الدورة التدريبية: احتراف إدارة المخاطر وأمن المعلومات باستخدام معيار ISO 27001:2022 للحماية الرقمية

#ISO6647

الدورة التدريبية ISO: احتراف إدارة المخاطر وأمن المعلومات باستخدام معيار 27001:2022 للحماية الرقمية

مقدمة الدورة التدريبية / لمحة عامة:

يُعد احتراف إدارة المخاطر وأمن المعلومات باستخدام معيار ISO 27001:2022 أمرًا بالغ الأهمية للمؤسسات التي تسعى لحماية أصولها الرقمية وبياناتها الحساسة في عصر التحول الرقمي. مع تزايد التهديدات السيبرانية، لم يعد أمن المعلومات مجرد مهمة تقنية، بل أصبح ضرورة استراتيجية تتطلب نهجًا شاملاً ومنظمًا. تستعرض هذه الدورة التدريبية من BIG BEN Training Center المبادئ الأساسية لنظام إدارة أمن المعلومات (ISMS) وفقًا لأحدث إصدار من معيار ISO 27001:2022، من الألف إلى الياء. سنغوص في كيفية تحديد مخاطر أمن المعلومات، تقييمها، ومعالجتها بفعالية، بالإضافة إلى تصميم وتنفيذ ضوابط أمنية قوية لحماية المعلومات. تعتمد الدورة على أحدث الممارسات والمعارف في مجال أمن المعلومات وإدارة المخاطر، مستلهمة من خبراء بارزين مثل البروفيسور غاري هولمز (Gary Hinson)، الذي قدم مساهمات قيمة في تبسيط فهم معايير أمن المعلومات، وكتابه "The ISO 27001:2022 Implementation Handbook" الذي يُعد دليلًا عمليًا لا غنى عنه. ستُمكّن هذه الدورة المشاركين من بناء نظام إدارة أمن معلومات متكامل لا يلتزم بالمعايير الدولية فحسب، بل يوفر أيضًا حماية قوية ضد التهديدات السيبرانية، ويعزز الثقة لدى العملاء والشركاء، ويضمن استمرارية الأعمال في المشهد الرقمي المتطور.

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:

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

- فهم المتطلبات الأساسية لمعيار ISO 27001:2022.
- تحديد وتقييم مخاطر أمن المعلومات بفعالية.
- تطوير وتنفيذ ضوابط أمن المعلومات المناسبة.
- إنشاء نظام إدارة أمن المعلومات (ISMS) متوافق مع ISO 27001.
- 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:

يقدم BIG BEN Training Center هذه الدورة التدريبية بمنهجية شاملة تركز على التطبيق العملي، لتمكين المشاركين من احتراف إدارة المخاطر وأمن المعلومات وفقًا لمعيار ISO 27001:2022. تبدأ الدورة بمحاضرات نظرية معمقة تشرح كل بند من بنود المعيار، مع التركيز على تفسير المتطلبات وتقديم أمثلة واقعية. يتم تعزيز الفهم من خلال دراسات حالة مستوحاة من سيناريوهات أمن معلومات حقيقية، مما يتيح للمشاركين تحليل التحديات وتطوير حلول عملية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن المعلومات ومعيار ISO 27001:2022

- مقدمة لأمن المعلومات وأهميته الاستراتيجية.
- نظرة عامة على معيار ISO 27001:2022.
- 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.

الوحدة الرابعة: تنفيذ ضوابط أمن المعلومات والتحقق منها

- 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).

الوحدة الخامسة: التدقيق الداخلي والتحسين المستمر والشهادة

- 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 ISO 27001:2022.
- التحديات المستقبلية في أمن المعلومات وكيفية مواجهتها.

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتقديم محتوى شامل وعميق يغطي أحدث متطلبات معيار ISO 27001:2022، مع التركيز بشكل خاص على الجانب العملي لإدارة المخاطر وأمن المعلومات. تتجاوز الدورة مجرد الشرح النظري، لتقدم للمشاركين الأدوات والتقنيات اللازمة لتصميم، تنفيذ، وتقييم نظام إدارة أمن معلومات فعال في مؤسساتهم. يتميز المحتوى بالتوازن بين المفاهيم الأكاديمية وأفضل الممارسات الصناعية، مدعومًا بدراسات حالة واقعية وتمارين تطبيقية. هذه الدورة مثالية للمهنيين الذين يسعون لتعزيز خبراتهم في حماية الأصول الرقمية، وتأمين البيانات الحساسة، وبناء ثقافة أمن معلومات قوية، مما يجعلهم قادة في مجال الحماية الرقمية المتطور.