# أهمية استراتيجيات الأمان السيبراني وإدارة المخاطر القانونية والحوكمة في العالم العربي

**المدة:** 5 يوم

**اللغة:** ar

**كود الكورس:** PI1-112

## هدف الكورس

:عند إتمام هذه الدورة، سيكون المشاركون قادرين على

- .في أمن المعلومات ISO تلبية متطلبات
- .تحديد تهديدات الأمن السيبراني
- .تطبيق أحدث استراتيجيات الأمن السيبراني لتقليل المخاطر
- .الامتثال لعملية التدقيق والمعايير القانونية المتعلقة بالأمن السيبراني

- مواكبة أحدث الطرق الفعالة لمكافحة التهديدات السيبرانية.
- التعامل مع المعلومات الشخصية بشكل أكثر أمانًا وفقًا للامتثال للبيانات.
- فهم المخاطر القانونية المتعلقة بخرق الأمن السيبراني.

## الجمهور

تهدف هذه الدورة إلى أي شخص يحتاج إلى فهم أعمق للأمن السيبراني والتهديدات التي يشكلها العالم الرقمي على الشركات والمؤسسات. ستكون هذه الدورة مفيدة بشكل خاص لـ:

- مديري أمن المعلومات
- محللي الأمن السيبراني
- مديري حماية البيانات
- ضباط أمن المعلومات التجارية
- مديري مشاريع الأمن السيبراني
- أصحاب الأعمال
- مديري العمليات
- مديري تكنولوجيا المعلومات
- أعضاء الإدارة العليا

## منهجية التدريب

يستخدم هذا الدورة مجموعة واسعة من أساليب تعليم الكبار لتقديم فهم شامل ومباشر للأمن السيبراني وكيفية تطبيق أفضل الممارسات لحماية الشركات والعملاء.

ستوفر هذه الدورة عروض تقديمية، وتمارين تفاعلية، ودراسات حالة، ومواد فيديو لفهم أفضل للأمن السيبراني، والامتثال للبيانات، والمخاطر القانونية، وعمليات التدقيق. سيشارك المشاركون في تمارين تفاعلية لتحديد التهديدات واكتشاف أفضل السبل لإدارتها. بنهاية الدورة، سيكون لدى المشاركين المهارات والمعرفة اللازمة لتطبيق الأدوات والسياسات والإجراءات والممارسات الصحيحة لمنع احتمالية حدوث هجوم سيبراني.

## الملخص

بفضل التقدم التكنولوجي والنمو المتسارع للتكنولوجيا، يجب على الشركات أن تكون أكثر يقظة فيما يتعلق بالأمن السيبراني. تسعى الشركات والمنظمات دائمًا لتطوير طرق أفضل لمنع تهديدات أو أضرار الهجمات السيبرانية. وتشمل هذه التهديدات الاختراق، فيروسات البرمجيات الخبيثة، هجمات كلمات المرور، هجمات حجب الخدمة الموزعة، والعديد من التهديدات الأخرى.

يسعى مجرمو الإنترنت دائمًا للبحث عن طرق جديدة لاستغلال الثغرات في أنظمة الكمبيوتر. وللأسف، أصبحوا أكثر تطورًا في أساليبهم للهجمات السيبرانية. وهذا يعني أن الشركات والمنظمات يجب أن تطور إجراءات حماية أكثر أمانًا لحماية معلوماتها وعملائها أو زبائنها.
بفضل التخطيط الاستراتيجي الأفضل، تقوم الشركات والمنظمات أيضًا بابتكار طرق أكثر أمانًا لتقليل الأضرار، ومنع فقدان المعلومات، والتنبؤ بالتهديدات الأمنية الجديدة. ومع التدريب على أحدث برامج الأمان والمعرفة بالاختراقات الأمنية المحتملة، يجد مجرمو الإنترنت صعوبة متزايدة في مهاجمة الشركات والمنظمات.

## محتوى الكورس والمخطط الزمني

**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.

## تفاصيل الشهادة

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.

## التصنيفات

تطبيقات تكنولوجيا المعلومات والكمبيوتر, الشؤون القانونية والعقود, التكنولوجيا, الذكاء الاصطناعي وإدارة البيانات

## مقالات ذات صلة


**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