Programme on

Cyber Resilience Leadership: Governance, Risk & Operational Excellence

(March 16 - 20, 2026)

Administrative Staff College of India

(accredited as उत्कृष्ट by Capacity Building Commission, GoI)

PREFACE

In today's hyper-connected world, organizations across public and private sectors face complex cyber risks that impact governance, operations, and reputational trust. Senior leaders are increasingly accountable for ensuring operational continuity while managing regulatory compliance, third-party dependencies, and emerging threats such as AI-enabled attacks.

Cyber Resilience Leadership: Governance, Risk & Operational Excellence is a five-day executive programme designed to equip senior leaders with the knowledge, perspective, and practical experience needed to address these challenges. The curriculum is aligned with cyber resilience core pillars, enabling leaders to strengthen governance and risk oversight, understand operational security and Zero Trust principles, and build readiness for incident response, continuity, and crisis management.

Through a combination of theory sessions, real-world case discussions, live demonstrations, and immersive tabletop exercises, participants gain actionable, leadership-oriented insights into threat detection, forensic readiness, and emerging risks. The programme emphasizes executive decision-making, accountability, and proactive governance, empowering leaders to safeguard digital assets, ensure regulatory alignment, and foster a resilient organizational culture capable of withstanding and recovering from cyber disruptions

OBJECTIVES

Upon successful completion of the programme, participants will be able to:

- Build awareness of cyber resilience pillars and leadership accountability within regulatory frameworks.
- Strengthen governance, risk, and compliance oversight, including supply chain management and alignment with international standards.
- Develop understanding of security operations, network and application risks, and overall organizational cyber posture.
- Prepare for effective incident response, ransomware simulations, and business continuity and disaster recovery planning.
- Equip leaders to manage emerging AI-driven threats, lead cyber crises, participate in tabletop exercises, and sustain organizational resilience.

WHY THIS PROGRAMME IS UNIQUE

- **Progressive Learning Journey**: Moves logically from threat awareness to governance, operations, response, investigation, and future readiness.
- **Executive-Centric Approach:** Designed for decision-makers across all sectors, with no low-level technical or coding focus.

- **Real-World Preparedness**: Uses practical exercises, simulations, and tabletop discussions to build confidence and readiness.
- **Integrated Risk View:** Connects application risks, operational security, incident response, forensics, and business continuity.
- **Forward-Looking Focus:** Incorporates AI-related risks and emerging threats to prepare leaders for the next phase of cyber challenges.

CURRICULUM STRUCTURE

Day 1: Foundations of Cyber Resilience & Legal Accountability

Topics
Theory • Cyber resilience pillars (NIST CSF, ISO 22301) tailored to operational continuity. • Leadership roles in governance: accountability under DPDP Act 2023 and CERT-In directives. • Data fiduciary duties, reputational risks, and aligning cyber with business ops
CTmP Experiences & Activities • Spot-the-Phish Challenge: Analyse real pharma phishing • Data Classification Exercise: Hands-on tagging for operational assets. • Social Engineering Techniques & Tactics

Day 2: Governance, Risk Management & Secure Operations

Topics
Theory • GRC frameworks (ISO 27001, COBIT) for operational alignment and audits. • Cloud/shared responsibility model; third-party risk in supply chains. • Securing infrastructure: From endpoints to vendor ecosystems
CTmP Experiences & Activities • OWASP Top 10 Review: Operational vulnerability mapping. • Audit Report Interpretation: Decode findings for team fixes. • Cyber-Secure Procurement Exercise

Day 3: Threat Detection & Zero Trust Operations

Topics
Theory • SOC essentials: Metrics, KPIs, and escalation for leaders. • Zero Trust implementation: Segmentation to limit blast radius in ops environments. • Architectural decisions impacting daily workflows.
CTmP Experiences & Activities • Live SOC Demo: Monitor simulated threats. • Security Review Exercises: Endpoint/network/app walkthroughs. • Zero Trust Architecture Build: Design for your org.

Day 4: Incident Response & Continuity in Operations

Topics
Theory • IR lifecycles: Executive roles in response and NCIIPC reporting. • Ransomware tactics; business continuity/DR for critical ops. • Forensic readiness and supply chain breach handling.
CTmP Experiences & Activities • Ransomware and incident response simulation • Supply Chain Risk Assessment: breach scenario. • Digital Forensics Drill: Evidence collection

Day 5: Emerging Risks, Crisis Leadership & Sustained Resilience

Topics
Theory • AI risks: Deepfakes, automated attacks, defensive AI strategies. • Crisis comms, budgeting, and fostering resilience culture. • Continuous improvement via metrics and ethical AI governance

