JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في سجل مخاطر الذكاء الاصطناعي واختبار الضوابط

6 – 10 سبتمبر 2027

مدريد

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في سجل مخاطر الذكاء الاصطناعي واختبار الضوابط

المرجع: 55693_1506 **التاريخ:** 6 – 10 سبتمبر 2027 **المكان:** مدريد **الرسوم:** GBP 6200

سجل مخاطر الذكاء الاصطناعي واختبار الضوابط دورة تدريبية مدتها أسبوع لمديري المخاطر المؤسسية ومخاطر تقنية المعلومات والامتثال الذين يوثقون تعرضات الأنظمة الذكية ويختبرون ضوابطها في وحدات الأعمال، ويخرج منها المشاركون بخطة اختبار ضوابط الذكاء الاصطناعي. فمع انتقال النماذج من التجارب المعزولة إلى الإقراض وخدمة العملاء وتشغيل الشبكات، تتوقع مجالس الإدارة أن تظهر هذه التعرضات في السجل نفسه مع سائر المخاطر. وتقدم جوبيتر برايم للتدريب هذه الدورة لوظائف خط الدفاع الثاني.

لماذا يهم سجل مخاطر الذكاء الاصطناعي واختبار الضوابط الآن

تضغط ثلاث جهات اليوم على خط الدفاع الثاني: وحدات الأعمال تنشر النماذج والخدمات الذكية المشتراة أسرع مما تستطيع فرق الرقابة حصره، والمدققون يطلبون دليلا على أن الضوابط تعمل فعلا لا أنها مكتوبة فقط، والمجالس تريد معرفة التعرض مقارنة بشهية المخاطر المعتمدة. والمؤسسة التي تحتفظ بسجل حي وتختبر ضوابطها تكتشف إخفاقات النماذج الصامتة مبكرا وتجيب أسئلة التدقيق بالأدلة، أما غيرها فلا تعلم بالاستخدام غير الموثق إلا بعد وقوع حادثة. وتستند الدورة إلى ISO/IEC 42001، المعيار الدولي لنظام إدارة الذكاء الاصطناعي، وإلى إطار إدارة مخاطر الذكاء الاصطناعي AI RMF NIST.

المستفيدون من سجل مخاطر الذكاء الاصطناعي واختبار الضوابط

- أصحاب السجل المؤسسي وتصنيفاته
- مختصو مخاطر التقنية الذين يقيمون النماذج ومسارات البيانات والخدمات الذكية
- كوادر الامتثال الذين يربطون الاستخدام بالسياسات الداخلية والمتطلبات الخارجية
- مختبرو الضوابط الذين يخططون جولات التتبع وسحب عينات الأدلة
- كوادر مخاطر الموردين الذين يراجعون المنتجات الذكية المشتراة

تستفيد وظيفة خط الدفاع الثاني أكثر حين يحضر صاحب السجل ومختص مخاطر التقنية ومختبر الضوابط فيها معا.

قدرات سجل مخاطر الذكاء الاصطناعي واختبار الضوابط

يحول المشاركون الاستخدام المتناثر للأنظمة الذكية إلى قيود مصنفة الدرجة مقرونة بضوابط قابلة للاختبار والإبلاغ.

- بناء جرد للأنظمة الذكية وقيود موثقة بأصحابها ودرجاتها — لجنة المخاطر
- حساب التعرض الكامن والمتبقي بمقياس تقدير موحد — قرارات الشهية
- تصميم ضوابط خاصة بالبيانات وتغيير النماذج والإشراف البشري — أصحاب وحدات الأعمال
- اختبار تشغيل الضوابط بجولات التتبع والعينات وإعادة الأداء — التدقيق الداخلي
- تقييم الخدمات الذكية للأطراف الخارجية باستبيانات العناية الواجبة — موافقة المشتريات
- عرض التعرض مقارنة بالشهية في لوحة لمجلس الإدارة — أعضاء المجلس

مصطلحات سجل مخاطر الذكاء الاصطناعي واختبار الضوابط الأساسية

- جرد الأنظمة الذكية — قائمة محدثة بكل نموذج وخدمة ذكية مستخدمة مع المالك والغرض ومصادر البيانات.
- الخطر الكامن — التعرض الذي يحمله النظام الذكي قبل تطبيق أي ضابط.
- الخطر المتبقي — التعرض الباقي بعد وجود الضوابط وعملها.
- بيان شهية المخاطر — حد يعتمده المجلس لمقدار التعرض الذي تقبله المؤسسة من الأنظمة الذكية.
- اختبار فاعلية التشغيل — دليل على أن الضابط عمل كما صمم خلال فترة، لا على الورق فقط.
- مؤشر الخطر الرئيسي — إشارة مقاسة مثل انحراف النموذج أو معدل التجاوز تنبه عند ارتفاع التعرض.

