JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة ضوابط المخاطر الرقمية لنظم المعلومات

1 – 5 مارس 2027

الدار البيضاء

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة ضوابط المخاطر الرقمية لنظم المعلومات

المرجع: 3117_118307 **التاريخ:** 1 – 5 مارس 2027 **المكان:** الدار البيضاء **الرسوم:** GBP 4900

ضوابط المخاطر الرقمية لنظم المعلومات دورة تدريبية مدتها أسبوع لمسؤولي المخاطر والرقابة الداخلية وأمن المعلومات، يخرج منها المشاركون بمصفوفة ضوابط المخاطر الرقمية لنظام معلومات واحد. ومع انتقال الأنظمة إلى الاستضافة السحابية والموردين والوصول عن بعد، صار على المنظمات أن تثبت أن كل ضابط يعمل فعلا لا أنه موجود على الورق فقط. وتقدم جوبيتر برايم للتدريب ضوابط المخاطر الرقمية عملا مشتركا بين وظائف المخاطر والرقابة والأمن.

لماذا تهم ضوابط المخاطر الرقمية الآن

ثلاث قوى تشكل ضوابط المخاطر الرقمية اليوم. فالعمليات الأساسية تجري على منصات مستضافة وخدمات موردين، فلم تعد حدود الرقابة تطابق شبكة المنظمة نفسها. ولجان المراجعة والمراجعون الخارجيون يطلبون أدلة على أن الضوابط تعمل على امتداد فترة زمنية، لا مجرد سياسات مكتوبة. كما يستهدف المهاجمون بيانات الدخول أكثر من البنية التحتية، فانتقل الاهتمام إلى صلاحيات الوصول والمراقبة. والمنظمة التي تربط كل أصل معلوماتي بضوابط مختبرة تتعامل مع الحوادث بوضوح، أما التي تعتمد على إعدادات غير مختبرة فتكتشف ثغراتها أثناء مراجعة أو اختراق.

المستفيدون من ضوابط المخاطر الرقمية

- المسؤولون عن سجل مخاطر الأصول المعلوماتية وتقدير التعرض الكامن والمتبقي
- مختصو الرقابة الداخلية الذين يصممون ضوابط الأنظمة الآلية واليدوية ويوثقونها ويختبرونها
- مسؤولو أمن المعلومات عن قواعد الوصول وإعدادات التشفير ومعالجة التنبيهات
- مراجعو التأكيد الذين يفحصون عينات أدلة الضوابط ويرفعون أوجه القصور إلى لجان المراجعة
- قادة الإشراف على الموردين الذين يقيمون الخدمات المستضافة وعمليات الأنظمة المسندة إلى جهات خارجية

تتحقق أقوى النتائج حين تحضر وظيفة المخاطر مع زملائها في الرقابة الداخلية وفريق الأمن معا.

قدرات ضوابط المخاطر الرقمية

ينتقل المشاركون من سرد التهديدات إلى إثبات أن ضمانات محددة تخفض التعرض في نظام بعينه.

- تقييم الأصول المعلوماتية حسب أثر السرية والسلامة والتوافر — قرار المعالجة لدى مالك الخطر
- تصميم ضوابط وقائية وكاشفة وتصحيحية للوصول والتشفير — مالك النظام
- تحديد قواعد التسجيل والمراقبة التي تنتج تنبيهات قابلة للاستخدام — قائد عمليات الأمن
- اختبار ضوابط الموردين والخدمات المستضافة مقابل شروط العقد — وظيفة المشتريات والإشراف على الموردين
- بناء ملفات أدلة الضوابط التي تصمد أمام فحص العينات — مراجعو التأكيد الداخليون والخارجيون
- عرض أوجه قصور الضوابط مع درجة خطورتها ومالكي المعالجة — لجنة المراجعة

مصطلحات ضوابط المخاطر الرقمية الأساسية

- الأصل المعلوماتي — أي مجموعة بيانات أو تطبيق أو خدمة يضر فقدانها أو تغييرها أو تعطلها بعمليات المنظمة أو تعهداتها.
- الخطر المتبقي — التعرض الذي يبقى بعد تطبيق الضوابط القائمة، ويقارن بمستوى قبول المخاطر المعلن لدى المنظمة.
- الحد الأدنى من الصلاحيات — مبدأ أن يحمل كل مستخدم أو حساب خدمة صلاحيات الوصول التي تتطلبها مهمته الحالية فقط.
- فاعلية تشغيل الضابط — دليل على أن الضابط عمل كما صمم طوال فترة محددة، لا في لحظة واحدة فقط.
- نموذج المسؤولية المشتركة — توزيع مهام الأمن بين مزود الخدمة المستضافة والمنظمة العميلة التي تستخدمها.
- الضابط التعويضي — ضمانة بديلة تخفض الخطر حين يتعذر تطبيق الضابط المفضل كاملا.

