معايير أنظمة الإدارة

مخاطر نظم المعلومات – ISO/IEC 27005:2022

ISO/IEC باتباع توصيات ،ISO/IEC 27001:2022 يومان لإجراء تقدير مخاطر أمن المعلومات ومعالجتها كما يتطلبهما المقاربة بالأحداث أو بالأصول والسيناريوهات والمعايير وخطة المعالجة وقبول المخاطر المتبقية: .27005:2022 .تُطبَّق المنهجية على نظم معلوماتكم ومزوديكم، وصولاً إلى سجل مخاطر قابل للاستغلال

المدة : 2 أيام

الأهداف

1. ISO/IEC 27001:2022 بالنسبة لمتطلبات ISO/IEC 27005:2022 شرح دور
2. تحديد السياق ومعايير قبول المخاطر ومعايير تقديرها
3. تحديد سيناريوهات الخطر وفق مقاربة بالأحداث أو بالأصول
4. A تحليل المخاطر وتقييمها، ثم بناء خطة معالجة مرتبطة بتدابير الملحق
5. تنظيم مراقبة المخاطر ومراجعتها والتواصل بشأنها على المدى الطويل

البرنامج

اليوم 1 – صباحًا

بخصوص تقدير ISO/IEC 27001:2022 لماذا منهجية: ما يتطلبه
- المخاطر ومعالجتها

المفردات: مصدر الخطر والتهديد والثغرة والحدث والعاقبة
- والاحتمال
- السياق ومعايير قبول المخاطر ومعايير التقدير
- مالكو المخاطر ودور الإدارة

اليوم 1 – مساءً

المقاربة بالأحداث والمقاربة بالأصول: متى نختار الواحدة أو
- الأخرى
- الأصول والتهديدات والثغرات؛ وبناء سيناريوهات الخطر
- التحليل: العواقب والاحتمال ومستوى الخطر

البريد) تمرين: سيناريوهات خطر على نطاق من مقاولتكم
- (ومعطيات الزبناء ERPالإلكتروني و

اليوم 2 – صباحًا

- تقييم المخاطر وترتيبها
- خيارات المعالجة: التقليص والتفادي والتقاسم والاحتفاظ
- وبيان قابلية التطبيق A خطة معالجة مرتبطة بتدابير الملحق
- قبول المخاطر المتبقية وإخبار الإدارة

اليوم 2 – مساءً (ورشة)

- مراقبة المخاطر ومراجعتها: المؤشرات ومحفزات التحيين
- التواصل والتشاور حول المخاطر
- ورشة: سجل المخاطر وخطة المعالجة لنطاقكم
- اختبار المكتسبات وعرض السجل

المقاربة البيداغوجية

- تمارين على نظم معلوماتكم وتدفقات معطياتكم وعقود المناولة المعلوماتية
- مقارنة المقاربتين على نطاق واحد
- نموذج لسجل المخاطر ولخطة المعالجة، قابل للملاءمة مع أداتكم
- دراسة حالة: خطر مرتبط بمزود خدمات الحوسبة السحابية
- اختبار في منتصف الدورة واختبار نهائي حول المنهجية

التقييم والوثائق

شهادة تكوين مرقّمة وقابلة للتحقق .(J+1) اختبار في منتصف الدورة واختبار للمكتسبات في نهايتها، وتقييم فوري في اليوم الموالي .عبر الإنترنت لكل مشارك، وتتوصل المقاولة بتقرير عن التكوين وبسجل المخاطر وخطة المعالجة الناتجين عن الورشة

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

معلومة مفيدة

المتطلبات» (يومان). – ISO/IEC 27001:2022» ويقدمها تكوين ،ISO/IEC 27001:2022 يفترض هذا التكوين معرفة متطلبات .«تدبير المخاطر – ISO 31000:2018» وتُعالج المنهجية العامة لتدبير المخاطر في

معلومات عملية

المدة	أيام 2
الفئة المستهدفة	مسؤولو أمن النظم ومديرو نظم المعلومات ومدبرو المخاطر ومسؤولو المطابقة والمدققون الداخليون لنظام أمن المعلومات
المتطلبات المسبقة	ISO/IEC 27001:2022 معرفة أساسية بـ
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	والمغرب ،GIAC ومجموعات الاستشارة ،(TFP) العقود الخاصة للتكوين لدى مكتب التكوين المهني .المقاولات: تُعدّ الملفات معكم دون أي تكلفة إضافية
تكييف البرنامج	برنامج مكيَّف مع مساطركم وتجهيزاتكم والفئة المستهدفة

أسئلة شائعة

ISO/IEC 27005؟ هل يمكن الحصول على شهادة

المتعلقة بالمخاطر، وهذه ISO/IEC 27001:2022 توصيات. وهو يساعد على استيفاء متطلبات ISO/IEC 27005:2022 لا. يقدم .المتطلبات هي التي تُدقَّق عند المصادقة

هل يلزم برنامج لتدبير المخاطر؟

.لا. يكفي جدول بيانات جيد البنية للانطلاق. ويقدم التكوين نموذجاً؛ ثم يأتي اختيار أداة، بحسب حجم النطاق وعدد مالكي المخاطر

ISO 31000:2018؟ ما الفرق بينه وبين

فيطبقها على أمن المعلومات: الأصول ISO/IEC 27005:2022 خطوطاً توجيهية عامة لتدبير المخاطر. أما ISO 31000:2018 يقدم .ISO/IEC 27001:2022 من A والتهديدات والثغرات والسيناريوهات والصلة بتدابير الملحق

من ينبغي أن يشارك؟

مسؤول أمن النظم ومدير نظم المعلومات ومدبرو المخاطر ومالكو العمليات المهنية. ويجب أن يفهم مالكو المخاطر المنهجية .ليقبلوا المخاطر المتبقية عن دراية