CONCEPT

إدارة مخاطر أمن المعلومات وفق ISO 27005:
التقييم والمعالجة وقبول المخاطر

إدارة مخاطر أمن المعلومات وفق ISO 27005: التقييم والمعالجة وقبول المخاطر

مقدمة:

تجري منشآت كثيرة تقييما لمخاطر أمن المعلومات مرة كل عام، لكن نتائجه نادرا ما توجه القرارات: فمعايير المخاطر غامضة، ودرجات الاحتمالية تقديرية، والسجل يسرد الأصول بدلا من السيناريوهات، وخيارات المعالجة لا يمكن تتبعها إلى الضوابط. تتناول هذه الدورة من كور كونسبت إدارة مخاطر أمن المعلومات وفق ISO 27005 بعمق، بدءا من السياق ومعايير المخاطر، مرورا بتحليل السيناريوهات وتقييمها، وصولا إلى المعالجة والقبول والمراجعة. ويقارن المشاركون نهج ISO/IEC 27005 بمناهج منشورة أخرى، وينفذون تقييما كاملا على حالة عملية، ليخرجوا بتقرير تقييم مخاطر أمن المعلومات وخطة معالجة المخاطر.

أهداف الدورة:

- تحديد السياق والنطاق ومعايير المخاطر لتقييم مخاطر أمن المعلومات بما يتوافق مع ISO/IEC 27005:2022
- الاختيار بين النهج المبني على الأحداث والنهج المبني على الأصول في تحديد المخاطر وتبرير الاختيار لنطاق محدد
- تحليل التهديدات والثغرات والعواقب باستخدام مقاييس معايرة للاحتمالية والعواقب
- تقييم المخاطر وترتيب أولوياتها في سجل يوثق مالكي المخاطر والسيناريوهات ومستويات الخطر
- اتخاذ قرارات معالجة المخاطر وربطها بالضوابط المرجعية في الملحق A من ISO/IEC 27001 وتوثيق المخاطر المتبقية للقبول
- عرض نتائج التقييم على الإدارة وتحديد محفزات المراقبة والمراجعة التي تستدعي إعادة التقييم

الفئة المستهدفة:

- المديرون الذين يقودون تقييمات مخاطر أمن المعلومات عبر وحدات الأعمال
- مديرو نظام إدارة أمن المعلومات المسؤولون عن عملية تقييم المخاطر ومعالجتها
- محللو المخاطر الذين يبنون سجلات مخاطر أمن المعلومات ويحدثونها
- مصممو البنية الأمنية الذين يحولون سيناريوهات المخاطر إلى قرارات بشأن الضوابط
- مالكو المخاطر في تقنية المعلومات والأعمال الذين يعتمدون خطط المعالجة ويقبلون المخاطر المتبقية

محاور الدورة:

اليوم 1: سياق إدارة المخاطر ومعاييرها

- بنية ISO/IEC 27005:2022 وعلاقته بمعيار إدارة المخاطر ISO 31000 ومعيار نظام إدارة أمن المعلومات ISO/IEC 27001
- تحليل السياق الداخلي والخارجي لنطاق تقييم المخاطر
- معايير قبول المخاطر ومعايير إجراء التقييمات
- تحديد مالكي المخاطر ومصفوفة المساءلة
- مراجعة نضج منهجية تقييم المخاطر المعمول بها حاليا

اليوم 2: مناهج تحديد المخاطر والأساليب البديلة

- التحديد المبني على الأحداث: مصادر المخاطر وأهدافها والسيناريوهات الاستراتيجية
- التحديد المبني على الأصول: الأصول الأولية والأصول الداعمة وترابطاتها
- مبادئ منهجية OCTAVE للتقييم الأمني القائم على المخاطر
- منهجية EBIOS Risk Manager: تحليل تكراري ينتقل من المهام الرئيسية إلى الوظائف التقنية
- عملية التقييم في دليل NIST SP 800-30 Rev. 1 والتسلسل الهرمي ذو المستويات الثلاثة

اليوم 3: تحليل التهديدات والثغرات والمخاطر

- فهرس التهديدات وتوصيف مصادر التهديد
- تحديد الثغرات من نتائج الفحص وملاحظات التدقيق وسجلات الحوادث
- مقاييس الاحتمالية والعواقب: النوعية وشبه الكمية والكمية
- ورقة تحليل المخاطر ومعايرة مصفوفة مستويات الخطر
- تقييم المخاطر وسجل مخاطر أمن المعلومات مرتبا حسب الأولوية

اليوم 4: المعالجة والمخاطر المتبقية والمراجعة

- اختيار خيار المعالجة: التجنب أو المشاركة أو التخفيف أو القبول
- تتبع خطة معالجة المخاطر إلى الضوابط المرجعية في الملحق A من ISO/IEC 27001
- تقدير المخاطر المتبقية وسجلات القبول الرسمي للمخاطر
- أخطاء التقييم الشائعة: انحياز التقدير والاحتساب المزدوج والسيناريوهات المجمعة
- محفزات المراقبة والمراجعة ومؤشرات المخاطر الرئيسية ودورات إعادة التقييم

اليوم 5: ورشة تقييم مخاطر كاملة على حالة عملية

- ورشة الحالة: السياق والنطاق ومعايير المخاطر لمزود خدمات دفع
- ورشة الحالة: بناء السيناريوهات وتقدير الاحتمالية والعواقب
- ورشة الحالة: التقييم وقرارات المعالجة والمخاطر المتبقية
- صياغة تقرير تقييم مخاطر أمن المعلومات وخطة معالجة المخاطر
- إحاطة الإدارة بالمخاطر ولجنة مساءلة قرارات قبول المخاطر

المهارات التي ستكتسبها:

- تصميم معايير المخاطر
- بناء سيناريوهات المخاطر
- تحليل التهديدات والثغرات
- معايرة الاحتمالية والعواقب
- إدارة سجل المخاطر
- تقييم خيارات المعالجة
- تبرير المخاطر المتبقية
- المقارنة بين مناهج تقييم المخاطر

لماذا تحضر هذه الدورة:

- العودة بتقرير تقييم مخاطر أمن المعلومات وخطة معالجة المخاطر مبنيين من تقييم كامل لحالة عملية
- استبدال الدرجات غير المتسقة بمقاييس ومعايير يطبقها المقيمون المختلفون بالطريقة نفسها
- الدفاع عن قرارات المعالجة والقبول أمام الإدارة بمسار واضح يربط السيناريو بالضابط
- مقارنة ممارسات التقييم مع مختصي مخاطر من القطاع المالي والرعاية الصحية والخدمات الحكومية والتقنية

الخاتمة:

لا يفيد تقييم مخاطر أمن المعلومات إلا إذا كانت معاييره متفقا عليها، وسيناريوهاته واقعية، ودرجاته متسقة، وقرارات المعالجة فيه قابلة للتتبع والمراجعة. تنتقل الدورة من السياق ومعايير المخاطر، إلى التحديد المبني على الأحداث والأصول والمناهج المنشورة البديلة، ثم تحليل التهديدات والثغرات والعواقب، وصولا إلى المعالجة والمخاطر المتبقية والمراجعة. ويطبق اليوم الأخير عملية ISO/IEC 27005 كاملة على حالة عملية، ليخرج المشاركون بتقرير تقييم مخاطر أمن المعلومات وخطة معالجة المخاطر جاهزين لمراجعة الإدارة.