BLACKBIRD FOR TRAINING

أساسيات ISO/IEC 27001:2022

March 2027 19 – 15

برشلونة (إسبانيا)



أساسيات ISO/IEC 27001:2022

المرجع: 330346_3255054 **التاريخ:** 15 – 19 March 2027 **المكان:** برشلونة (إسبانيا) **الرسوم:** GBP 5900

مقدمة

في ظل تطور التهديدات السيبرانية بشكل متسارع وتعقّدها المستمر، أصبحت أمن المعلومات من أولويات الاستراتيجية العليا للمؤسسات بمختلف أنواعها. فالأفراد والمنظمات باتوا معرضين لمخاطر متعددة مثل فقدان البيانات، الاختراقات، والهجمات الإلكترونية، مما يهدد سمعة المؤسسة ويؤثر بشكل كبير على استمرارية الأعمال.

تهدف هذه الدورة إلى تقديم مقدمة متكاملة وعملية حول المعيار الدولي ISO/IEC 27001:2022، الذي يُعد الإطار الأكثر اعتمادًا عالميًا لتطبيق نظام إدارة أمن المعلومات ISMS. ويزود هذا المعيار المؤسسات بالأدوات والمنهجيات اللازمة لتقييم المخاطر، وتطبيق الضوابط الأمنية المناسبة، والعمل على التحسين المستمر لنظام ISMS.

طوال فترة التدريب، سيتعرف المشاركون على مبادئ حوكمة أمن المعلومات، وهيكل المعيار وبنوده، وآليات تصميم وتنفيذ ومراقبة نظام إدارة فعال. كما تركز الدورة على الجوانب العملية مثل التوثيق، والتدقيق الداخلي، والاستعداد لعمليات الحصول على الشهادات. والهدف النهائي هو دعم المؤسسات في تحقيق الامتثال، وحماية أصول المعلومات، وبناء ثقة مستدامة مع العملاء وأصحاب المصلحة.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- فهم الغرض من معيار ISO/IEC 27001:2022 وفوائده المؤسسية.
- التعرف على الهيكل العام ومتطلبات المعيار الأساسية.
- إدراك مبادئ إدارة أمن المعلومات ضمن سياق تنظيمي متكامل.
- تطبيق عمليات تقييم ومعالجة المخاطر بشكل عملي.
- الإلمام بمتطلبات التوثيق، وعمليات التدقيق الداخلي، وإجراءات الحصول على الشهادة.



محاور الدورة

اليوم الأول: مقدمة في أمن المعلومات ومعيار ISO/IEC 27001:2022

- استعراض شامل لمفاهيم أمن المعلومات ومشهد التهديدات السيبرانية.
- أهمية وفوائد تطبيق معيار ISO/IEC 27001 في دعم استمرارية الأعمال.
- تطور المعيار من إصدار 2013 إلى 2022.
- الهيكل العام وبنود المعيار وفق تنسيق Annex SL.
- المصطلحات الأساسية والتعريفات في مجال أمن المعلومات.

اليوم الثاني: مفاهيم ISMS وسياق المنظمة

- الفهم العميق لنظام إدارة أمن المعلومات ISMS.
- البند 4: سياق المؤسسة وتحليل البيئة الداخلية والخارجية.
- البند 5: القيادة والالتزام بدعم وتفعيل ISMS.
- البند 6: التخطيط واستخدام منهجية التفكير المبني على المخاطر.
- تحليل الأطراف المعنية وتحديد نطاق النظام.

اليوم الثالث: إدارة المخاطر والتخطيط التشغيلي

- البند 6.1: آليات تقييم المخاطر ومعالجتها.
- تحديد معايير القبول للمخاطر وتقييم تأثيرها.
- البند 7: عناصر الدعم الموارد، الكفاءات، التوعية، الاتصال.
- البند 8: الرقابة التشغيلية وإدارة العمليات الخارجية.
- نظرة عامة على بيان قابلية التطبيق SoA.

اليوم الرابع: تقييم الأداء والتحسين

- البند 9: تقييم الأداء باستخدام أدوات المراقبة والقياس والتحليل.
- خطوات تنفيذ المراجعة الداخلية والتخطيط لها.
- مراجعة الإدارة: الأهداف، المدخلات، والمخرجات.
- البند 10: التعامل مع عدم المطابقة والإجراءات التصحيحية.
- التركيز على التحسين المستمر لنظام ISMS.



اليوم الخامس: ضوابط الملحق A والاستعداد للشهادة

- نظرة شاملة على 93 ضابطًا ضمن الملحق A، موزعة على 4 محاور رئيسية.
- فهم أهداف الضوابط وكيفية اختيارها وتطبيقها.
- تطوير السياسات الأمنية ومتطلبات التوثيق المؤسسي.
- مراحل الحصول على الشهادة، والجهات المعتمدة، وتقييم الجاهزية.
- مراجعة شاملة للمحتوى، جلسة أسئلة وأجوبة، وتقييم نهائي إن وجد.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- تعزيز المهارات العملية في إدارة المخاطر وتطبيق ضوابط أمنية فعّالة.
- تأهيل المشاركين لدعم منظماتهم خلال عمليات التدقيق الخارجي والحصول على الشهادة.
- بناء ثقافة مؤسسية قائمة على الامتثال والحوكمة الأمنية المستدامة.
- تطبيق مباشر لما تم تعلمه في بيئة العمل الواقعية.

الخاتمة

مع نهاية هذه الرحلة التدريبية، سيكون لدى المشاركين فهم شامل ومتوازن لمعيار ISO/IEC 27001:2022، مدعومًا بتطبيقات عملية تسهم في تعزيز أمن المعلومات المؤسسي.

سيتمكن المشاركون من تحليل السياق التنظيمي، تحديد المخاطر المحتملة، وصياغة سياسات أمنية تتماشى مع متطلبات المعيار. كما سيصبحون مؤهلين لمرافقة مؤسساتهم في إجراءات الحصول على الشهادة الدولية، مما يعزز من مكانة المؤسسة في بيئة العمل التنافسية.

من خلال هذه الدورة، سيكون للمشاركين دور فعال في تعزيز المرونة المؤسسية أمام التهديدات الرقمية، وترسيخ التميز في حوكمة أمن المعلومات، وخلق بيئة قائمة على الامتثال والتحسين المستمر في عالم سريع التغير تقنيًا.

