Cyber Security, Legal Risk Management & Governance Strategies

Duration: 5 Days

Language: en

Course Code: PI1-112

Objective

Upon completion of this course, participants will be able to:

- Meet ISO requirements in information security.
- Identify cyber security threats.
- Implement the latest cyber security strategies to reduce risks.
- Comply with the audit process and legal standards around cyber security.
- Stay up to date with the most efficient ways to combat cyber threats.
- Handle personal information more securely in line with data compliance.

- Understand the legal risks regarding a cybersecurity breach.

Audience

This course is aimed at anyone who requires a greater understanding of cybersecurity and the threats the online world poses for businesses and organisations. It would be most beneficial for:

- Information Security Managers
- Cyber Security Analysts
- Data Protection Managers
- Business Information Security Officers
- Cyber Security Project Managers
- Business owners
- Operations Managers
- IT Managers
- Senior staff members

Training Methodology

This course uses a wide range of adult learning methods to provide a comprehensive but direct understanding of cybersecurity and how to demonstrate best practices to protect businesses and customers.
This course will provide presentations, interactive exercises, case studies, and video materials to better understand cybersecurity, data compliance, legal risks, and audit processes. Participants will participate in interactive exercises to identify threats and discover how best to manage them. By the end of the course, participants will have the skills and knowledge necessary to implement the correct tools, policies, procedures, and practices to prevent the possibility of a cyber-attack.

Summary

Thanks to technological advancements and the exponential rate at which technology grows, companies must be more vigilant regarding cybersecurity. Businesses and organisations always develop better ways to prevent cyber-attack threats or damage. These include hacking, malware viruses, password attacks, DDoS attacks, and many more.

Cybercriminals are always looking for new ways to exploit vulnerabilities in computer systems. Unfortunately, they are becoming more sophisticated in their approach to cyber-attacks. This means businesses and organisations must develop more secure safeguards to protect their information and customers or clients.
Thanks to more strategic planning, businesses and organisations are also devising more secure ways to minimise damage, prevent information loss, and anticipate new security threats. With up-to-date security software training and knowledge of potential security breaches, cybercriminals find it increasingly harder to attack businesses and organisations.

Course Content & Outline

Section 1: Cyber Security Management

- What is cyber security?
- Learning how to identify online threats and risks.
- How to securely store information online.
- How to comply with legal standards regarding data compliance.
- How to develop skills in combating cyber threats.

Section 2: Audit, Legal, & ISO Standards

- Learn how to identify cyber risks.
- How to adhere to audit and legal standards.
- How to comply with data compliance.
- How to apply up-to-date security measures.
- How to develop policies and procedures regarding cyber security.
- How to communicate security awareness.

Section 3: Implement New Technologies

- Learning how to understand Key Risk Indicators (KRIs).
- How to implement security controls.
- How to effectively manage cyber risks and issues.
- How to produce a cybersecurity incident log and best manage incidents.
- Applying cyber countermeasures and continuity plans in case of a crisis.

Section 4: System Applications

- Learn how to execute Firewall applications.
- How to utilise network protocols.
- Being able to produce network safeguarding.
- How to apply certain encryption technologies.
- Learning different roles of management when it comes to cyber security.

Section 5: Current Trends in Cybersecurity

- Learning different cloud types.
- Understanding hacking principles.
- Being able to identify vulnerabilities in systems.
- Understanding blockchain technology.
- Learn how to improve your working knowledge of cyber security and stay up to date.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Assessment Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

IT & Computer Application, Law, Contracts and Legalities, Technology, AI, Data and Visualisation

Tags

Cyber security, Threats, Strategies, Governance, Legal Risk, technology, IT, Firewall, Network Protocol

Related Articles

Navigating Cyber Threats: A Full Guide to Risk Management

In the digital era, cybersecurity risk management is paramount. This blog post delves into the process of identifying, assessing, and mitigating cyber risks. Learn about AI-driven solutions, UK laws, and how to integrate risk management with your business objectives.