JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة حوكمة الأمن السيبراني والمخاطر والامتثال

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة حوكمة الأمن السيبراني والمخاطر والامتثال

حوكمة الأمن السيبراني والمخاطر والامتثال دورة تدريبية مدتها أسبوع لمحللي الحوكمة والمخاطر والامتثال ومسؤولي أمن المعلومات والمدققين الداخليين، يعود منها المشاركون بمصفوفة الضوابط السيبرانية وحزمة الأدلة التي تربط السياسات بالضوابط وبإثباتات التدقيق. فالعملاء وشركات التأمين ولجان التدقيق باتوا يطلبون ضوابط سيبرانية قابلة للإثبات لا مجرد تطمينات، فصار التسلسل المتماسك للسياسات والأدلة القابلة للتتبع حاجة يومية. تقدم جوبيتر برايم للتدريب هذه الدورة في حوكمة الأمن السيبراني والمخاطر والامتثال.

لماذا تهم حوكمة الأمن السيبراني والمخاطر والامتثال الآن

تلتقي ثلاثة ضغوط على فرق الحوكمة السيبرانية: لجان تدقيق تريد تقييما واضحا للوضع الأمني كل ربع سنة، ومتطلبات ضوابط متداخلة من العقود وشركات التأمين والقواعد القطاعية، وخدمات سحابية تنقل ملكية بعض الضوابط إلى الموردين. الفريق الذي يملك مكتبة ضوابط واحدة تطابق مرة وتختبر باستمرار يجيب عن كل استبيان جديد خلال أيام، أما الفريق الذي يفتقدها فيعيد بناء الأدلة مع كل طلب. وتستند الدورة إلى إطار NIST Cybersecurity Framework 2.0 المعروف اختصارا NIST CSF 2.0 الذي تؤطر وظيفة Govern فيه الإشراف، وإلى معيار ISO/IEC 27001:2022 لمتطلبات نظام إدارة أمن المعلومات.

المستفيدون من حوكمة الأمن السيبراني والمخاطر والامتثال

- محللو الحوكمة والمخاطر والامتثال الذين يديرون مكتبات الضوابط وسجلات السياسات وتقويم الامتثال
- مسؤولو أمن المعلومات الذين يصوغون السياسات ويعتمدون الاستثناءات
- المدققون الداخليون الذين يختبرون الضوابط السيبرانية ويحكمون على كفاية الأدلة
- أخصائيو خط الدفاع الثاني الذين يقيمون التعرض السيبراني ضمن ملف مخاطر المؤسسة
- موظفو ضمان الموردين الذين يقيمون استبيانات الأمن وشهادات المطابقة المقدمة من الموردين

تستفيد وظيفة خط الدفاع الثاني أكثر حين ترسل محلل الحوكمة ومدققا داخليا معا، فيعودان متفقين على الدليل الذي يثبت فعالية الضابط.

قدرات حوكمة الأمن السيبراني والمخاطر والامتثال

يحول المشاركون السياسات والمتطلبات المبعثرة إلى سلسلة واحدة قابلة للتتبع من التعهد إلى الضابط المختبر.

- تصميم هيكل حوكمة سيبرانية بمواثيق وأدوار وخطوط تصعيد — اللجنة التوجيهية للأمن
- بناء تسلسل السياسات من السياسة إلى المعيار إلى الإجراء — مالكو السياسات ومعتمدوها
- مواءمة المتطلبات المتداخلة في مصفوفة ضوابط واحدة باستخدام NIST CSF 2.0 وISO/IEC 27001:2022 — مالكو الضوابط
- تحديد معايير الأدلة وأسلوب العينات لاختبار الضوابط — المدققون الداخليون والخارجيون
- موازنة طلبات استثناء السياسات مقابل المخاطر المتبقية — جهة قبول المخاطر
- إيصال الوضع السيبراني عبر المؤشرات والخرائط الحرارية — لجنة التدقيق والمخاطر

مصطلحات حوكمة الأمن السيبراني والمخاطر والامتثال الأساسية

- مصفوفة الضوابط — جدول يربط كل متطلب بالضابط الداخلي ومالكه وأسلوب اختباره والدليل عليه.
- تسلسل السياسات — مجموعة متدرجة من السياسات والمعايير والإجراءات والإرشادات، كل مستوى أكثر تفصيلا مما فوقه.
- استثناء السياسة — خروج معتمد ومحدد المدة عن سياسة ما، مع تدابير تعويضية ومالك مخاطر مسمى.
- اختبار فعالية الضوابط — التحقق بالفحص أو الملاحظة أو إعادة التنفيذ من أن الضابط يعمل كما صمم.
- بيان قابلية التطبيق — وثيقة في ISO/IEC 27001 تبين الضوابط المطبقة والمستبعدة وأسباب ذلك.
- الوضع السيبراني — الحالة العامة لدفاعات المؤسسة السيبرانية، معبرا عنها بالمؤشرات وتقييمات النضج.

