ENGINEERING STAFF COLLEGE OF INDIA

Autonomous Organ of The Institution of Engineers (India)
ISO 9001:2015 Certified, AICTE & CEA Recognized Institution
4 Decades of Excellence in Nation Building

ESCI

PROFESSIONAL DEVELOPMENT PROGRAM

Building Cyber Security & AI Resilience for Senior Managers & Leaders



Key Focus Areas

- Cyber Security Governance & Risk Management
- AI for Threat Detection & Incident Response
- Building Organisational Resilience
- Leadership Strategies for a Secure Digital Future
- Policies, Compliance & Best Practices

01 - 03 Dec 2026

IEI Centre, Shimla, HP

(An ISO 9001:2015 Certified, AICTE & CEA Recognized Institution)

Centre for Promotion of Professional Excellence

www.escihyd.org , it@escihyd.org, 040-66304124/25/23, 8886661060

Introduction

- In today's hyper-connected digital economy, cybersecurity and artificial intelligence (AI) are no longer purely technical concerns—they are core business priorities that demand strong leadership oversight. As organizations increasingly rely on digital platforms and AI-driven decision-making, the risk landscape has expanded to include sophisticated cyber threats, data breaches, and emerging AI vulnerabilities such as bias, misuse, and adversarial attacks. For senior managers and leaders, building resilience means going beyond compliance to proactively integrating security and responsible AI practices into strategy, governance, and culture.

Objective

- Objective of this program is to equip decision-makers with the knowledge, frameworks, and practical insights needed to anticipate risks, respond effectively to incidents, and lead their organizations with confidence in an era of rapid technological change.

Course Content

Cyber Risk Oversight for Leadership

- Cybersecurity as a business risk
- Role of leadership in cyber resilience
- Understanding threat landscape
- NIST Cybersecurity Framework
- ISO/IEC 27001 overview

Threat Landscape & Emerging Risks

- Nation-state threats & cyber warfare
- Insider threats and human risks
- Third-party & supply chain vulnerabilities
- Risk mapping exercise for participants

Cyber Risk Governance

- Board-level reporting & KPIs
- Cyber risk quantification (financial impact)
- Aligning cybersecurity with business strategy
- India DPDP Act

Incident Response & Crisis Leadership

- Building an incident response plan
- Leadership role during breach
- Communication strategy (internal + public)
- WannaCry ransomware attack Case Study

Introduction to AI Risks for Leaders

- AI adoption trends in enterprises
- Risks: bias, hallucination, data leakage, adversarial attacks

AI Security & Threats

- Prompt injection attacks
- Data poisoning
- Model theft & adversarial AI
- Risks in generative AI platforms like ChatGPT

Responsible & Ethical AI Governance

- AI governance frameworks
- Explainability & transparency
- Regulatory trends (EU AI Act, global policies)
- OECD AI Principles
- World Economic Forum AI governance guidelines

Securing AI Systems in Enterprises

- Secure AI lifecycle
- DevSecOps for AI
- Vendor risk management for AI tools
- AI risk assessment workshop

Cyber Resilience Strategy

- From prevention → resilience mindset
- Business continuity & disaster recovery
- Zero Trust Architecture

Human Factor & Culture

Integrating Cybersecurity & AI

Future Trends & Leadership Roadmap

Methodology

Methodology of the programme includes class room sessions with Lecture / Discussion with Hands- on Practical, with tools, audio visual aid, bench marked video shows, Chalk & Talk sessions, group discussions, case studies, debates, sharing of experiences etc. All the sessions will be interactive demanding active participation from all the members.

Target Participants

- Managers / Team Leaders / Project Heads / Professional working in government, Public, Private Banks and financial Sector organizations.
- Scientist's, Officer's and Engineers working in Defence,DGQA, DRDO & Research organizations.
- Any officials / Senier Executive interested in Gen AI

Course Director

Mr. Syed Azgar , MBA(IT), RHCE, MCSA,
Sr Faculty & Head IT,
Information Technology Division,

Course Fee

Fee per participant on Single Occupancy **Rs.48,000 + 18% GST**	**Rs. 43,000 + 18% GST** Each, For batch of Five & above
Fee per participant on Twin Sharing Occupancy **Rs.42,000 + 18% GST**	**Rs. 38,000+18% GST** Each, For batch of Five & above
Non-Residential Fee per Participant **Rs.35,000 + 18% GST**	**Rs. 30,000 + 18% GST** Each, For batch of Five & above

GST @18% is to be paid extra and above the training fee as training. **PAN Card No.** AAATT3439Q. **GST No: 36AAATT3439Q1ZV, HS No.: 999293** (under commercial training or coaching services – clause 65(105) (ZZC) of Finance act – 1994).

Programme fee is to be paid in in favour of **"THE INSTITUTION OF ENGINEERS (INDIA) – ENGINEERING STAFF COLLEGE OF INDIA"** by **Electronic Fund Transfer (EFT)** to ESCI – **Axis Bank** A/c No. **912010049234564** with The Axis Bank Ltd, Old Mumbai Hwy, Cyberhills Colony, P Janardhan Reddy Nagar, GachiBowli Hyderabad-500032 by NEFT/ RTGS/ IFSC Code No. UTIB 0000733 – MICR No.500211020. **While using EFT method of payment, please ensure to communicate us your company name, our invoice reference and programme title.**

Registration

To register manually please send your nominations giving details of name, designation, contact address, email address, mobile no, telephone and fax number of the participant along with the details of mode of payment of fee, addressed to : **it@escihyd.org**

A Certificate of participation will be awarded to each participant on conclusion of the programme

Glimpses of our Recent Programmes





Information Technology Division, Engineering Staff College of India
Gachi Bowli, Hyderabad – Telangana 500 032
Phone: 040 – 66304100 (EPABX) 66304123/24/25 (Direct), 8886661060 Fax: 040 – 66304103
Email: it@escihyd.org, **web portal**: www.escihyd.org