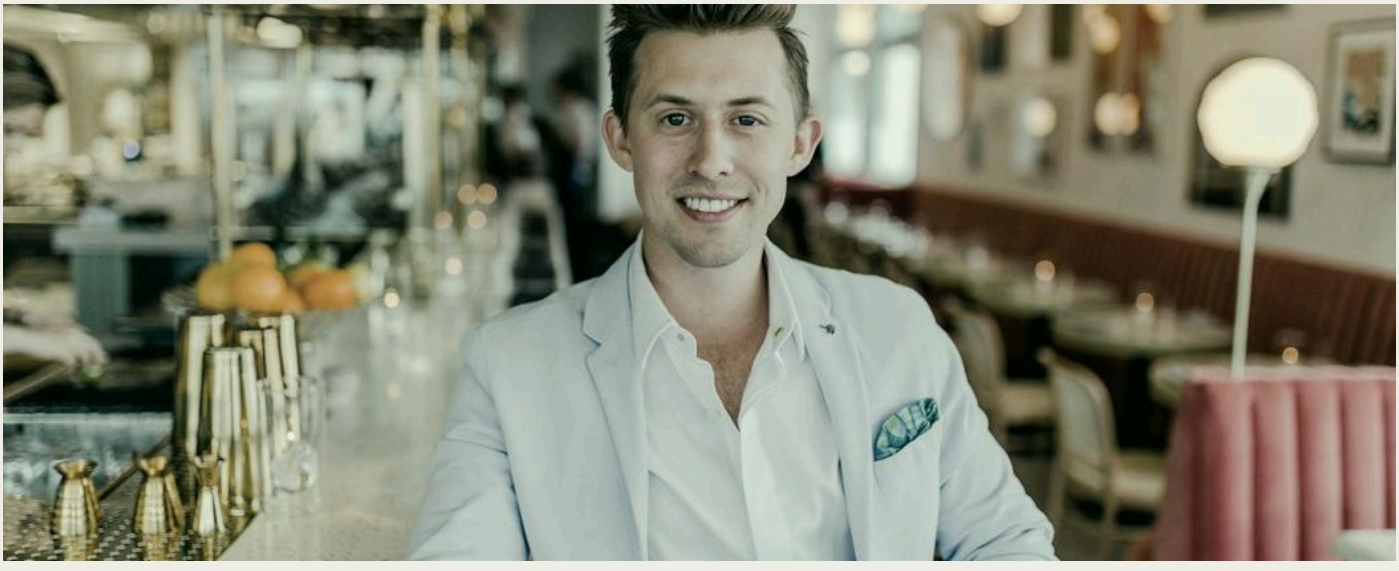
- Cyber risk in business terms
- Key security controls explained
- Reading security reports and metrics
- DPDP Act and CERT-In basics
- Questions to ask security teams

03 Leading Through Cyber Incidents

4 HOURS

Practical: Make leadership decisions in a ransomware tabletop exercise with time-pressured updates.

- Incident response roles
- Decisions during ransomware events
- Communicating with customers and regulators
- Building a security-aware culture
- Post-incident learning



What you'll focus on.

DPDP Act 01

CERT-In 02

Cyber Threats in Plain Language 03

Reading Cyber Risk and Controls 04

Leading Through Cyber Incidents 05



Projects & capstone

01

Threat Awareness Brief

Summarise the top cyber threats facing your business area and their likely business impact in plain language.

02

Leader's Question List

Create a practical list of questions to ask security teams about risks, controls and readiness.

03

Incident Decision Card

Build a one-page decision guide covering leadership roles, escalation points and communication steps during a cyber incident.



CAPSTONE

Cyber Readiness Leadership Review

Assess a case organisation's cyber readiness from a leadership perspective, using a sample risk report and incident scenario, then present priority concerns, questions for management and recommended leadership actions.

CERTIFICATION

SAM-CSRNTL

Awarded on successful completion of the program assessments.

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

HOW YOU LEARN · THE SAM LEARNING FRAMEWORK™

01 Scenario

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

02 Apply

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

03 Master

Assessment, peer review and certification prep.

04 Mentor

Post-program career guidance and support.



Delivery: Instructor-Led (ILT) · Virtual Instructor-Led · Self-Paced Online · E-Learning Licensing · Blended Learning · Corporate Onsite

Where this program fits

Executive

You are here

BEFORE THIS

A starting point — no prerequisite program needed.

UP NEXT

The top of this pathway — explore related programs.



Questions, answered

Do I need prior experience to join?

No technical background is needed. The program is built specifically for non-technical leaders and explains cyber threats, controls and incident decisions in plain business language with practical examples.

How is the program delivered and scheduled?

Delivery is instructor-led, either live virtual or blended with in-person sessions. Batch timings, weekday or weekend options and corporate cohort schedules are confirmed at enrolment, with session materials provided for revision.

What certification will I receive?

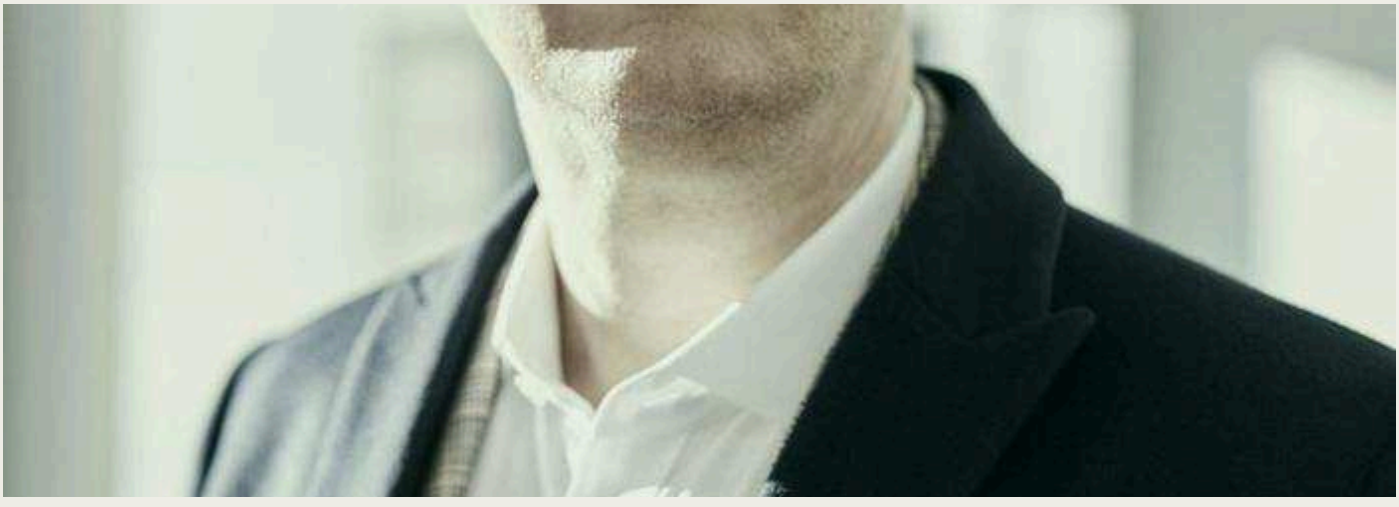
Learners who attend the sessions and pass the required assessments receive the Samcommunity Academy SAM-CSRNTL certificate of completion. It recognises the skills demonstrated in the program and is not a third-party vendor credential.

