



تطبيق ضوابط الملحق A في ISO 27001 وبيان قابلية التطبيق والتدقيق الداخلي عليها

13 - 17 Sep 2027

لندن - فندق أربع نجوم في وسط لندن



تطبيق ضوابط الملحق A في ISO 27001 وبيان قابلية التطبيق والتدقيق الداخلي عليها

المرجع: 1256_7516 التاريخ: 13 - 17 Sep 2027 الموقع: لندن - فندق أربع نجوم في وسط لندن الرسوم: SAR 23000

العوق التقني: مهارس - أسلوب التطبيق: دراسة حالة

مقدمة

تحول مؤسسات كثيرة شهادة IEC/ISO 27001 أو تخطط للحصول عليها، لكن ضوابطها موجودة غالباً على الورق فقط. فبيان قابلية التطبيق منسوخ من نموذج جاهز، وهناك الضوابط لا يملكون أدلة، والتدقيق الداخلي يختبر الوثائق لا فاعلية الضوابط. تأخذ هذه الدورة من كور كونسبت المشاركون عبر ضوابط الملحق A في إصدار 2022، من اختيار الضوابط وتطبيقها إلى تخطيط التدقيق واختبار الأدلة وصياغة الملاحظات. وتستند الحالات إلى قطاعات متعددة، ويخرج المشاركون بحزمة تطبيق الضوابط والتدقيق عليها لمؤسساتهم.

أهداف الدورة

- تحديد نطاق نظام إدارة أمن المعلومات ورصد فجوات الضوابط مقابل الملحق A في IEC/ISO 27001:2022
- تطبيق إرشادات IEC/ISO 27002:2022 ومعالجة المخاطر وفق IEC/ISO 27005:2022 لاختيار الضوابط وتبويبها
- تطبيق الضوابط التنظيمية والبشرية والمادية والتقنية مع تحديد الهلاك والأدلة
- تخطيط تدقيق داخلي قائم على المخاطر للضوابط وتنفيذه وفق ISO 19011:2018 و IEC/ISO 27007:2020
- تصنيف حالات عدم المطابقة وصياغة ملاحظات التدقيق والتحقق من الإجراءات التصحيحية
- إعداد حزمة تطبيق الضوابط والتدقيق عليها جاهزة لمراجعة الإدارة

الفئة المستهدفة

- منفذو ومنسقو نظام إدارة أمن المعلومات المسؤولون عن تطبيق الضوابط
- ملاك الضوابط في تقنية المعلومات والمرافق والموارد البشرية والمشتريات المطالبون بتقديم الأدلة
- المدققون الداخليون وأخصائيو التأكيد الذين يختبرون ضوابط أمن المعلومات
- مسؤولو الامتثال القانونيون على سجلات الضوابط والجاهزية للتدقيق
- محللو أمن تقنية المعلومات الداعمون لتدقيق منح الشهادة والتدقيق الرقابي

محاور الدورة

اليوم الأول: نظام إدارة أمن المعلومات وضوابط إصدار 2022

- نظرة عامة على متطلبات IEC/ISO 27001:2022 والتعديل الأول لعام 2024
- بيان نطاق النظام وتحليل الأطراف المعنية
- هيكل الملحق A: 93 ضابطاً في أربعة محاور
- تقييم فجوات الضوابط مقابل الملحق A
- المقابلة بين ضوابط إصدار 2013 وضوابط إصدار 2022

اليوم الثاني: معايير التطبيق والتدقيق

- خصائص الضوابط وإرشادات تطبيقها في IEC/ISO 27002:2022
- إرشادات تطبيق نظام إدارة أمن المعلومات في IEC/ISO 27003:2017
- ربط خطة معالجة المخاطر بمتطلبات IEC/ISO 27005:2022
- مبادئ التدقيق وإدارة برنامج التدقيق وفق ISO 19011:2018 إرشادات تدقيق أنظمة الإدارة
- تدقيق أنظمة أمن المعلومات وفق IEC/ISO 27007:2020 وتقييم الضوابط وفق IEC/ISO TS 27008:2019

اليوم الثالث: تطبيق الضوابط

- صياغة بيان قابلية التطبيق مع مبررات الإدراج والاستبعاد
- الضوابط التشغيلية: السياسات الموضوعية وسجل الوصول واتفاقيات الموردين
- الضوابط البشرية: التحقق من الخلفية والتوعية والعزل عن بعد
- الضوابط المادية: المناطق الآمنة وحماية المعدات وسياسة المكتب النظيف
- الضوابط التقنية: حقوق الوصول والسجلات والإعدادات والنسخ الاحتياطي

اليوم الرابع: التدقيق على الضوابط

- خطة التدقيق الداخلي وتصميم قائمة تدقيق قائمة على المخاطر
- أساليب جمع أدلة التدقيق: المقابلة والملاحظة وأخذ العينات وإعادة الأداء
- اختبار الضوابط المستحدثة في 2022: معلومات التهديدات والخدمات السحابية وإخفاء البيانات وتصفية الويب
- تصنيف حالات عدم المطابقة وصياغة عبارات الملاحظات
- التحقق من الإجراءات التصحيحية وتحليل السبب الجذري بأسلوب النسل الخمسة 5 Whys

اليوم الخامس: دراسات الحالة وحزمة تطبيق الضوابط والتدقيق عليها

- دراسة حالة مزود خدمات برمجية سحابية: مراجعة ملف الندلة
- دراسة حالة مستشفى: تدقيق ضوابط الوصول والسجلات
- بيان قابلية التطبيق وخطة تطبيق الضوابط لهيئة المشارك
- بناء برنامج التدقيق الداخلي ونصوص اختبار الضوابط
- عرض ملاحظات التدقيق ومناقشتها مع الزملاء

المهارات المكتسبة

- تحديد نطاق نظام إدارة أمن المعلومات
- اختيار الضوابط وتبريرها
- تخطيط تطبيق الضوابط
- تقييم أدلة التدقيق
- اختبار الضوابط
- صياغة ملاحظات التدقيق
- متابعة الإجراءات التصحيحية

لهذا تحضر هذه الدورة

- تعود بحزمة تطبيق الضوابط والتدقيق عليها تعكس نطاق مؤسستك ومخاطرها وضوابطها الفعلية
- تستبدل عبارات الضوابط المنسوخة من النماذج بأدلة تصمد أمام التدقيق الخارجي
- تتعرف على مجالات الضوابط التي تكثر فيها الملاحظات في تدقيق منح الشهادة والتدقيق الرقابي
- تتبادل خبرات التدقيق العملية مع زملاء من قطاعات ودول مختلفة

الخاتمة

لا يكون نظام إدارة أمن المعلومات أقوى من الضوابط التي تعمل يوميا ومن التدقيق الذي يختبرها بموضوعية. تنتقل هذه الدورة من ضوابط إصدار 2022 والمعايير التي توجه تطبيقها والتدقيق عليها، مروراً بتطبيق الضوابط التنظيمية والبشرية والمادية والتقنية، وصولاً إلى تخطيط التدقيق واختبار الأدلة وتصنيف الملاحظات. ويخرج اليوم الأخير بحزمة تطبيق الضوابط والتدقيق عليها يعود بها المشاركون إلى مؤسساتهم، جاهزة لدعم مراجعة الإدارة ودورة التدقيق التالية.