CTmP Experiences & Activities • AI Threat Analysis: Dissect generated phishing/deepfakes • Executive TTX: Multi-scenario cyber crisis simulation.
Valedictory & Feedback

WHO SHOULD ATTEND

This programme is designed for senior leaders and decision-makers across all sectors, including government, public organizations, private enterprises, and critical industries. Ideal participants include Board Members, CXOs (CEO, CIO, CISO, CTO, COO), Managing Directors, SVPs, GMs, Business Unit Heads, Chief Risk, Compliance, and Data Officers, and Heads of IT, Security, Risk, Compliance, Audit, Procurement, Supply Chain, and Business Continuity. Ideal for those overseeing operations, digital initiatives, risk management, regulatory compliance (DPDP/CERT-In), and organizational cyber preparedness.

FACULTY & DELIVERY PARTNERS

The programme is delivered through a strategic partnership with senior government policymakers, renowned academics from premier national institutions, and leading cybersecurity experts from the industry. This unique coalition ensures participants receive a holistic education that blends high-level national strategy with practical, cutting-edge skills.

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 **5 days** starting from **March 16 - 20, 2026.** The participants are expected to arrive a day before commencement and may leave after the conclusion of the programme.

PROGRAMME FEE

Residential Fee: Rs. 69,500/- (US $ 1086 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. 59,500/- 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 March 13, 2026.

Note: Kindly forward us the details of Bank/Wire transfer of programme fee 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 **March 09, 2026**. Kindly contact Programmes Officer for further details (contact details are given at the end of the nomination form).

LAST DATE FOR WITHDRAWAL

March 12, 2026. 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
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.

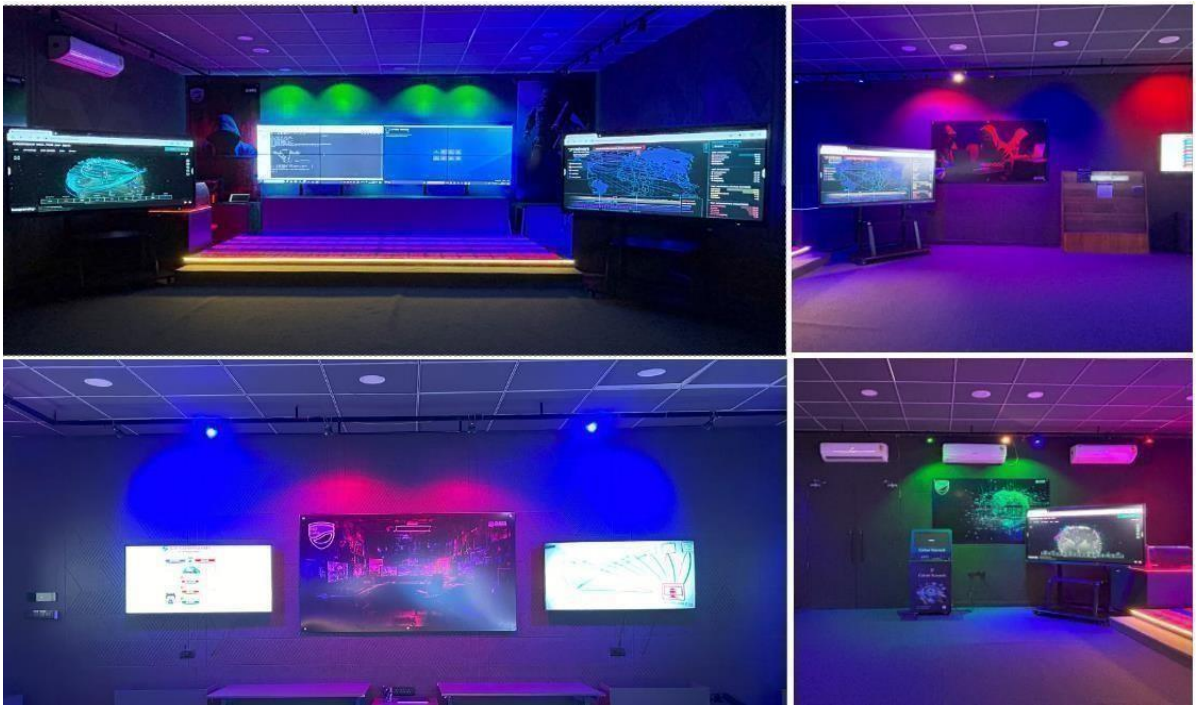
As a result, ASCI enjoys the trust and confidence of the government and industry and is relied upon and entrusted with assignments of varied scale, scope, sweep, spread and specialization.

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 centre 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

Programme on

Cyber Resilience Leadership:
Governance, Risk & Operational Excellence

(March 16 - 20, 2026)

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**