

دورة تقييم مخاطر أمن المعلومات ومعالجتها وفق معييار ISO 27005

2027 11 – 7 يونيو

روما





دورة تقييم مخاطر أمن المعلومات ومعالجتها وفق معيار ISO 27005

المرجع: 22986_368 التاريخ: 7 - 11 يونيو 2027 المكان: روما الرسوم: GBP 5500

ملخص البرنامج

تقييم مخاطر أمن المعلومات ومعالجتها وفق معيار ISO 27005 محور دورة تدريبية تمتد 5 أيام لمديري أمن المعلومات ومسؤولي المخاطر ورؤساء أمن المعلومات بمستوى إداري، ويخرج منها كل مشارك بحزمة لتقييم المخاطر ومعالجتها في مؤسسة واحدة. فسجلات المخاطر كثيرا ما يتعذر ربطها بالأمول والسيناريوهات والقرارات. ويتدرج البرنامج من المعيار وسياق المخاطر، إلى تشخيص الأمول والتهديدات والضوابط القائمة، ثم إلى التحليل والتقييم وتصميم المعالجة، وصولا إلى التطبيق في مؤسسة بعينها. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في تقييم مخاطر أمن المعلومات ومعالجتها.

المبررات المؤسسية

حين تقييم مخاطر أمن المعلومات بمقاييس متفاوتة، يتبع الإنفاق على المعالجة العادة لا حجم التعرض الفعلي. أما القادة الذين يثبتون المنهجية والمعايير وإيقاع المراجعة فيستطيعون بيان سبب قبول كل خطر أو خفضه أو نقله أو تجنبه، وهو ما يحتاج إليه المسؤولون التنفيذيون والمدققون حين يسألون عن سبب التهاون في خطر ما، وحين تتنافس ميزانيات الأمن مع أولويات أخرى على تمويل محدود.

- الإنفاق على المعالجة: يتوافق مع حجم التعرض حين تقاس المخاطر بمقياس واحد.
- ملاحظات التدقيق: تقل حين يرتبط السجل بالخطة واختيار الضوابط ارتباطا يمكن تتبعه.
- سرعة القرار: تتحسن حين يعرف أصحاب المخاطر معايير القبول وحدود التصعيد مسبقا.

المبادئ والأساس المعرفي

- معيار ISO/IEC 27005 إرشادات إدارة مخاطر أمن المعلومات: يقدم مسار السياق والتحديد والتحليل والتقييم والمعالجة والمتابعة الذي تيسر عليه الجلسات من 1 إلى 4.
- معيار ISO/IEC 27001 متطلبات نظم إدارة أمن المعلومات: يؤثر تقييم المخاطر وخطة المعالجة واختيار الضوابط التي يعدها المشاركون في الجلسة 3.
- معيار ISO 31000 مبادئ إدارة المخاطر وعمليتها: يشكل معايير المخاطر وترتيبات الإبلاغ والمراجعة المبنية في الجلستين 1 و4.



المشاركون المستهدفون

- مدبرو الأمن الذين يملكون مسار مخاطر أمن المعلومات في مؤسساتهم.
- مسؤولو المخاطر الذين يجمعون مخاطر الأمن في تقارير المؤسسة.
- قادة الأمن الذين يقبلون قرارات المعالجة أو يمولونها أو يصعدونها.
- مسؤولو نظم الإدارة والمدققون الذين يعتمدون على سجلات المخاطر.

يخدم البرنامج المصارف وشركات الاتصالات والطاقة وفرق التقنية في القطاع العام.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم مسار مخاطر أمن المعلومات في المؤسسة في ضوء ISO/IEC 27005 و ISO/IEC 27001.
2. سيكون المشاركون قادرين على تشخيص الثغرات في تغطية الأصول والتهديدات ونقاط الضعف والضوابط.
3. سيكون المشاركون قادرين على بناء معايير المخاطر ومقاييسها وحدود القبول.
4. سيكون المشاركون قادرين على مقارنة خيارات المعالجة وتصميم خطة لمعالجة المخاطر.
5. سيكون المشاركون قادرين على ترتيب المخاطر المتبقية بحسب القبول أو التصعيد.
6. سيكون المشاركون قادرين على تبرير حزمة تقييم المخاطر ومعالجتها أمام لجنة توجيهية للأمن.

