GFSU

GFSU

NAAC ACCREDITED 'A' GRADE

Gujarat Forensic Sciences University

Knowledge | Wisdom | Fulfilment

विद्या अमृतं अश्नुते

Gujarat Forensic Sciences University, A State University under the Home Department, Govt. of Gujarat & Recognized by UGC

Introduces IBA/RBI Recognized

Certified Information Security Professional (CISP)

Course Details

6 Modules related to cyber security concepts, regulatory & compliance

Course Duration

6 Months Online
(virtual/class room, Hands-on lab).
40 Hours Virtual or Offline Classes
40 Hours Hands-on Practice
4 Weeks Capstone Project
2 Mock Tests

Who Can apply ?

• Banks/ Bankers working in IT
• Students/prospective employees desirous of beccomming cyber security exprets

Registrations for eligible candidates will commence from 11th December , 2017

Course Fee:

INR 50,000/-
(Incl. Application, Tution & Examination Fee)

Contact Details:

Sector-9, Gandhinagar-382007, India
Phone: 079-23977102/103/104/113, GFSU
E-mail: registrar@gfsu.edu.in
         cyber_ibatrg@gfsu.edu.in

VISIT: http://www.gfsu.edu.in/ibarbi-approved-certified-information-securi-ty-professional-course-cyber-security/

Certified
Information Security Professional (CISP)

CISP Course

Data security is a critical new front in the combat counter to financial crime. Until now, there is no single technology for it to handle such type of cyber threats, the only way to prevent is to impart the knowledge of identification, protection and defending skills and techniques. The mission of this certification course is to enable the participants to gain advanced cyber security skills to help the organization to detect, protect and respond from critical cyber attacks. The course modules covers cyber security techniques, Digital Forensics investigation, and incident response strategies.

Key Points

• The emerging threat landscape of cyber attacks on the banking and other sector of the country.

• Identifying the source of an attack through root cause analysis.

• Possible attacks on various network topologies and it's components.

• Strategies followed in assessing the web and mobile application.

• Handling & Responding to the cyber attacks.

• Effective methodologies followed under various digital investigations.

• Strategies followed in immediate fixation, short & long-term fixation of vulnerabilities encountered in an incident.

• Malware detection and analysis.

• Protecting the digital assests from the cyber attacks.

Course Outcome

• Information Assurance Strategy.

• Essential tools for hardening and securing the infrastructure.

• Build strategy to respond to diverse set of incidents.

• Effective cyber incident response & crisis management .

• Making the organization intellectual properties to be invulnerable to cyber attacks.

• Earns the key knowledge on the emerging and evolving IT and IS technologies.

Modules

Module 1: Introduction to Cyber Security.

Module 2: Cyber Security Tactics, Techniques & Procedures.

Module 3: Cyber Defence.

Module 4: Digital Forensic Investigation Techniques.

Module 5: Incident Response Management.

Module 6: Information Security Governance & Risk Management.

Practical Lab Scenarios

• Identification of Vulnerable Systems and Services.

• Data breach investigation.

• Log Analysis.

• Network traffic analysis & Threat Identification.

• Mobile Forensics.

• Detection of Web Application Vulnerabilities.

• Email Investigation.

Tools & Technologies

• Advanced Cyber Defence tools .

• Network & Web Exploitation Tools .

• Computer & Network Forensic Tools .

• Malware Analysis Tools .