

دورة الإشراف على مخاطر الأمن السيبراني: تقبل المخاطر والضوابط والأطراف الخارجية

2027 – 19 سبتمبر

الدوحة





دورة الإشراف على مخاطر الأمن السيبراني: تقبل المخاطر والضوابط والأطراف الخارجية

المرجع: 21330_319 التاريخ: 19 - 23 سبتمبر 2027 المكان: الدوحة الرسوم: GBP 4300

ملخص البرنامج

الإشراف على مخاطر الأمن السيبراني محور دورة تدريبية تمتد أسبوع بمسئول إداري لأعضاء مجالس الإدارة ورؤساء المخاطر والامتثال وقيادات الوحدات، ويخرج منها كل مشارك بحزمة إشراف على المخاطر السيبرانية لمؤسسة أو إدارة واحدة. فالحوكمة السيبرانية تتوزع غالباً بين فرق تقنية ولجان لا ترى إلا تقارير جزئية. ويتدرج البرنامج من الأدوار وتقبل المخاطر، مروراً بتقييم المخاطر والضوابط، إلى مخاطر الأطراف الخارجية ورفع التقارير للمجلس، ثم إلى حزمة عملية. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في الإشراف على مخاطر الأمن السيبراني.

المبررات المؤسسية

القيادات التي لا تستطيع تحديد حجم المخاطر السيبرانية التي تقبلها المؤسسة تعرف الجواب عادة بعد وقوع حادث. أما الإشراف الذي يحدد مستوى التقبل ويختبر تأكيد الضوابط ويتابع الموردين، فيمنح المجالس والإدارات التنفيذية أدلة لمساعدة الإدارة وتوجيه الاستثمار.

- المخاطر السيبرانية بلا مالك: تنخفض حين تحل بيانات التقبل والملك ودورات المراجعة محل الترتيبات غير الرسمية.
- فجوات تأكيد الضوابط: تضيق حين تطلب القيادات أدلة على عمل الضوابط لا على وجود السياسات فقط.
- التعرض عبر الأطراف الخارجية: يقل حين تحدد فئات الموردين ومتطلبات العقود والمتابعة بحسب المخاطر.

المبادئ والأساس المعرفي

- NIST Cybersecurity Framework 2.0 إطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير: تنظم وظيفة الحوكمة فيه، من السياق واستراتيجية المخاطر والأدوار والسياسات، عمل الإشراف في الجلستين 1 و4.
- ISO/IEC 27005 إدارة مخاطر أمن المعلومات: توجه إرشاداته عمل تقييم المخاطر وسجلها في الجلسة 2.
- ISO 31000 إدارة المخاطر: تقوم عليه قرارات تقبل المخاطر ومعالجتها ومتابعتها في الجلستين 1 و3.



المشاركون المستهدفون

- أعضاء مجالس الإدارة الذين يشرفون على مخاطر المؤسسة ويساءلون الإدارة عن التعرض السيبراني.
- رؤساء المخاطر والامثال الذين يديرون السجلات والسياسات وخطط التأكد.
- قيادات الوحدات التي تملك العمليات والبيانات والموردين الحاملين للمخاطر السيبرانية.
- أمناء اللجان الذين يعدون التقارير السيبرانية للمنتديات العليا.

يخدم البرنامج المصارف وقطاع الطاقة والرعاية الصحية وجهات القطاع العام.

مخرجات التعلم

1. سيكون المشاركون قادرين على تحديد أدوار الحوكمة السيبرانية وصلاحيات القرار لدى المجلس واللجنة والإدارة التنفيذية.
2. سيكون المشاركون قادرين على بناء بيان لتقبل المخاطر بحدود سيبرانية قابلة للقياس.
3. سيكون المشاركون قادرين على تقييم سجل المخاطر السيبرانية من حيث الملكية ومنطق التصنيف ودالة المعالجة.
4. سيكون المشاركون قادرين على تشخيص فجوات التأكد بمقارنة أدلة الضوابط بالسياسة المعلنة.
5. سيكون المشاركون قادرين على ترتيب أولويات مخاطر الموردين والأطراف الخارجية بحسب الفئة ومتطلبات العقد.
6. سيكون المشاركون قادرين على تبرير حزمة التقارير للمجلس وقواعد التصعيد أمام رئيس اللجنة.

