



دورة نظام إدارة أمن المعلومات وفق ISO/IEC 27001 من التطبيق إلى الجاهزية للشهادة



دورة نظام إدارة أمن المعلومات وفق ISO/IEC 27001 من التطبيق إلى الجاهزية للشهادة

مقدمة:

دورة نظام إدارة أمن المعلومات وفق ISO/IEC 27001 من التطبيق إلى الجاهزية للشهادة تمتد أسبوع لكوادر أمن المعلومات وتنسيق نظام الإدارة وتقنية المعلومات والمخاطر، وتنتهي بإعداد خطة تطبيق نظام إدارة أمن المعلومات ومجموعة المعلومات الموثقة الإلزامية. فكثر من المؤسسات تشتري نماذج جاهزة وتستعجل بيان قابلية التطبيق، ثم تصل إلى تدقيق الشهادة بنظام قائم على الورق بلا نطاق فعلي أو منهجية مخاطر أو برنامج تدقيق داخلي أو مراجعة إدارية. ويتولى المشاركون أصلاً تنسيق أعمال الأمن أو التقنية أو المخاطر، ويتدربون عبر دراسات حالة على نطاقات وسجلات من قطاعات متعددة. وتقدم كور كونسبت هذه الدورة في تطبيق النظام.

أهداف الدورة:

- تحديد سياق المؤسسة ومتطلبات الأطراف المعنية ونطاق النظام وفق البنود 4.1 إلى 4.3، بما فيها اعتبار تغير المناخ الذي أضافه التعديل 1:2024 Amendment
- صياغة سياسة أمن المعلومات وتوزيع أدوار القيادة ووضع أهداف أمن المعلومات وخطط تحقيقها
- تحديد منهجية تقييم المخاطر ومعالجتها ثم إعداد خطة معالجة المخاطر وبيان قابلية تطبيق مسبب
- إرساء ترتيبات الكفاءة والتوعية والتواصل وضبط المعلومات الموثقة بما ينتج سجلات قابلة للتدقيق
- إعداد الرصد والقياس وبرنامج التدقيق الداخلي والمراجعة الإدارية وآلية الإجراءات التصحيحية
- بناء خطة تطبيق النظام ومجموعة المعلومات الموثقة الإلزامية بما يثبت الجاهزية للشهادة

الفئة المستهدفة:

- مديرو أمن المعلومات المسؤولون عن إنشاء نظام الإدارة وتشغيله
- منسقو نظام إدارة أمن المعلومات المسؤولون عن المعلومات الموثقة والسجلات والجاهزية للتدقيق
- مديرو تقنية المعلومات المسؤولون عن الأنظمة والخدمات الواقعة ضمن نطاق النظام
- مديرو المخاطر المسؤولون عن منهجية مخاطر أمن المعلومات وملك المخاطر
- أعضاء فرق التطبيق المسؤولون عن مهام المشروع وجمع الأدلة

محاوّر الدورة:

اليوم 1: أسس النظام والسياق وتحليل الفجوات

- الإصدار الحالي من ISO/IEC 27001 والتعديل الأول والهيكل الموحد
- البند 4.1 القضايا الداخلية والخارجية وتغير المناخ
- البند 4.2 بناء سجل متطلبات الأطراف المعنية
- البند 4.3 حدود نطاق النظام وواجهاته وتبعياته
- تحليل الفجوات للبند 4 إلى 10 مقارنة بالممارسة الحالية

اليوم 2: القيادة والتخطيط ومنهجية المخاطر

- البند 5 تحديد أدوار القيادة ومسؤولياتها وصلاحياتها
- البند 5.2 صياغة سياسة أمن المعلومات واعتمادها
- البند 6.1.2 منهجية تقييم المخاطر ومعايير قبولها
- البند 6.1.3 خيارات معالجة المخاطر وهيكل خطة المعالجة
- البند 6.2 أهداف أمن المعلومات وخطط تحقيقها

اليوم 3: الدعم والتشغيل والمعلومات الموثقة

- مقارنة الملحق أ لاتخاذ قرار ببيان قابلية التطبيق
- البند 7 سجلات الكفاءة وخطط التوعية ومصفوفة التواصل
- البند 7 ضبط المعلومات الموثقة وإدارة الإصدارات
- البند 8 التخطيط التشغيلي وترتيبات ضبط التغيير
- البنود 8.2 و8.3 سجلات نتائج تقييم المخاطر ومعالجتها

