GTC International Consulting Limited
Riverbank House
1 Putney Bridge Approach
Fulham, London, SW6 3BQ
T: +44(0)2037055710
E:enquiries@thegtcgroup.com
W: www.thegtcgroup.com

Cyber Security: Developing a Cyber-security Plan

COURSE OVERVIEW

This course provides practical guidance on creating a comprehensive strategy to protect organizational assets, data, and systems from cyber threats. It covers essential elements of a cybersecurity plan, including policy development, access controls, incident response, compliance, and employee awareness. Participants will learn how to assess risks, identify vulnerabilities, and establish security objectives aligned with business goals. Through a structured framework, participants will gain the knowledge to design, implement, and maintain effective cybersecurity plans tailored to their organization's needs, whether in small businesses, enterprises, or public sector environments.

WHO SHOULD ATTEND?

This course is designed for IT managers, cybersecurity professionals, risk officers, compliance personnel, and business leaders responsible for protecting digital assets and ensuring business continuity. It also benefits individuals involved in IT governance, policy development, or strategic planning who want to understand how to build a strong cybersecurity framework. In addition, small business owners, project managers, and aspiring cybersecurity practitioners will find this course especially valuable in learning how to create and implement a tailored cybersecurity plan suited to their organization's size and risk profile.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Understand the key components and purpose of a cybersecurity plan.
- Assess organizational risks and identify critical vulnerabilities.
- Define cybersecurity objectives aligned with business goals.
- Develop policies and procedures for access control, data protection, and threat management.
- Establish incident response and recovery strategies.
- Ensure compliance with relevant security standards and regulations.
- Promote a security-aware culture through employee training and awareness programs.
- Implement monitoring and reporting mechanisms to measure the effectiveness of the cybersecurity plan.
- Customize a cybersecurity framework to suit different organizational types and sizes.
- Maintain and update cybersecurity plans to address emerging threats and changes in technology.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- Designing and implementing a comprehensive cybersecurity plan.
- Risk assessment and vulnerability identification.
- Developing security policies and access controls.
- Incident response planning and compliance management.
- Promoting employee cybersecurity awareness.
- Aligning security objectives with business goals.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.
1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded