ISO للحماية الدورة التدريبية: احتراف إدارة المخاطر وأمن الرقمية المعلومات باستخدام معيار ٢٧٠٠١:٢٠٢٢

مايو ٢٠٢٦ ٢٢ - ١٨

ميلان

(للشخص الواحد) € ٥٧٠٠

Ref: #ISO6647_451784

مقدمة الدورة التدريبية / لمحة عامة:

وبياناتها الحساسة معيار ٢٧٠٠١:٢٠٢٢ ISO أمرًا بالغ الأهمية للمؤسسات يُعد احتراف إدارة المخاطر وأمن المعلومات باستخدام
لم يعد أمن المعلومات مجرد مهمة تقنية، في عصر التحول الرقمي. مع تزايد التهديدات التي تسعى لحماية أصولها الرقمية
Training ومنظمًا. تستعرض هذه الدورة التدريبية منBIG BEN بل أصبح ضرورة استراتيجية تتطلب نهجًا شاملاً السيبرانية،
في كيفية٢٧٠٠١:٢٠٢٢ المعلومات (ISMS) وفقًا لأحدث إصدار من معيارISO المبادئ الأساسية لنظام إدارة أمن Center
بالإضافة إلى تصميم وتنفيذ ضوابط أمنية تحديد مخاطر أمن المعلومات، تقييمها، ومعالجتها ، من الألف إلى الياء. سنغوص
البروفيسور الممارسات والمعارف في مجال أمن المعلومات وإدارة قوية لحماية المعلومات. تعتمد الدورة على أحدث بفعالية،
أمن المعلومات، وكتابه "The غاري هولمز (Gary Hinson)، الذي قدم مساهمات قيمة المخاطر، مستلهمة من خبراء بارزين مثل
عمليًا لا غنى عنه. ستُمكّن هذه الدورة الذي يُعد "ISO ٢٧٠٠١:٢٠٢٢ Implementation Handbook في تبسيط فهم معايير
ويعزز الثقة لا يلتزم بالمعايير الدولية فحسب، بل يوفر أيضًا المشاركين من بناء نظام إدارة أمن معلومات متكامل دليلا
المشهد الرقمي المتطور. لدى العملاء والشركاء، ويضمن استمرارية الأعمال في حماية قوية ضد التهديدات السيبرانية،

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو أمن المعلومات.
- مديرو تقنية المعلومات.
- مسؤولو حوكمة أمن المعلومات والامتثال.
- مديرو المخاطر.
- مدققو أمن المعلومات الداخليون والخارجيون.
- أعضاء فرق أمن المعلومات وتكنولوجيا المعلومات.
- المستشارون في مجال أمن المعلومات.
- أي شخص مسؤول عن حماية المعلومات في المؤسسة.

القطاعات والصناعات المستهدفة:

- قطاع البنوك والخدمات المالية.
- قطاع الاتصالات.
- القطاع الحكومي والمؤسسات العامة.
- قطاع تكنولوجيا المعلومات وتطوير البرمجيات.
- قطاع الرعاية الصحية.
- القطاع الصناعي والتصنيع.
- التجارة الإلكترونية والبيع بالتجزئة.
- الخدمات الاستشارية.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- إدارة تقنية المعلومات.
- إدارة المخاطر.
- الامتثال والشؤون القانونية.
- التدقيق الداخلي.
- التطوير والبحث.
- العمليات التشغيلية.
- الخصوصية وحماية البيانات.

أهداف الدورة التدريبية:

أتقن المهارات التالية: بنهاية هذه الدورة التدريبية، سيكون المتدرب قد

- فهم المتطلبات الأساسية لمعيار.ISO ٢٧٠٠١:٢٠٢٢
- تحديد وتقييم مخاطر أمن المعلومات بفعالية.
- تطوير وتنفيذ ضوابط أمن المعلومات المناسبة.
- ISO ٢٧٠٠١. إنشاء نظام إدارة أمن المعلومات (ISMS) متوافق مع
- إجراء عمليات التدقيق الداخلي لنظام أمن المعلومات.
- إدارة الحوادث الأمنية والاستجابة لها.
- تحسين أمن المعلومات بشكل مستمر داخل المؤسسة.
- المساهمة في بناء ثقافة أمن معلومات قوية.

