ISO 27001 قائد التنفيذ: مراقب رئيسي (نظام إدارة أمان المعلومات)

المدة: 5 يوم

اللغة: ar

كود الكورس: PI1 - 141

هدف الكورس

:By the end of this course, participants will be able to

- .Interpret and apply ISO/IEC 27001:2022 requirements effectively
- .Develop an ISMS framework tailored to organisational needs
- .Conduct risk assessments and implement appropriate security controls
- .Establish monitoring, measurement, and continuous improvement processes
- .Prepare organisations for ISO 27001 certification and external audits

الجمهور

هذه الدورة مثالية لـ:

- مديري ومسؤولي أمن المعلومات.
- المتخصصين في تكنولوجيا المعلومات والامتثال.
- خبراء إدارة المخاطر.
- مديري المشاريع الذين يقودون تنفيذ نظم إدارة أمن المعلومات.
- المستشارين والمدققين الباحثين عن خبرة في معيار ISO 27001.

منهجية التدريب

يجمع هذا الدورة بين الجلسات التفاعلية وورش العمل ودراسات الحالة الواقعية. سيقوم المشاركون بتطبيق مبادئ المعيار على سيناريوهات تطوير نظام إدارة أمن المعلومات المحاكية وتمارين إدارة المخاطر.

الملخص

يوفر هذا البرنامج التدريبي المتقدم للمهنيين المعرفة والأدوات العملية اللازمة لتصميم وتنفيذ وإدارة نظام فعال لإدارة أمن

المعلومات (ISMS) بما يتماشى مع معيار ISO/IEC 27001:2022.

سيكتسب المشاركون فهماً عميقاً لمنهجيات تقييم المخاطر، وعناصر التحكم الأمنية، وعمليات التوثيق، وأطر الحوكمة الضرورية لتحقيق والحفاظ على شهادة ISO 27001. من خلال مزيج من النظريات والتمارين العملية، يُعد هذا البرنامج المهنيين لقيادة مشاريع تنفيذ ISMS التي تعزز من مرونة أمن المعلومات والامتثال والثقة التنظيمية.

محتوى الكورس والمخطط الزمني

Section 1: Introduction to ISO/IEC 27001 and ISMS Fundamentals

- Overview of ISO 27001 and the ISO/IEC 27000 family.
- Understanding the structure and clauses of ISO 27001:2022.
- Core ISMS principles and terminology.
- Business benefits of information security and certification.

Section 2: Planning and Scoping an ISMS

- Determining ISMS scope and boundaries.
- Identifying internal and external issues and interested parties.
- Establishing ISMS objectives and policies.
- Roles, responsibilities, and leadership involvement.

Section 3: Risk Assessment and Control Implementation

- Risk identification, analysis, and evaluation methods.
- Applying Annex A controls and mapping them to ISO 27002:2022.
- Developing the Statement of Applicability (SoA).
- Implementing risk treatment plans and monitoring mechanisms.

Section 4: ISMS Documentation, Operation and Performance

- Developing ISMS documentation and mandatory records.
- Managing incidents and nonconformities.

- Measuring ISMS performance and continual improvement.
- Internal audit preparation and management review process.

Section 5: Implementation Leadership and Certification Readiness

- Change management in information security.
- Communicating ISMS objectives across departments.
- Ensuring compliance with legal, regulatory, and contractual obligations.
- Certification process overview and external audit readiness.

تفاصيل الشهادة

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

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

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.

التصنيفات

الذكاء الاصطناعي وإدارة البيانات, تطبيقات تكنولوجيا المعلومات والكمبيوتر

مقالات ذات صلة

Top 10 Cybersecurity Courses And Training Programs

In today's digital era, mastering cybersecurity is vital. Courses like CISSP, CEH, and CISM cover security fundamentals, risk management, access control, and software security. They prepare professionals for certifications, incident handling, identity management, compliance, and resilient application development, ensuring robust protection of digital .assets