Training Course	**ROCHESTON CyberSecurity Compliance Officer (RCCO) Certification**
Course Language	**English**
Course Duration	**Total Number of hours : 40 hours** **Days : 5 days** **Time: 8 am – 4pm**
Course Objectives	**The process of continually planning, doing, checking, and acting has a dizzying amount of protocol, paperwork, and intricacies associated with it. Cybersecurity initiatives do not become viable until compliance is established.** **In this RCCO course, participants will identify opportunities to facilitate leadership in the cybersecurity field, and arm the themselves with knowledge to participate in the cyber security assessment of enterprises in different sectors. A RCCO officer will become a sought after strategic partner in cybersecurity controls for organizations.**

Course Content	**Course Key Topic Area Includes:** **Domain 1: DATA Protection** **Domain 2: Scanning, Logging and Monitoring** **Domain 3: Infrastructure Security** **Domain 4: Extreme Hacking Penetration Testing** **Domain 5: Cyber Forensics** **Domain 6: Identity and User Protection** **Domain 7: Hardware Security** **Domain 8: Application Security** **Domain 9: OS Security** **Domain 10: Governance**
Learning Outcomes	**At the end of the program the trainees will be able to:** - **Will be acquainted with the different standards, regulations and protocols constituting the backbone for sustaining cybersecurity in specific industries** - **Communicate risk and need for compliance to organizations and brief board members on cyber threats and attacks.** - **Educate owners and managers, and determine which standards are applicable to the specific industry** - **Enforce guidelines of cyber risk management set in different globally recognized national and international standards and protocols, that are relevant to the particular industry** - **Appreciate that employee breaches could be a fundamental reason behind cyber risk and generate awareness on the need for ethical adherence to policies** - **Ensure that business owners, managers and employees understand ethics and follow best practices for cybersecurity controls** - **Regular monitoring via internal on-site auditing, reviewing reports and access information, etc.** - **Define third-party responsibilities in terms of cyber security procedures, and strategize over necessary responses in the event of privacy breaches**

Target Audience	**Targeted at individuals who are responsible for framing and implementing an organizations IT and Cybersecurity infrastructure, this can include Admin, HR and Legal teams as well.**
Course Material /Technology used/ Details Relevant to the course.	**Electronic Kit via Cyberclass (ROCHESTON's E-Learning Platform) inclusive of online Course Materials for 1 year access.**
Course Fees	**QAR 6,000 (inclusive of Exam Fee of USD400)** **15% discount on online registration.**