multisoft
Systems

Certified in Governance, Risk and Compliance (CGRC) Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The Certified in Governance, Risk, and Compliance (CGRC) training course by Multisoft Systems provides professionals with comprehensive skills essential for effectively managing organizational risks, regulatory compliance, and robust governance practices.

Module 1: Information Security Risk Management Program

- ✓ Understand the foundation of an organization information security risk management program
- ✓ Understand risk management program processes
- ✓ Understand regulatory and legal requirements

Module 2: Scope of the Information System

- ✓ Define the information system
- ✓ Determine categorization of the information system

Module 3: Selection and Approval of Security and Privacy Controls

- ✓ Identify and document baseline and inherited controls
- ✓ Select and tailor controls to the system
- ✓ Develop continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)
- ✓ Review and approve security plan/Information Security Management System (ISMS)

Module 4: Implementation of Security and Privacy Controls

- ✓ Implement selected controls
- ✓ Document control implementation

Module 5: Assessment/Audit of Security and Privacy Controls

- ✓ Prepare for assessment/audit
- ✓ Conduct assessment/audit
- ✓ Prepare the initial assessment/audit report
- ✓ Review initial assessment/audit report and perform remediation actions

- ✓ Develop final assessment/audit report
- ✓ Develop remediation plan

Module 6: Authorization/Approval of Information System

- ✓ Compile security and privacy authorization/approval documents
- ✓ Determine information system risk
- ✓ Authorize/approve information system

Module 7: Continuous Monitoring

- ✓ Determine impact of changes to information system and environment
- ✓ Perform ongoing assessments/audits based on organizational requirements
- ✓ Review supply chain risk analysis monitoring activities (e.g., cyber threat reports, agency reports, news reports)
- ✓ Actively participate in response planning and communication of a cyber event
- ✓ Revise monitoring strategies based on changes to industry developments introduced through legal, regulatory, supplier, security and privacy updates
- ✓ Keep designated officials updated about the risk posture for continuous authorization/approval
- ✓ Decommission information system