ضوابط المخاطر الرقمية يوما بيوم

اليوم 1: رسم خريطة الأصول المعلوماتية والتعرض

- جرد الأصول المعلوماتية — أي الأنظمة تحفظ السجلات الحرجة
- تقدير الأثر على السرية والسلامة والتوافر — أولوية المعالجة
- ربط التهديدات بنقاط الضعف — سيناريوهات خسارة واقعية لكل أصل
- تقدير الخطر الكامن مقابل المتبقي — حدود قبول المخاطر وتحملها
- تعيين مالك الخطر — المساءلة عن تعرض كل نظام

اليوم 2: ضمانات الوصول والتشفير

- تصميم الوصول حسب الأدوار والحد الأدنى من الصلاحيات — قواعد الالتحاق والنقل والمغادرة
- الإشراف على الحسابات ذات الامتيازات — خيارات الموافقة وتسجيل الجلسات
- إعادة التصديق الدورية على وصول المستخدمين — إزالة الصلاحيات الزائدة في وقتها
- التشفير أثناء التخزين والنقل — حفظ المفاتيح وتدويرها
- مصفوفة تعارض الفصل بين المهام — منع الاحتيال والخطأ

اليوم 3: التسجيل والمراقبة والكشف

- اختيار مصادر السجلات وقواعد الاحتفاظ بها — الجاهزية للتحقيق
- عتبات التنبيه وحالات الاستخدام — تقليل الضوضاء على المحللين
- مراقبة التغييرات والإعدادات — كشف تغييرات الأنظمة غير المعتمدة
- مسارات تصعيد الحوادث — من يقرر الاحتواء والإفصاح
- مؤشرات أداء الضوابط — إبلاغ القيادة بسلامة الكشف

اليوم 4: اختبار الموردين والخدمات المستضافة والأدلة

- رسم المسؤولية المشتركة — أي المهام تبقى لدى المنظمة
- مراجعة تقارير تأكيد الموردين — الاعتماد على شهادات الأطراف الخارجية
- بنود الأمن التعاقدية وحق المراجعة — أدوات الإشراف على الموردين
- اختبار التصميم مقابل اختبار التشغيل — اختيار طريقة أخذ العينات
- هيكل ملف أدلة الضوابط — الصمود أمام عينات مراجعة التأكيد

اليوم 5: ممارسة مصفوفة ضوابط المخاطر الرقمية

- ملف الأصول والتعرض لنظام مختار — الاتفاق على النطاق
- ربط ضوابط الوصول والتشفير والمراقبة بالمخاطر — فجوات التغطية
- الضوابط التعويضية وتقدير أوجه القصور — ترتيب أولويات المعالجة
- مراجعة الأقران لأدلة الضوابط — الجاهزية لعينات التأكيد
- إكمال مصفوفة ضوابط المخاطر الرقمية — اعتمادها من مالك النظام

تطبيق ضوابط المخاطر الرقمية بعد الدورة

- إجراء إعادة تصديق على وصول المستخدمين في تطبيق حرج واحد، وتوثيق الصلاحيات المزالة دليلا على عمل الضابط.
- مقارنة تقرير التأكيد لخدمة مستضافة واحدة بخريطة المسؤولية المشتركة، وتسجيل أي مهام غير مغطاة.

أسئلة حول ضوابط المخاطر الرقمية

ما ضوابط المخاطر الرقمية لنظم المعلومات ولماذا تهم الآن؟

ضوابط المخاطر الرقمية هي الضمانات التي تخفض التعرض في البيانات والتطبيقات والخدمات. وتهم الآن لأن الأنظمة تعمل عبر موردين ومنصات مستضافة، ولأن مجالس الإدارة تطلب دليلا على أن كل ضمانة تعمل فعلا، لا مجرد سياسة مكتوبة.

من المستفيد الأكبر من دورة ضوابط المخاطر الرقمية؟

يستفيد أكثر مسؤولو المخاطر ومختصو الرقابة الداخلية ومسؤولو أمن المعلومات. ويستفيد كذلك قادة الإشراف على الموردين ومراجعو التأكيد من مجموعة الضوابط الموحدة.

بم تختلف دورة ضوابط المخاطر الرقمية عن دورة عامة في الأمن السيبراني؟

تركز على تصميم الضوابط واختبارها وأدلتها بدلا من أدوات الدفاع التقنية. فتعمل على تقدير التعرض وربط الضمانات بالمخاطر وإثبات التشغيل أمام المراجعين.

ماذا تعود به من دورة ضوابط المخاطر الرقمية؟

تعود بمصفوفة ضوابط مكتملة لنظام معلومات واحد، فيها المخاطر المقدرة والضمانات المرتبطة بها ومراجع الأدلة ومالكو المعالجة.

ضوابط المخاطر الرقمية: الطريق إلى الأمام

توجه مصفوفة ضوابط المخاطر الرقمية أول قرار حول أوجه القصور التي يمولها مالك النظام ويعالجها أولا. يستخدمها مسؤولو المخاطر لتحديث تقديرات الخطر المتبقي، وفرق الأمن لضبط المراقبة، ومراجعو التأكيد لتخطيط العينات. وبعد أول استخدام لها، تستحق مراجعة توزيع مهام الخدمات المستضافة، لأن تغير الموردين ينقل حدود الرقابة بسرعة.