معايير أنظمة الإدارة

المتطلبات – ISO/IEC 27001:2022

والتحضير للحصول على شهادة نظام تدبير أمن المعلومات. النطاق وتقدير ISO/IEC 27001:2022 يومان لفهم ما يتطلبه والحوادث واستمرارية النشاط: يُطبَّق كل مفهوم A المخاطر ومعالجتها وبيان قابلية التطبيق و93 تدبيراً من الملحق .على أصولكم ومزوديكم ومساطركم. وتنصرفون بأول بيان لقابلية التطبيق وبقائمة أوجه القصور ذات الأولوية

المدة : 2 أيام

الأهداف

1. في المقاربة A وموقع الملحق ISO/IEC 27001:2022 شرح بنية
2. تحديد نطاق النظام انطلاقاً من السياق والأطراف المعنية والواجهات مع المزودين
3. تطبيق منهجية لتقدير مخاطر أمن المعلومات ومعالجتها
4. A بناء بيان لقابلية التطبيق معلّل انطلاقاً من 93 تدبيراً في الملحق
5. التحضير لتدبير الحوادث واستمرارية النشاط والتدقيق الداخلي ومراجعة الإدارة

البرنامج

اليوم 1 – صباحًا

ISO/IEC 27001 السرية والسلامة والتوافر: ما تثبته شهادة
• لزبنائكم
• أدوار 27001 و27002 و27005 :ISO/IEC 27000 عائلة
السياق والأطراف المعنية والمتطلبات القانونية والتعاقدية،
• ومنها القانون رقم 09-08 للمعطيات الشخصية
مجال التطبيق: المواقع والأنشطة ونظم المعلومات
• والمزودون

اليوم 1 – مساءً

• القيادة وسياسة أمن المعلومات والأدوار والمسؤوليات
• تقدير المخاطر: المعايير والتحديد والتحليل والتقييم
خيارات المعالجة وخطة المعالجة وقبول المخاطر المتبقية من
• طرف مالكيها
• تمرين: تقدير مخاطر عملية من عمليات مقاولتكم

اليوم 2 – صباحًا

تدبيراً موزعة على أربعة محاور: تنظيمي وبشري A: 93 الملحق
• ومادي وتقني
بيان قابلية التطبيق: التدابير المعتمدة والاستثناءات المعلّلة
• وحالة التنفيذ
تدابير تُفحص كثيراً في التدقيق: حقوق الولوج والنسخ
الاحتياطية والمزودون وخدمات الحوسبة السحابية وتتبع
• الأحداث
• تدبير حوادث الأمن وأمن المعلومات أثناء الاضطرابات

اليوم 2 – مساءً (ورشة)

• المراقبة والقياس والتدقيق الداخلي ومراجعة إدارة النظام
• حالات عدم المطابقة والإجراءات التصحيحية
ورشة: مسودة بيان قابلية التطبيق لديكم وقائمة أوجه القصور
• ذات الأولوية
• اختبار المكتسبات والعرض

المقاربة البيداغوجية

• A قراءة مشروحة للمتطلبات والملحق
• تمارين على أصولكم وتدفقات معطياتكم وعقود مزودي خدمات المعلوميات
• بناء موجَّه لبيان قابلية التطبيق
• دراسة حالة لحادثة أمنية، من الكشف إلى الإجراء التصحيحي
• اختبار في منتصف الدورة واختبار نهائي حول متطلبات النظام

التقييم والوثائق

شهادة تكوين مرقّمة وقابلة للتحقق. اختبار في منتصف الدورة (J+1) واختبار للمكتسبات في نهايتها، وتقييم فوري في اليوم الموالي عبر الإنترنت لكل مشارك، وتتوصل المقاولة بتقرير عن التكوين وبمسودة بيان قابلية التطبيق وقائمة أوجه القصور.

دعامات ثنائية اللغة لكل مشارك؛ وكل تكوين حضوري مرفق بنسخته الرقمية على منصة OmniLearn.

معلومة مفيدة

تكوين «مخاطر نظم المعلومات» (يومان). أما «ISO/IEC 27005:2022 – لتعميق منهجية تقدير المخاطر، يكمّل هذا التكوين «ISO/IEC 27701:2025 حماية المعطيات الشخصية والقانون 09-08» فنُعالج في القانون 09-08 والقانون.

معلومات عملية

المدة	أيام 2
عدد المشاركين	مجموعات من 6 إلى 12 مشاركًا داخل المقاولة
الصيغة	داخل المقاولة، حضوريًا في موقعكم
اللغة	الفرنسية أو الدارجة أو الإنجليزية؛ دعامات ثنائية اللغة
التمويل	العقود الخاصة للتكوين لدى مكتب التكوين المهني والمغرب GIAC، ومجموعات الاستشارة (TFP). المقاولات: تُعدّ الملفات معكم دون أي تكلفة إضافية.
تكييف البرنامج	برنامج مكيَّف مع مساطركم وتجهيزاتكم والفئة المستهدفة

أسئلة شائعة

هل يلزم أن يكون المرء مهندساً معلوماتياً لمتابعة التكوين؟

لا. فمتطلبات المعيار تخص التنظيم أولاً: النطاق والمخاطر والأدوار والمزودون والحوادث. وتُشرح التدابير التقنية دون مصطلحات معقدة، وحضور مدير نظم المعلومات أو مسؤول أمن النظم يساعد على ربطها ببنيتكم التحتية.

هل يجب أن يعتمد بيان قابلية التطبيق التدابير الـ 93 كلها؟

هل هو معتمد أم مستبعد، ولماذا. وتنتج هذه الاختيارات عن تقدير المخاطر، A لا. فهو يبين، بالنسبة لكل تدبير من الملحق ومعالجتها، ويتحقق مدقق الشهادة من اتساقها.

ما الصلة بالقانون 09-08؟

تحديد المتطلبات القانونية ISO/IEC 27001:2022 ينظم القانون رقم 09-08 معالجة المعطيات ذات الطابع الشخصي. ويطلب المطبقة ومراعاتها: فالقانون يدخل في السياق وفي معالجة المخاطر، دون أن تعادل الشهادة المطابقة القانونية.

الاستناد إلى نظامه؟ ISO 9001 هل يمكن لموقع حاصل أصلاً على شهادة

نعم. يتقاسم المعياران البنية الموحدة: التحكم في الوثائق والتدقيق الداخلي ومراجعة الإدارة والإجراءات التصحيحية يمكن أن تكون مشتركة. أما العمل الخاص بـ ISO/IEC 27001 فيتعلق بمخاطر أمن المعلومات وتدابير الملحق A.