سجل مخاطر الذكاء الاصطناعي واختبار الضوابط يوما بيوم

اليوم 1: تعرض المؤسسة للأنظمة الذكية

- مسح اكتشاف الاستخدام — العثور على النماذج والخدمات غير الموثقة
- حقول جرد الأنظمة الذكية — المالك والغرض والبيانات ودرجة الأهمية
- نطاق نظام الإدارة وفق ISO/IEC 42001 — حدود السجل
- تصنيف المخاطر الذكية — فئات الإنصاف والمتانة والخصوصية والأمن
- مقارنة حالتي البنوك والاتصالات — اختلاف التعرض حسب القطاع

اليوم 2: تقدير المخاطر الذكية وتوثيقها

- نموذج القيد — السبب والحدث والأثر والمالك
- مقاييس الاحتمال والأثر للنماذج — درجات كامنة متسقة
- وظيفة الرسم في NIST AI RMF — تحديد السياق والضرر
- بيانات شهية المخاطر للأنظمة الذكية — حدود تحمل يعتمدها المجلس
- مؤشرات الخطر للانحراف والتجاوزات — عتبات الإنذار المبكر

اليوم 3: تصميم ضوابط الأنظمة الذكية

- ضوابط جودة البيانات ونسبها — المدخلات التي تغذي النماذج
- ضوابط تغيير النماذج وإطلاقها — الموافقة قبل التشغيل
- نقاط الإشراف البشري — مواضع مراجعة الأشخاص للقرارات الآلية
- استبيان العناية الواجبة للأطراف الخارجية — معايير اعتماد المورد
- مصفوفة ربط الضوابط بالمخاطر — فجوات التغطية في السجل

اليوم 4: الاختبار والتصعيد والإبلاغ

- جولات التتبع واختبارات فاعلية التصميم — مدى ملاءمة الضابط
- اختيار العينات وإعادة الأداء — إثبات فاعلية التشغيل
- وظيفتا القياس والإدارة في NIST AI RMF — الأدلة والمعالجة
- مسار تصعيد الحوادث الذكية — عتبات إبلاغ كبار المالكين
- لوحة المجلس للتعرض الذكي — التعرض المتبقي مقابل الشهية

اليوم 5: ممارسة خطة اختبار ضوابط الذكاء الاصطناعي

- حالة نموذج التصنيف الائتماني — تطبيق الجرد والتقدير والضوابط
- حالة خدمة المحادثة مع العملاء — اختبار ضوابط مورد خارجي
- تقدير النتائج وتحديد مالكي المعالجة — سد فجوات الضوابط
- تحديث السجل بعد الاختبار — درجات متبقية معدلة
- خطة اختبار ضوابط الذكاء الاصطناعي — النطاق والعينات والجدول والإبلاغ

تطبيق سجل مخاطر الذكاء الاصطناعي واختبار الضوابط بعد الدورة

- إجراء مسح اكتشاف في وحدة أعمال واحدة وإضافة كل نموذج غير موثق إلى السجل مع مالكه ودرجته الكامنة.
- قيادة جولة تتبع واختبار عينات لضابط تغيير نموذج واحد وعرض النتيجة مقارنة بالشهية المعتمدة.

أسئلة حول سجل مخاطر الذكاء الاصطناعي واختبار الضوابط

ما سجل مخاطر الذكاء الاصطناعي واختبار الضوابط ولماذا يهم الآن؟

هو توثيق تعرضات الأنظمة الذكية في السجل المؤسسي وإثبات أن ضوابطها تعمل. ويهم الآن لأن الاستخدام ينتشر أسرع من الرقابة، والمدققون والمجالس يتوقعون أدلة مختبرة لا بيانات سياسات.

من الأدوار الأكثر استفادة من سجل مخاطر الذكاء الاصطناعي واختبار الضوابط؟

مديرو المخاطر المؤسسية ومختصو مخاطر التقنية ومديرو الامتثال ومختبرو الضوابط هم الأكثر استفادة. وتستفيد إن كنت تملك سجلا أو تعتمد موردين للأنظمة الذكية أو تخطط أعمال التأكيد.

كيف يختلف سجل مخاطر الذكاء الاصطناعي واختبار الضوابط عن دورة في حوكمة الذكاء الاصطناعي؟

يعمل على مستوى القيود والدرجات واختبارات الضوابط لا على السياسات وتصميم اللجان. وتخرج بأساليب سحب العينات ونصوص الاختبار بدلا من ميثاق حوكمة.

ماذا تعود به من سجل مخاطر الذكاء الاصطناعي واختبار الضوابط؟

تعود بخطة لاختبار الضوابط تضم نطاق الجرد والقيود المقدرة ومصفوفة ربط الضوابط وأحجام العينات وصيغة الإبلاغ للمجلس.

سجل مخاطر الذكاء الاصطناعي واختبار الضوابط: الطريق إلى الأمام

تحدد خطة اختبار ضوابط الذكاء الاصطناعي أولا الأنظمة التي تخضع للاختبار في هذه الدورة الرقابية. ويستخدمها أصحاب السجل ومختصو مخاطر التقنية والتدقيق الداخلي للاتفاق على النطاق والأدلة. وبعد أول استخدام لها تستحق مقاييس التقدير المراجعة، لأن نتائج الاختبار تكشف غالبا أن بعض الدرجات الكامنة وضعت أقل من اللازم للنماذج التي تتعامل مع العملاء مباشرة.