هيكل البرنامج

اليوم 1: مبادئ مخاطر أمن المعلومات ومعيار ISO/IEC 27005 وسياق المخاطر

ما الذي يطلبه المعيار من مسار مخاطر أمن المعلومات، وفي أي سياق يعمل؟

- نظرة عامة على مسار ISO/IEC 27005
- الصلات بين ISO/IEC 27001 و ISO 31000
- بيان النطاق والحدود
- مصفوفة ملكية المخاطر
- معايير المخاطر وسلم القبول

اليوم 2: تشخيص الأصول والتهديدات ونقاط الضعف والضوابط القائمة

أين تكمن قيمة المؤسسة، وما الذي يهددها اليوم؟



- جرد الأصول وورقة تقدير قيمتها
- فهرس التهديدات ونقاط الضعف
- مراجعة فعالية الضوابط القائمة
- تحديد المخاطر انطلاقاً من الأصول
- تحديد السيناريوهات انطلاقاً من الأحداث

اليوم 3: التحليل والتقييم وتصميم معالجة المخاطر

كيف تقاس المخاطر وترتب وتعالج، وما الضوابط التي تترتب على ذلك؟

- منهج تقدير الاحتمال والأثر
- تقييم المخاطر قياساً إلى المعايير
- مقارنة خيارات المعالجة
- قالب خطة معالجة المخاطر
- مسودة بيان قابلية التطبيق

اليوم 4: الإبلاغ عن مخاطر أمن المعلومات ومتابعتها ومراجعتها

كيف يرى صناع القرار المخاطر، وكيف يبقى السجل محدثاً؟

- هيكل سجل المخاطر
- سجل قبول المخاطر المتبقية
- مجموعة مؤشرات المخاطر الرئيسية
- خطة الإبلاغ عن المخاطر
- جدول إعادة التقييم

اليوم 5: تطبيق تقييم مخاطر أمن المعلومات ومعالجتها في مؤسسة واحدة

هل حزمة التقييم والمعالجة جاهزة ليعتمدها المجلس التوجيهي؟

- تطبيق معايير الجلسة 1 على المؤسسة المختارة
- اختبار سيناريوهات الجلسة 2 قياساً إلى الضوابط القائمة
- مراجعة خطة معالجة الجلسة 3 مع أصحاب المخاطر
- وضع مؤشرات المتابعة من مجموعة الجلسة 4
- إنجاز حزمة تقييم المخاطر ومعالجتها



المنهجية

يقوم البرنامج على تمارين منظمة تستند إلى حالات مجهولة المصدر من المصارف والاتصالات ومشغلي الطاقة. يعمل المشاركون في فرق صغيرة بأدوار مدير الأمن وصاحب الخطر والمدقق الداخلي، وينقلون مؤسسة واحدة من النطاق إلى خطة معالجة جرت مراجعتها.

- نشاط مقترح: تقدير مجموعة من السيناريوهات على المقياس المتفق عليه والدفاع عن كل تقدير.
- نشاط مقترح: المفاضلة بين الخفض والقبول والتجنب والنقل لثلاثة مخاطر.
- نشاط مقترح: تتبع بند واحد من السجل إلى ضوابطه في مسودة بيان قابلية التطبيق.

المخرج الختامي

يعد كل مشارك حزمة لتقييم المخاطر ومعالجتها في مؤسسة واحدة. وتضم بيان النطاق، ومعايير المخاطر، وقائمة السيناريوهات، وسجل مخاطر مقيما، وخطة معالجة بأسماء أصحابها، ومسودة بيان قابلية التطبيق، ومؤشرات المتابعة. وتستخدم الحزمة في إحاطة اللجنة التوجيهية وتجهيز المراجعة التالية.

الأسئلة الشائعة

هل يناسب تقييم مخاطر أمن المعلومات ومعالجتها المديرين الذين ليسوا متخصصين تقنيين؟

نعم، فتقييم مخاطر أمن المعلومات ومعالجتها بمستوى إداري، ويفترض أنك تملك مسار المخاطر أو تعتمد عليه لا أنك تضبط الأدوات التقنية بنفسك.

ما المعايير التي يقوم عليها تقييم مخاطر أمن المعلومات ومعالجتها في هذا التدريب؟

يقوم تقييم مخاطر أمن المعلومات ومعالجتها على معيار ISO/IEC 27005، مع ISO/IEC 27001 لنظام الإدارة وISO 31000 لمبادئ إدارة المخاطر.

كيف تستخدم حزمة تقييم مخاطر أمن المعلومات ومعالجتها في العمل؟

تستخدم حزمة تقييم مخاطر أمن المعلومات ومعالجتها في إحاطة اللجنة التوجيهية، وتحديد أصحاب المخاطر، وتمويل المعالجة، وجدولة المراجعة التالية.



بماذا يختلف تقييم مخاطر أمن المعلومات ومعالجتها عن دورة في حوكمة الأمن السيبراني؟

يركز تقييم مخاطر أمن المعلومات ومعالجتها على منهج لتحديد المخاطر وتقييمها ومعالجتها، بينما تركز حوكمة الأمن السيبراني على رقابة المجلس والمساءلة.