حوكمة الأمن السيبراني والمخاطر والامتثال يوما بيوم

اليوم 1: هياكل الحوكمة والمساءلة

- نموذج الخطوط الثلاثة في المجال السيبراني — الفصل بين الملكية والإشراف والضمان
- ميثاق اللجنة التوجيهية للأمن — تحديد صلاحيات القرار ومسارات التصعيد
- وظيفة Govern في NIST CSF 2.0 — تأطير السياق المؤسسي والأدوار
- مصفوفة RACI لملكية الضوابط — إزالة المسؤوليات غير المسندة
- مقارنة الحوكمة في القطاع البنكي وقطاع الطاقة — مواءمة الهيكل مع التعرض

اليوم 2: تسلسل السياسات والاستثناءات

- طبقات السياسة والمعيار والإجراء — وضع كل متطلب في موضعه الصحيح
- أعراف صياغة السياسات — كتابة عبارات قابلة للاختبار
- دورة اعتماد السياسات ومراجعتها — إبقاء الوثائق محدثة
- مسار طلب الاستثناء — تسجيل التدابير التعويضية وتاريخ الانتهاء
- إقرار الاطلاع على السياسات — إثبات علم الموظفين بها

اليوم 3: أطر الضوابط والمطابقة

- محاور الملحق A في ISO/IEC 27001:2022 — هيكلة مكتبة الضوابط
- صياغة بيان قابلية التطبيق — تبرير الإدراج والاستبعاد
- المطابقة مع فئات NIST CSF 2.0 — تلبية عدة متطلبات دفعة واحدة
- استقبال متطلبات العقود وشركات التأمين — إضافة التعهدات دون تكرار
- توارث الضوابط من الموردين — تحديد ما يغطيه مزودو الخدمات السحابية

اليوم 4: مراقبة الامتثال وأدلة التدقيق

- أساليب اختبار الضوابط — الاختيار بين الفحص والملاحظة وإعادة التنفيذ
- معايير كفاية الأدلة — الحكم على الاكتمال والموثوقية
- تغذيات المراقبة المستمرة للضوابط — تقليل جمع العينات يدويا
- تصنيف الملاحظات وتتبع المعالجة — ترتيب أولويات الإجراءات التصحيحية
- ربط سجل المخاطر السيبرانية — وصل الضوابط المخففة بالتعرض

اليوم 5: التطبيق العملي لمصفوفة الضوابط السيبرانية وحزمة الأدلة

- مراجعة فجوات الحوكمة — تطبيق دروس الميثاق ومصفوفة RACI على حالة
- لجنة قرارات الاستثناء — تطبيق تقدير المخاطر المتبقية على الطلبات
- محاكاة جولة تدقيق — تطبيق معايير الأدلة على ضوابط نموذجية
- لوحة الوضع السيبراني للجنة — اختيار المؤشرات المناسبة لأعضاء المجلس
- مصفوفة الضوابط السيبرانية وحزمة الأدلة — استكمال المطابقات والمالكين والإثباتات

تطبيق حوكمة الأمن السيبراني والمخاطر والامتثال بعد الدورة

- مطابقة استبيان أمني وارد من أحد العملاء مع مصفوفة الضوابط وتسجيل الأدلة التي تجيب عنه حاليا.
- مراجعة جميع استثناءات السياسات المفتوحة وإغلاق كل منها أو تجديده مع مالك مخاطر مسمى.

أسئلة حول حوكمة الأمن السيبراني والمخاطر والامتثال

ما حوكمة الأمن السيبراني والمخاطر والامتثال، ولماذا تهم الآن؟

هي توجيه الأمن السيبراني عبر الهياكل والسياسات وأطر الضوابط والأدلة. وتهم الآن لأن اللجان والعملاء وشركات التأمين يطلبون إثبات عمل الضوابط، ولأن المتطلبات المتداخلة تضاعف الجهد في غياب مكتبة ضوابط واحدة مطابقة.

من أكثر المستفيدين من تدريب حوكمة الأمن السيبراني والمخاطر والامتثال؟

يستفيد أكثر محللو الحوكمة والمخاطر والامتثال ومسؤولو أمن المعلومات والمدققون الداخليون. فهم يملكون السياسات ومطابقات الضوابط والأدلة التي يعتمد عليها كل تدقيق واستبيان.

كيف تختلف حوكمة الأمن السيبراني والمخاطر والامتثال عن دورة حوكمة الذكاء الاصطناعي؟

تغطي بيئة الضوابط السيبرانية كلها لا الإشراف على نماذج تعلم الآلة وحدها. فدورة حوكمة الذكاء الاصطناعي تتناول سجلات النماذج والمخاطر الخوارزمية، أما هذا المجال فيبني تسلسل السياسات ومطابقات الضوابط وأدلة التدقيق عبر جميع نظم المعلومات.

ماذا تعود به من تدريب حوكمة الأمن السيبراني والمخاطر والامتثال؟

تعود بمصفوفة الضوابط السيبرانية وحزمة الأدلة. تطابق المتطلبات مع الضوابط وتسمي المالكين وتحدد أساليب الاختبار وتسرد الأدلة التي يحتاجها كل ضابط.

حوكمة الأمن السيبراني والمخاطر والامتثال: الطريق إلى الأمام

توجه مصفوفة الضوابط السيبرانية وحزمة الأدلة أول قرار حول الضوابط التي تختبر قبل دورة التدقيق التالية. ويستخدمها محللو الحوكمة ومالكو الضوابط والمدققون الداخليون للإجابة عن الاستبيانات وتخطيط الاختبارات وتتبع المعالجة. وبعد أول تدقيق خارجي تستحق معايير الأدلة المراجعة، إذ تكشف ملاحظات المدققين مواضع ضعف الإثبات أو زيادته لكل ضابط مختبر.