هيكل البرنامج

اليوم 1: الإشراف على مخاطر الأمن السيبراني: الأدوار وتقبل المخاطر

من يقرر في المخاطر السيبرانية، وما القدر الذي تقبله المؤسسة؟

- وظيفة الحوكمة في NIST Cybersecurity Framework 2.0
- خريطة صلاحيات القرار وتفويض اللجان
- بيان تقبل المخاطر وفق ISO 31000
- مقاييس حدود تحمل المخاطر السيبرانية
- مراجعة حالتين لإخفاقات حوكمة من قطاعين

اليوم 2: تقييم المخاطر والسجل

كيف تحدد المخاطر السيبرانية وتصنف وتسجل بصورة تتيح للقيادات مساءلتها؟



- عملية تقييم المخاطر وفق ISO/IEC 27005
- مراجعة سجل المخاطر السيبرانية
- تصنيف أثر السيناريوهات واحتمالها
- مصفوفة مساءلة مالكي المخاطر
- مراجعة فجوات إطار السياسات

اليوم 3: الضوابط والتأكيد والأطراف الخارجية

ما الدليل على أن الضوابط تعمل وأن الموردين تحت الإدارة؟

- طلب أدلة تأكيد الضوابط
- خريطة التأكيد بخطوط الدفاع الثلاثة
- نموذج تصنيف الموردين بحسب المخاطر
- قائمة متطلبات الأمن في العقود
- قواعد متابعة المعالجة

اليوم 4: التقارير والحوادث والتصعيد

ما الذي ينبغي أن يراه المجلس، ومتى يصعد الموضوع؟

- حزمة تقارير المخاطر السيبرانية للمجلس
- مجموعة مؤشرات المخاطر الرئيسية
- حدود التصعيد في الحوادث
- أدوار الإبلاغ للجهات الرقابية والعملاء
- مجموعة أسئلة المساءلة في اللجنة

اليوم 5: تطبيق الإشراف على مخاطر الأمن السيبراني على مؤسسة واحدة

هل حزمة الإشراف جاهزة ليعتمدها رئيس اللجنة والراعي التنفيذي؟

- تطبيق بيان التقبل من الجلسة 1 على المؤسسة المختارة
- اختبار السجل من الجلسة 2 على سيناريوهات نموذجية
- فحص طلبات التأكيد من الجلسة 3 مقابل فئات الموردين
- تطبيق حدود التصعيد من الجلسة 4 على القضايا المفتوحة
- إنجاز حزمة الإشراف على المخاطر السيبرانية



المنهجية

يقوم البرنامج على تمارين منظمة وتحليل حالات، إذ يعمل المشاركون على مؤسسة مجهولة المصدر وسجل نموذجي وأدلة نموذجية للموردين والضوابط، فيحددون مستوى التقييم ويصنفون السيناريوهات ويصوغون التقارير في فرق صغيرة، ثم يدافعون عن حزمهم أمام لجنة مجلس محاكاة. ولا يتطلب البرنامج خلفية تقنية في الأمن.

- نشاط مقترح: صياغة ثلاثة حدود لتحمل المخاطر لشركة مدفوعات.
- نشاط مقترح: مساهمة بند نموذجي في السجل يفتقر إلى مالِك وموعد للمعالجة.
- نشاط مقترح: تصنيف عشرة موردين نموذجيين واختيار طلبات الأدلة لكل فئة.

المخرج الختامي

يعد كل مشارك حزمة إشراف على المخاطر السيبرانية لمؤسسة أو إدارة واحدة. وتتضمن خريطة لصلاحيات القرار، وبياننا لتقبل المخاطر، وسجلا مراجعا للمخاطر، وخطة للتأكيد والموردين، وحزمة تقارير، وقواعد للتصعيد. وتستخدم لإحاطة رئيس اللجنة والراعي التنفيذي.

الأسئلة الشائعة

هل يناسب الإشراف على مخاطر الأمن السيبراني أعضاء مجالس الإدارة من غير ذوي الخبرة التقنية؟

نعم، فالإشراف على مخاطر الأمن السيبراني بمستوى إداري، ويفترض مسؤولية عن المخاطر أو الامتثال أو قرارات الأعمال، لا مهارات في الأمن التقني أو البرمجة.

ما الأطر التي يقوم عليها الإشراف على مخاطر الأمن السيبراني؟

يقوم الإشراف على مخاطر الأمن السيبراني على NIST Cybersecurity Framework 2.0 للحوكمة، وISO/IEC 27005 لتقييم المخاطر، وISO 31000 لإدارة المخاطر.

كيف تستخدم الحزمة الناتجة عن الإشراف على مخاطر الأمن السيبراني في العمل؟

تستخدم الحزمة الناتجة عن الإشراف على مخاطر الأمن السيبراني لإحاطة رئيس اللجنة والراعي التنفيذي، ومساهمة الإدارة بالأدلة، وتحديد دورات المراجعة.



بماذا يختلف الإشراف على مخاطر الأمن السيبراني عن التدريب على تدقيق الأمن السيبراني؟

يركز الإشراف على مخاطر الأمن السيبراني على قرارات القيادات وتقبل المخاطر والتقارير، بينما يركز التدريب على تدقيق الأمن السيبراني على اختبار الضوابط وكتابة ملاحظات التدقيق.