Cyber Security, Legal Risk Management

Duration: 4 Days

Language: en

Course Code: PI1-103

Objective

- To be able to determine cyber security risks in data management
- To be able to develop skills to identify and combat threats relating to cyber security
- To be able to learn all cyber security risks, issues and threats
- To be able to put effective controls and solutions from cyber threats in place
- To be able to develop policy and communications that address information governance, compliance and standards and also address legal and audit requirements
- To be confident in communicating security awareness and training
- To be able to improve existing cyber security strategies, confidently review tools and discuss security, confidentially, and business solutions to reduce operational risks
- To be able to improve working knowledge, global industry standards and best practices in cyber security and information risk management
- To be able to apply ISO standards including ISO15489 Records Management Compliance and ISO 27001 Information security management to reduce threats and risks

Audience

- Technology Engineers,
- Chief Technology Officer
- Chief Information Officer
- Chief Risk Officers
- Application Development Personnel
- Data Research Personnel
- Professionals wanting to learn about cyber security strategies, information governance and ISO standards
- Those who work in IT systems management, legal, risk management, information security, projects, HR and procurement
- Those looking to transition to management and IT security roles

Training Methodology

Teaching takes place in a variety of settings including face to face in a classroom environment and will ensure that participants can expand their knowledge of the subject and increase their skill set. The course is delivered via various methods by a specialist tutor. This will include PowerPoint presentations, reviewing articles and other relevant materials, group or individual exercises and discussions. There may be some independent work set, and the course will involve a requirement to submit articles to demonstrate understanding and an end of course test. Note-taking is encouraged, and you are welcome to use electronic devices to do this.

The course manual will form part of the learning but give you references for the future. You are encouraged to ask questions and, if needed, spend time one to one with your tutor to go over any issues. During your time in the classroom, you will be able to network with peers in similar roles.

Summary

The digital age continues to evolve at an astounding pace. This means all organisations are now using technology that comes at a price. There is an increased risk of cyberattacks stealing information and the requirement to comply with legal regulations, audits, and other compliance issues. If you are working in the field, this course will offer you everything you need to know about protecting data and cyber security. It will run through ways to reduce the risks within an organisation and discuss meeting all global compliance standards. There will be information on how to protect end-user privacy and work within the confines of ISO regulations for information security management.

The course keeps up with the latest best practices and shows you all the required skills to manage information, ensure that legal regulations and standards are met and implement audit controls. You will also learn about how to stay safe when working online and how you can protect your personal and sensitive information. This is a must for those responsible for mitigating risks from cybercrime and help you understand the devastating effects of failing to protect your organisation correctly. All data-driven companies need to have at least one expert on their team. The course covers all elements of the data life cycle and helps you identify cyber security threats. In turn, you will learn how to bring about controls that will assist in reducing this risk and danger in the form of policies, strategies and systems. On top of this, you need to be aware of the ISO standards' requirements for audit and legal compliance standards. The course also covers new technologies like AI, IoT, cloud computing and

Blockchain as it is essential that you understand both the benefits and risks.

Course Content & Outline

Section 1: An Introduction to Cyber Security and Information Security

- Introduction to cyber security
- What are online threats, risks and issues?
- Business continuity, fraud and disaster management
- ISO27001 and related standards
- The governance of data, information and records
- Establishing the roles and responsibilities for information governance

Section 2: Audit requirements, Legalities, Risk Awareness and ISO

- Understanding and ranking physical and electronic risks
- Management of compliance: audit and legal risks
- Management compliance: documents and records
- A review of ISO15489 Records Management
- How to apply ISO27001 information security controls
- How to develop policies, procedures and standards
- A look at the current threat and trend analysis

Section 3: Implementation and Training for New Technologies

- What is a Key Risk Indicator (KRI)
- Project implementation plans and controls
- Developing risk and issue management plans
- Developing business continuity plan
- Cybersecurity incident management
- Cybersecurity crisis management

Section 4: IT Applications: Security and Safety

- Network protocols/communications/access
- Firewall/application/network security
- User management, including role-based access controls
- Encryption technologies/standards
- Email /web security
- Cyber security systems

Section 5: Cloud, IoT and Blockchain: New Trends in Cybersecurity

- Cloud computing, including public, private and hybrid
- Blockchain technology
- What is hacking
- The mathematics of hacking
- Vulnerabilities in the systems: tracing and preventing

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 Accreditation 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

Tags

Cyber security , legal risk management , cyber , IT , technology security

Related Articles

Navigating Cyber Threats: A Comprehensive 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.

YouTube Video

https://www.youtube.com/embed/RCd9Q42fT3E?si=hC7KTNVVH6wrri1u