JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها

12 – 16 سبتمبر 2027

القاهرة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها

المرجع: 41_1031 **التاريخ:** 12 – 16 سبتمبر 2027 **المكان:** القاهرة **الرسوم:** GBP 4000

حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها دورة تدريبية مدتها أسبوع لمختصي المخاطر والامتثال وحوكمة تقنية المعلومات المطالبين بإبقاء وكلاء الذكاء الاصطناعي المستقلين ضمن الصلاحيات المعتمدة، ويخرج كل مشارك منها بسجل ضوابط الوكلاء. تشغل المؤسسات اليوم وكلاء يرسلون الرسائل وينقلون البيانات وينفذون المعاملات بتدخل بشري محدود. وتقدم جوبيتر برايم للتدريب هذه الدورة لوظائف الرقابة التي تضع القواعد قبل توسع هؤلاء الوكلاء.

لماذا يهم حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها الآن

تشكل ثلاث قوى هذا المجال اليوم: منصات وكلاء تتيح لفرق الأعمال إطلاق سير عمل مستقل، ومدققون ومجالس إدارة يسألون عن المسؤول حين تتصرف البرمجيات من تلقاء نفسها، ومهاجمون يستهدفون الوكلاء عبر مدخلات متلاعب بها. المؤسسة التي تحسن حوكمة الوكلاء تكسب السرعة دون أن تفقد السيطرة على المدفوعات والبيانات وتعهدات العملاء، أما التي تهملها فلا تكتشف الإجراءات غير المصرح بها إلا بعد وقوع الضرر. وتستند الدورة إلى المعيار الدولي ISO/IEC 42001 لنظام إدارة الذكاء الاصطناعي، وإلى إطار NIST AI RMF NIST AI Risk Management Framework لرصد مخاطر الوكلاء وإدارتها.

المستفيدون من حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها

- مختصو المخاطر الذين يقيمون التقنيات الجديدة ويحدثون سجل المخاطر
- مسؤولو الامتثال الذين يتحققون من مطابقة الإجراءات الآلية للسياسات والحدود التعاقدية
- قادة حوكمة تقنية المعلومات الذين يديرون حقوق الوصول وحسابات الخدمة واعتماد التغييرات
- المدققون الداخليون الذين يحتاجون مسارات أدلة للقرارات الآلية
- فرق أمن المعلومات التي تحمي الأنظمة من إساءة استخدام أدوات الوكلاء

تحقق وظائف الرقابة أعلى استفادة عندما يحضر معا زملاء من المخاطر والامتثال وحوكمة تقنية المعلومات، لأن ضوابط الوكلاء تمتد عبر هذه المجالات الثلاثة.

قدرات حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها

يغادر المشاركون وهم قادرون على تصنيف الوكلاء المستقلين وتقييدهم ومراقبتهم وتدقيقهم ضمن الحدود المعتمدة.

- تقييم مخاطر الوكيل بدرجات الاستقلالية والأثر وإمكانية التراجع — للجان المخاطر التي تعتمد التشغيل
- تصميم تفويض الصلاحيات والأذونات بأقل امتياز للوكلاء — لملاك العمليات والأنظمة
- تحديد نقاط الإشراف البشري للإجراءات عالية الأثر — للمعتمدين في وحدات الأعمال
- بناء متطلبات المراقبة وسجلات التدقيق التي تعيد بناء سلوك الوكيل — للمدققين الداخليين والخارجيين
- اختبار أدلة الاستجابة للحوادث بما فيها مفاتيح الإيقاف والاحتواء — لعمليات الأمن

مصطلحات حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها الأساسية

- الذكاء الاصطناعي الوكيل — أنظمة ذكاء اصطناعي تخطط لمهام متعددة الخطوات وتنفذها مستدعية الأدوات والأنظمة بتوجيه بشري محدود.
- تفويض الصلاحيات — الحدود الموثقة لما يجوز لشخص أو وكيل اتخاذه من قرارات أو إجراءات دون اعتماد إضافي.
- أقل امتياز — منح الوكيل الحد الأدنى فقط من الوصول والإجراءات اللازمة لمهمته المحددة.
- نقطة الإشراف البشري — موضع محدد يجب فيه أن يراجع شخص الإجراء المقترح من الوكيل أو يعتمده قبل تنفيذه.
- سجل التدقيق — سجل محمي من العبث لمدخلات الوكيل وقراراته واستدعاءاته للأدوات ونتائجه لمراجعتها لاحقا.
- مفتاح الإيقاف — ضابط يوقف نشاط الوكيل فورا عندما يصبح سلوكه غير آمن أو غير مصرح به.

حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها يوما بيوم

اليوم 1: كيف يغير وكلاء الذكاء الاصطناعي بيئة الرقابة

- بنية الوكيل — الأهداف وحلقات التخطيط والذاكرة واستدعاء الأدوات
- سلم مستويات الاستقلالية — من الاقتراح إلى التنفيذ دون إشراف
- جرد الوكلاء وملكيتهم — معرفة الوكلاء الذين يتصرفون باسم المؤسسة
- أنماط إخفاق الوكلاء المستقلين — انحراف الهدف والتكرار وتجاوز الصلاحية
- حالات استخدام الوكلاء في خدمة العملاء والمشتريات

اليوم 2: تفويض الصلاحيات والأذونات

- مصفوفات تفويض الصلاحيات — حدود الإنفاق والاعتماد والتواصل
- وصول الأدوات بأقل امتياز — تحديد نطاق واجهات البرمجة والأنظمة والإجراءات
- حدود أذونات البيانات — تصنيف ما يجوز للوكلاء قراءته أو كتابته
- هويات الوكلاء وبيانات اعتمادهم — حسابات الخدمة وإدارة الأسرار
- الفصل بين المهام بين الوكلاء والمعتمدين من البشر

اليوم 3: تقييم مخاطر الوكلاء وفق المعايير

- ضوابط ISO/IEC 42001 — إدراج الوكلاء ضمن نظام إدارة الذكاء الاصطناعي
- وظائف NIST AI RMF — الحوكمة والرصد والقياس والإدارة للأنظمة الوكيلة
- تقييم مخاطر الوكيل — الأثر والاستقلالية وإمكانية التراجع عن الإجراءات
- سيناريوهات التهديد — حقن الأوامر وإساءة استخدام الأدوات وتسريب البيانات
- منصات الوكلاء الخارجية — أسئلة التأكد من الموردين

اليوم 4: الإشراف والمراقبة والتعامل مع الحوادث

- نقاط الإشراف البشري — بوابات اعتماد للإجراءات عالية الأثر
- الحواجز أثناء التشغيل — حدود المعدل وسقوف الميزانية وقوائم الإجراءات المسموحة
- لوحات مراقبة السلوك — الشذوذ والتصعيد وعدد مرات التجاوز اليدوي
- سجلات التدقيق والإجراءات — إعادة بناء ما فعله الوكيل ولماذا
- أدلة الاستجابة لحوادث الوكلاء — مفاتيح الإيقاف والاحتواء ومراجعة السبب الجذري

اليوم 5: التطبيق العملي لسجل ضوابط الوكلاء

- تطبيق تقييم الاستقلالية والمخاطر — تصنيف وكلاء من مؤسسات المشاركين
- تصميم الأذونات والتفويض — وضع حدود لوكيل مختار
- خطة نقاط الإشراف والمراقبة — دمج أساليب الرقابة السابقة
- اختبار الجاهزية للتدقيق والحوادث — محاكاة إخفاق وكيل خطوة بخطوة
- سجل ضوابط الوكلاء — استكمال الوثيقة النهائية وعرضها

تطبيق حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها بعد الدورة

- بناء جرد للوكلاء المستخدمين في المؤسسة وتقييم كل منهم من حيث الاستقلالية والأثر
- إدخال نقاط اعتماد وتسجيل للإجراءات للوكيل الأعلى خطورة ومراجعتها مع مالكه في وحدة الأعمال

أسئلة حول حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها

ما هي حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها، ولماذا تهم الآن؟

هي مجموعة السياسات والأذونات والإشراف وضوابط التدقيق التي تبقي وكلاء الذكاء الاصطناعي المستقلين ضمن الصلاحيات المعتمدة. وتهم الآن لأن الوكلاء أصبحوا يتصرفون مباشرة في الأنظمة والبيانات ومع العملاء بمراجعة بشرية محدودة.

من هم الأكثر استفادة من حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها؟

الأكثر استفادة هم مختصو المخاطر والامتثال وحوكمة تقنية المعلومات. فأنت تعتمد المخاطر التقنية أو تتحقق من الامتثال للسياسات أو تدير الوصول، لذا تحتاج طرقا عملية لتصنيف سلوك الوكلاء وتقييده وتدقيقه.

كيف يختلف تدريب حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها عن دورة عامة في حوكمة الذكاء الاصطناعي؟

يركز هذا التدريب على الأنظمة التي تتصرف لا التي تقدم المشورة فقط. فالدورة العامة تغطي السياسات ومخاطر النماذج بوجه عام، أما هنا فتتناول حدود التفويض وأذونات الأدوات والحواجز أثناء التشغيل وسجلات التدقيق والتعامل مع الحوادث للوكلاء المستقلين.

ماذا تعود به من تدريب حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها؟

تعود بسجل ضوابط للوكلاء في مؤسستك. ويوثق لكل وكيل درجات الاستقلالية والمخاطر والأذونات ونقاط الإشراف ومتطلبات المراقبة وخطوات الاستجابة للحوادث.

حوكمة وكلاء الذكاء الاصطناعي والرقابة عليها: الطريق إلى الأمام

يحدد سجل ضوابط الوكلاء أولا الوكلاء المسموح بتشغيلهم دون إشراف والوكلاء الذين يحتاجون بوابات اعتماد. وتستخدمه فرق المخاطر والامتثال وحوكمة تقنية المعلومات للاتفاق مع ملاك الأعمال على الأذونات والمراقبة وأدلة التدقيق. وبعد الربع الأول، تستحق درجات الاستقلالية وعدد مرات التجاوز اليدوي مراجعة جديدة، لأن الاستخدام الفعلي يكشف مواضع تشدد الحدود أو تساهلها.