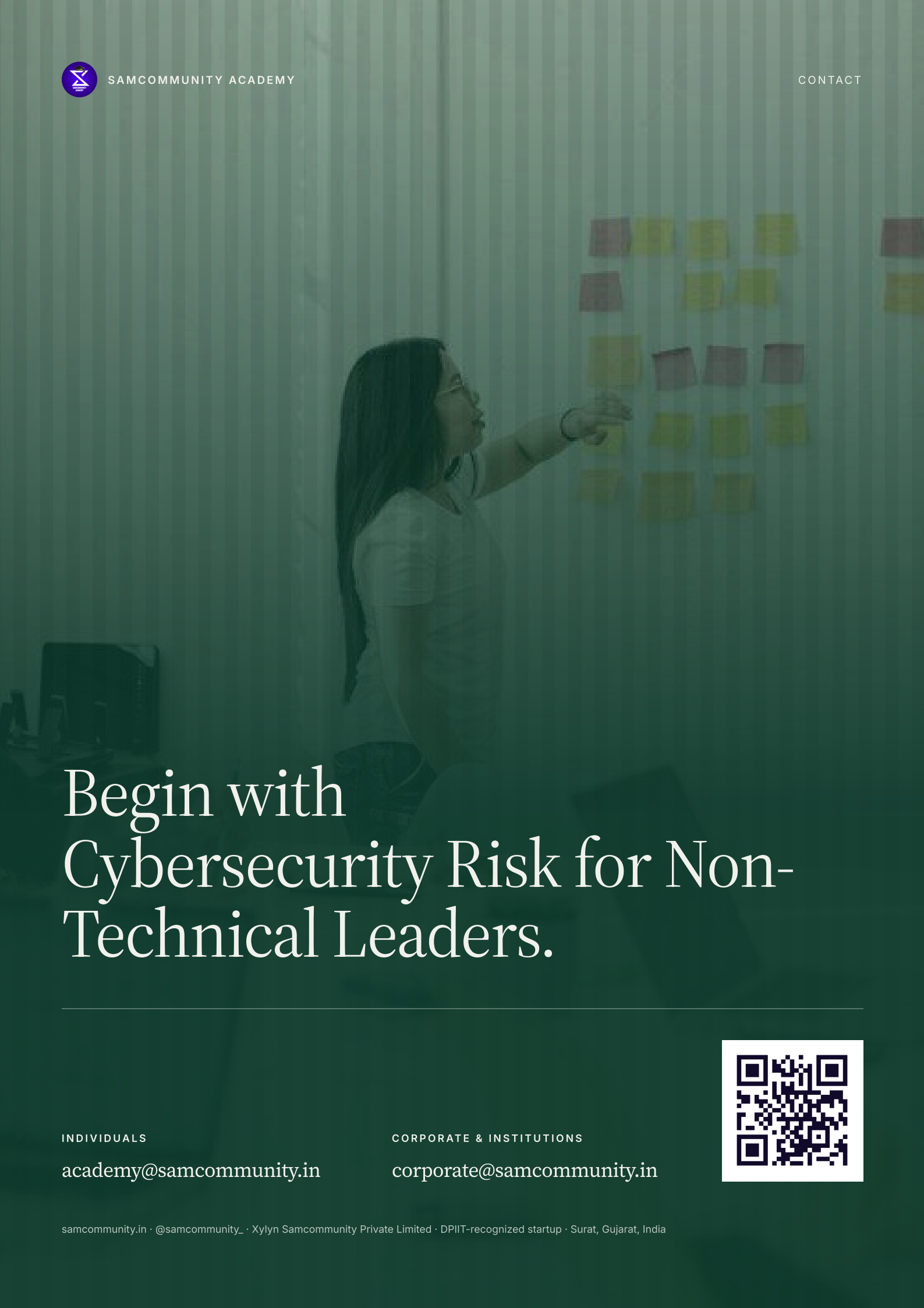
Will I get access to labs, tools and materials?

Yes. Sessions use realistic case studies, board-style simulations, discussion exercises and decision templates. Participants receive briefing materials and reusable frameworks; no technical software or hands-on configuration is required.

Is career support included?

Learners receive guidance on applying the skills at work, including mentor discussions and, where relevant, resume or portfolio feedback. Samcommunity Academy does not guarantee jobs, promotions or salaries; outcomes depend on individual effort.





SAMCOMMUNITY ACADEMY

CONTACT

Begin with Cybersecurity Risk for Non-Technical Leaders.

INDIVIDUALS

academy@samcommunity.in

CORPORATE & INSTITUTIONS

corporate@samcommunity.in

samcommunity.in · @samcommunity_ · Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India