



Diploma in CYBER SECURITY

Empowering leaders for tomorrow's
cyber defense landscape

-  **Starting: April 2025**
-  **4-Months Diploma**
-  **Rs. 170,000/- (+5% SST)**

Courses Included:

- 1** Cybersecurity Standards and Frameworks
- 2** Cybersecurity Governance and Compliance
- 3** Ethical Hacking and Penetration Testing
- 4** Digital Forensics and Incident Response

In
collaboration with



021 38104700 EXT (1154)



cict@iba.edu.pk



+92 326 2434642

Learning Outcomes:

Upon completion of the program, participants will be able to:

- Understand cybersecurity standards and frameworks.
- Implement ISO 27001 ISMS and NIST Cybersecurity Framework.
- Integrate standards into organizational practices.
- Grasp cybersecurity governance and compliance principles.
- Develop effective security policies and incident reporting mechanisms.
- Conduct security audits and ensure regulatory adherence.
- Design and deliver cybersecurity awareness programs.
- Learn ethical hacking principles and legal considerations.
- Perform vulnerability assessments and penetration testing.
- Secure web apps, networks, and counter social engineering.
- Understand digital forensics and incident response roles.
- Acquire, preserve, and analyze digital evidence effectively.
- Address web app vulnerabilities (OWASP Top 10) and perform CIS benchmarking.



Course topics

1

Cyber Security Governance and Compliance

- Understanding Cybersecurity Threats & Attack Vectors
- Information Security (IS) Governance Roles & Responsibilities
- Risk Management: Identifying, Analyzing, and Treating IS Risks
- IS Program Management & Success Metrics
- Developing a Robust IS Incident Response Plan
- Post-Incident Review & Continuous Improvement

3

Cyber Security Standards and Frameworks

- Overview of Information Security Frameworks (ISO 27001, PCI DSS)
- SECP & Telecom Sector Cybersecurity Frameworks
- NIST Cybersecurity Incident Handling
- Understanding the Attack Lifecycle with MITRE ATT&CK
- Implementing Cybersecurity Controls and Best Practices
- Compliance Monitoring and Reporting

2

Ethical Hacking and Penetration Testing

- Introduction to Ethical Hacking & Penetration Testing
- Information Gathering & Reconnaissance Techniques
- Scanning, Enumeration, and Vulnerability Identification
- Exploitation Tools & Post-Exploitation Techniques
- Web Application & Wireless Network Security
- Social Engineering Attacks: Types and Defenses

4

Digital Forensics and Incident Response

- Introduction to Digital Forensics & Incident Response
- Computer & Device Forensics: Data Acquisition & Handling
- Windows Forensics: Registry, Logs, & Memory Analysis
- Steganography Detection & Image File Forensics
- Malware Analysis: Static, Dynamic, and Reverse Engineering
- Incident Response Planning, Team Roles, & Playbooks