تقليل مخاطر الأمان السيبراني في العالم العربي

Duration: 5 Days

Language: ar

Course Code: IND18-103

Objective

:خلال هذه الدورة، ستتعلم

- .فهم أهمية الأمن السيبراني وتخفيف المخاطر داخل المؤسسة
- .تحديد القوانين واللوائح الإقليمية ذات الصلة في صناعات الطيران وكيفية تطبيقها
- تحليل النماذج المختلفة للأمن السيبراني وفوائدها وقيودها، بما في ذلك عملية الإشراف على الأمن السيبراني للطيران (CAP1753). في المملكة المتحدة
- .تقييم المعايير والممارسات الجيدة للأمن السيبراني في الطيران والتعرف عليها داخل مختلف منظمات الطيران
- .التحقيق في البيانات وتصنيفها وإعداد الأدلة للمراجعات الدورية للأمن السيبراني
- .(SeMS) وأنظمة إدارة الأمن (SMS) فهم التآزر بين أنظمة إدارة السلامة
- .تقييم عواقب ضعف الأمن السيبراني وغياب تخفيف المخاطر

Audience

تم تصميم هذه الدورة لأي شخص في صناعة الطيران يكون مسؤولاً عن إدارة نظم المعلومات والحفاظ على الأمن السيبراني. ستكون مفيدة بشكل خاص لـ:

- مهندسي تكنولوجيا المعلومات
- رؤساء قسم المعلومات (CIOs)
- مديري تكنولوجيا المعلومات
- مديري الأمن السيبراني

- مديري المخاطر
- محللي المخاطر
- مسؤولي الامتثال

Training Methodology

يستخدم هذا الدورة مجموعة متنوعة من أساليب التعلم للكبار لتعزيز الفهم والاستيعاب الكامل. سيقوم المشاركون بمراجعة دراسات حالة لأنظمة الأمن السيبراني الحالية لتسليط الضوء على الميزات الوقائية الرئيسية والمجالات التي تحتاج إلى تحسين.

سيتم تزويد المشاركين بجميع الأدوات والمعدات اللازمة للتفاعل الكامل مع أساليب التعلم. سيشاركون في عروض تقديمية، ومناقشات جماعية، وعروض عملية، وأنشطة جماعية. ستضمن هذه المجموعة من أساليب التعلم تطوير المشاركين لمعارفهم ومهاراتهم المتعلقة بالمحتوى المُدرّس بشكل كامل.

Summary

تُعتبر صناعة الطيران من القطاعات الواسعة التي تتعامل مع كميات ضخمة من البيانات، سواء كانت تتعلق بمعلومات العملاء أو أي بيانات تسهم في العمليات اليومية للمنظمة. يجب التركيز بشكل كبير على تنفيذ وصيانة نظام للأمن السيبراني لضمان استمرار جميع الوظائف والعمليات دون انقطاع.

يُعد الأمن السيبراني ضروريًا للحفاظ على أمان أي نظام إلكتروني يحتوي على بيانات حساسة. ولتأمين هذه البيانات بفعالية، من الضروري إجراء تدقيقات دورية للمخاطر في النظام لتحديد جميع المخاطر والتهديدات المحتملة. يجب تصنيف هذه المعلومات لاحقًا وتحديد أولوياتها للسماح باتخاذ وتنفيذ الإجراءات الوقائية والتصحيحية.

تخفيف مخاطر الأمن السيبراني هو خطوة حيوية في مجال الأمن السيبراني. يُعتبر منع المخاطر قبل حدوثها مثاليًا للحفاظ على استمرارية الأعمال. يمكن تنفيذ عدة استراتيجيات لتخفيف المخاطر داخل النظام، ويجب أن يكون الأفراد المعنيون مؤهلين لفهم كيفية عمل هذه الاستراتيجيات، ومراقبة أدائها، والتعرف على أي خلل عند حدوثه.

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

عند إتمام هذه الدورة التدريبية بنجاح، سيحصل المشاركون على شهادة إتمام التدريب من Holistique Training. وبالنسبة للذين يحضرون ويكملون الدورة التدريبية عبر الإنترنت، سيتم تزويدهم بشهادة إلكترونية (e-Certificate) من Holistique Training.

شهادات Holistique Training معتمدة من المجلس البريطاني للتقييم (BAC) وخدمة اعتماد التطوير المهني المستمر (CPD)، كما أنها معتمدة وفق معايير ISO 9001 وISO 21001 وISO 29993.

لهذه الدورة من خلال شهاداتنا، وستظهر هذه النقاط على شهادة إتمام (CPD) يتم منح نقاط التطوير المهني المستمر واحدة عن كل ساعة CPD يتم منح نقطة، CPD ووفقًا لمعايير خدمة اعتماد Holistique Training. التدريب من لأي دورة واحدة نقدمها حاليًا CPD حضور في الدورة. ويمكن المطالبة بحد أقصى قدره 50 نقطة.

Categories

إدارة الطيران والعمليات الجوية, تطبيقات تكنولوجيا المعلومات والكمبيوتر, التكنولوجيا

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