منهجية الدورة التدريبية:

وأمن المعلومات بمنهجية شاملة تركز على التطبيق العملي، لتمكين يقدم BIG BEN Training Center هذه الدورة التدريبية تشرح كل بند من بنود المعيار، مع وفقًا لمعيار .٢٧٠٠١:٢٠٢٢ ISO تبدأ الدورة بمحاضرات المشاركين من احتراف إدارة المخاطر يتم تعزيز الفهم من خلال دراسات حالة مستوحاة من التركيز على تفسير المتطلبات وتقديم أمثلة واقعية. نظرية معمقة تحليل التحديات وتطوير حلول عملية. سيناريوهات أمن معلومات حقيقية، مما يتيح للمشاركين

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

٢٧٠٠١:٢٠٢٢ الوحدة الأولى: أساسيات أمن المعلومات ومعيارISO

- مقدمة لأمن المعلومات وأهميته الاستراتيجية.
- نظرة عامة على معيار.٢٧٠٠١:٢٠٢٢ ISO
- مفاهيم ومصطلحات أمن المعلومات الرئيسية.
- فهم سياق المنظمة ومتطلبات الأطراف المعنية.
- نطاق نظام إدارة أمن المعلومات (ISMS).
- دور القيادة في أمن المعلومات.
- تخطيط أمن المعلومات.

الوحدة الثانية: تقييم وإدارة مخاطر أمن المعلومات

- منهجيات تحديد الأصول المعلوماتية.
- تحديد وتقييم مخاطر أمن المعلومات.
- معايير تقييم المخاطر ومعالجة المخاطر.
- صياغة خطة معالجة المخاطر.
- إعداد بيان قابلية التطبيق (.SoA)
- إدارة المخاطر المتبقية.
- المراقبة الدورية للمخاطر.

الوحدة الثالثة: ضوابط أمن المعلومات ((Annex A

- مقدمة لضوابط.Annex A
- ضوابط تنظيمية لأمن المعلومات.
- ضوابط الأشخاص وأمن الموارد البشرية.
- ضوابط الحماية المادية والبيئية.
- ضوابط إدارة العمليات.
- ضوابط إدارة الوصول.
- ضوابط أمن التشفير.

منها الوحدة الرابعة: تنفيذ ضوابط أمن المعلومات والتحقق

- أمن الاتصالات.
- أمن الاكتساب والتطوير والصيانة للأنظمة.
- ضوابط علاقات الموردين.
- إدارة حوادث أمن المعلومات.
- إدارة استمرارية أمن المعلومات.
- متطلبات الامتثال والالتزامات القانونية.
- ضوابط أمن المعلومات المتعلقة بالغيوم (Cloud Security).

والشهادة الوحدة الخامسة: التدقيق الداخلي والتحسين المستمر

- مفاهيم التدقيق الداخلي لأمن المعلومات.
- تخطيط وتنفيذ التدقيق الداخلي.
- إعداد تقارير التدقيق ومعالجة حالات عدم المطابقة.
- مراجعة الإدارة لنظام إدارة أمن المعلومات.
- التحسين المستمر لنظام أمن المعلومات.
- عملية الحصول على شهادة.٢٧٠٠١:٢٠٢٢ ISO
- مواجهتها. التحديات المستقبلية في أمن المعلومات وكيفية

الأسئلة المتكررة:

التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة.

الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

المدة إلى ٢٠-٢٥ بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

مع التحديات يمكن للمؤسسات ضمان بقاء نظام إدارة أمن المعلومات في ظل التطور السريع للتهديدات السيبرانية، كيف الجديدة بفعالية؟ لديها مرنًا وقادرًا على التكيف

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

المخاطر وأمن أحدث متطلبات معيار٢٠٢٢:٢٧٠٠١ ISO ، مع التركيز تتميز هذه الدورة بتقديم محتوى شامل وعميق يغطي الأدوات والتقنيات اللازمة لتصميم، المعلومات. تتجاوز الدورة مجرد الشرح النظري، لتقدم بشكل خاص على الجانب العملي لإدارة مدعومًا مؤسساتهم. يتميز المحتوى بالتوازن بين المفاهيم تنفيذ، وتقييم نظام إدارة أمن معلومات فعال في للمشاركين الذين يسعون لتعزيز خبراتهم في بدراسات حالة واقعية وتمارين تطبيقية. هذه الدورة الأكاديمية وأفضل الممارسات الصناعية، وبناء ثقافة أمن معلومات قوية، مما يجعلهم قادة في حماية الأصول الرقمية، وتأمين البيانات الحساسة، مثالية للمهنيين مجال الحماية الرقمية المتطور.