اليوم 4: تقييم الأداء والتحسين ومخاطر الجاهزية

- البند 9 اختيار طرق الرصد والقياس والمؤشرات
- البند 9 إعداد برنامج التدقيق الداخلي وتكليف المدققين
- البند 9 مدخلات المراجعة الإدارية ومخرجاتها ومحاضرها
- البند 10 سجل عدم المطابقة والإجراء التصحيحي والتحسين المستمر
- مراجعة الجاهزية للشهادة وفجوات التوثيق والأدلة الشائعة

اليوم 5: دراسات الحالة وإعداد خطة تطبيق النظام

- دراسة حالة لتحليل النطاق والسياق لدى مزود خدمات لوجستية
- دراسة حالة لعرض منهجية المخاطر وبيان قابلية التطبيق والدفاع عنهما
- خطة مشروع تطبيق النظام مع المراحل والمسؤولين
- تجميع مجموعة المعلومات الموثقة الإلزامية ومراجعتها بين الزملاء
- استكمال خطة تطبيق النظام ومجموعة المعلومات الموثقة

المهارات التي ستكتسبها:

- تحديد نطاق النظام
- تحليل الأطراف المعنية
- تصميم منهجية المخاطر
- تسبيب بيان قابلية التطبيق
- ضبط المعلومات الموثقة
- تخطيط برنامج التدقيق الداخلي
- إدارة المراجعة الإدارية
- تخطيط مشروع التطبيق

لماذا تحضر هذه الدورة:

- تسليم خطة تطبيق النظام ومجموعة المعلومات الموثقة الإلزامية إلى لجنة توجيه أمن المعلومات والإدارة العليا
- الحسم في ضوابط الملحق أ التي تدرج أو تستبعد وتوثيق مبررات ذلك في بيان قابلية التطبيق
- تجنب تأخر تدقيق الشهادة بسبب غياب النطاق أو منهجية المخاطر أو برنامج التدقيق أو سجل المراجعة الإدارية
- إطلاع ملاك المخاطر وملاك العمليات وزملاء فريق التطبيق على السجلات التي يتطلبها كل بند

الخاتمة:

بعد العودة إلى العمل يعرض المشاركون خطة تطبيق النظام ومجموعة المعلومات الموثقة الإلزامية على الإدارة العليا ولجنة توجيه أمن المعلومات، وتعتمد عليهما المؤسسة في إقرار نطاق النظام والسياسة ومنهجية المخاطر، وتعيين المسؤولين والمراحل، وتحديد موعد جاهزية النظام للتقدم إلى جهة منح الشهادة. وبعد أول تدقيق داخلي وأول مراجعة إدارية وفق الخطة يراجع الفريق حالات عدم المطابقة المفتوحة والسجلات الناقصة والمراحل المتأخرة، ثم يحدث الخطة ومجموعة الوثائق.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة نظام إدارة أمن المعلومات وفق ISO/IEC 27001؟

لا تشترط الدورة تدريباً سابقاً على ISO/IEC 27001. ويحتاج المشارك إلى خبرة عملية في تنسيق أعمال أمن المعلومات أو التقنية أو المخاطر، ويفيده إحصار السياسات الحالية أو سجل المخاطر أو ملاحظات النطاق لتطبيق دراسات الحالة على نظام مؤسسته.

بم تختلف دورة نظام إدارة أمن المعلومات وفق ISO/IEC 27001 عن دورات ضوابط الأمن؟

تبنى هذه الدورة نظام الإدارة ذاته عبر البنود 4 إلى 10 من السياق والنطاق والقيادة ومنهجية المخاطر إلى الدعم والتشغيل والتقييم والتحسين. أما دورات الضوابط فتركز على تطبيق ضوابط الملحق أ واختبارها، ولا تتناولها هذه الدورة إلا لقرار بيان قابلية التطبيق.

ما المعلومات الموثقة التي يتطلبها نظام إدارة أمن المعلومات وفق ISO/IEC 27001؟

يتطلب المعيار معلومات موثقة تشمل نطاق النظام وسياسة أمن المعلومات وعملية تقييم المخاطر ومعالجتها وبيان قابلية التطبيق وخطة معالجة المخاطر والأهداف ونتائج المخاطر، إضافة إلى أدلة الكفاءة والرصد والتدقيق الداخلي والمراجعة الإدارية والإجراءات التصحيحية.

ماذا يعود به المشارك من دورة نظام إدارة أمن المعلومات وفق ISO/IEC 27001؟

يعود المشارك بخطة تطبيق للنظام تحدد المراحل والمسؤولين، وبمجموعة المعلومات الموثقة الإلزامية لنطاق مؤسسته، تضم السياسة ومنهجية المخاطر وبيان قابلية التطبيق والأهداف وسجلات التدقيق والمراجعة التي يجب أن ينتجها النظام.