Cybersecurity Risk Mitigation

Duration: 5 Days

Language: en

Course Code: IND18-103

Objective

During this course, you'll learn:

- Understand the vitality of cybersecurity and risk mitigation within an organisation.
- Identify the relevant regional laws and regulations in aviation industries and how they may apply.
- Analyse various models for cybersecurity and their benefits and limitations, including the UK CAA Cybersecurity Oversight Process for Aviation (CAP1753).
- Assess good standards and practices of aviation cybersecurity and recognise these within different aviation organisations.
- Investigate data, categorise and prepare evidence for regular cybersecurity audits.
- Comprehend the synergy between safety management systems (SMS) and security management systems (SeMS).
- Evaluate the consequences of poor cybersecurity and a lack of risk mitigation.

Audience

This course is designed for anyone in the aviation industry responsible for managing information systems and maintaining cybersecurity. It would be most beneficial for:

- IT Engineers
- Chief Information Officers (CIOs)

- IT Managers
- Cybersecurity Managers
- Risk Managers
- Risk Analysts
- Compliance Officers

Training Methodology

This course uses a variety of adult learning styles to aid full understanding and comprehension. Participants will review case studies of existing cybersecurity systems to highlight key protective features and areas for improvement.
The participants will be provided with all the necessary tools and equipment to engage fully with the learning methods. They will participate in presentations, group discussions, practical demonstrations, and group activities. This collection of learning methods will ensure the participants fully develop their knowledge and skills relating to the taught content.

Summary

The aviation industry is vast and handles an incredible amount of data, whether regarding customer information or any data contributing to the organisation's daily functions. A strong focus on implementing and maintaining a cybersecurity system must be placed to ensure all functions and processes can continue without interruption.
Cybersecurity is essential for maintaining the security of any electronic system housing important data. To successfully secure this data, conducting regular risk audits of the system is crucial to identify all hazards and risks that are likely to occur. This information must later be categorised and prioritised to allow for preventative and corrective actions to be decided on and integrated.
Cybersecurity risk mitigation is a vital step in cybersecurity. Preventing risks before they occur is ideal for preserving business functions. Several risk mitigation strategies can be implemented within the system, and individuals involved must be competent at understanding how these work, monitoring their performance and recognising any faults as they occur.

Course Content & Outline

Section 1: Introduction to Cybersecurity

- Defining what cybersecurity is and why it's important within an organisation.

- Exploring the consequences of poor cybersecurity and its detriment on organisational information and stakeholders.
- Common issues faced within cybersecurity and how to appropriately prepare for them.
- Guaranteeing customer and organisational data can remain safe and protected at all times.
- Typical methods of cybersecurity utilised within aviation.

Section 2: Assessing Cyber Risk

- Conducting a risk audit to identify system risks, their probability of occurring and the detriment they would have on the organisation.
- Analysing risk audit data to categorise risks based on probability and severity.
- Utilising risk audit data to create a risk management plan detailing all risks, preventable actions and corrective actions.
- Balancing preventative action with corrective action based upon each risk.
- Integrating risk oversight into corrective action.

Section 3: Cybersecurity Regulations

- Reviewing organisation-specific and regional cybersecurity regulations.
- Ensuring full compliance with all cybersecurity regulations and standards.
- Analysing ICAO Annex 17 and how this would apply to the organisation.
- Implementing the Information Security Management System (ISMS) and ensuring accessibility to all necessary personnel.

Section 4: Cybersecurity Mitigation Strategies

- Exploring various risk mitigation strategies to protect valuable data.
- Establish secure network access controls and monitor their use regularly.
- Carefully supporting network traffic to prevent system overload that may leave data vulnerable.
- Creating a disaster management plan to work alongside the general risk management strategies.

Section 5: Monitoring Cybersecurity

- Enforcing regular system checks to ensure full productivity and security.
- Implementing a continuous cyber risk monitoring system to identify and alert to problems before they occur.
- Conducting regular maintenance on the physical,and electronic systems themselves to eliminate the risk of physical faults causing system faults.

- Updating risk management plans through regular system monitoring.

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

Aviation, IT & Computer Application, Technology

Tags

Risk Mitigation, Cyber security

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

YouTube Video

https://www.youtube.com/embed/o9jTy5pJ6pw?si=G84EbORL81-K-97K