JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في تطبيق نظام إدارة أمن المعلومات وتشغيله

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في تطبيق نظام إدارة أمن المعلومات وتشغيله

تطبيق نظام إدارة أمن المعلومات وتشغيله دورة تدريبية متقدمة مدتها أسبوعين لمديري أمن المعلومات ومالكي نظام ISMS وقادة الامتثال الذين ينقلون النظام من بيان النطاق إلى التشغيل المستقر، وتنتهي بخطة تطبيق مرحلية لنظام إدارة أمن المعلومات. فالعملاء والشركاء يطلبون اليوم دليلا على نظام عامل قبل مشاركة معلوماتهم الحساسة، والنظام غير المختبر يكلف العقود. وتقدم جوبيتر برايم للتدريب هذه الدورة لمن يبقين هذا النظام حيا.

لماذا يهم تطبيق نظام إدارة أمن المعلومات وتشغيله الآن

ثلاث قوى تدفع النظام من الوثائق إلى الممارسة اليومية: عملاء وشركاء في سلاسل الإمداد يطلبون أدلة على ضوابط عاملة في المناقصات والعقود، وخدمات سحابية ومسندة تطمس حدود المعلومات الخاصة بالمنشأة، ومدققون يختبرون انتظام عمل الضوابط لا مجرد وجود السياسات. المنشأة التي تشغل نظامها جيدا تكتشف الخلل عبر رقابتها الذاتية، أما التي تعامله مشروع شهادة فتكتشفه عبر الحوادث. وتستند الدورة إلى المعيار الدولي ISO/IEC 27001:2022 لأنظمة إدارة أمن المعلومات، بما في ذلك مجموعة ضوابط الملحق Annex A.

المستفيدون من تطبيق نظام إدارة أمن المعلومات وتشغيله

- مالكو النظام الذين يحددون النطاق والأهداف وبيان القابلية للتطبيق
- مديرو أمن المعلومات الذين يختارون ضوابط الملحق ويطبقونها ويراقبونها
- قادة الامتثال الذين ينقلون المتطلبات التعاقدية والقانونية إلى النظام
- المدققون الداخليون الذين يخططون عمليات التدقيق ويرفعون نتائجها
- مديرو خدمات تقنية المعلومات الذين يشغلون الضوابط التشغيلية التي يعتمد عليها النظام

تجني وظيفة الأمن الفائدة الكبرى حين توفد مالك النظام ومالكي الضوابط والمدقق الداخلي معا، إذ يرى كل منهم كيف يغذي جزؤه من الدورة الأجزاء الأخرى.

قدرات تطبيق نظام إدارة أمن المعلومات وتشغيله

يغادر المشاركون قادرين على تحديد نطاق النظام وبنائه وتشغيله بحيث ينتج أدلته بنفسه ويتحسن بين عمليات التدقيق.

- تحديد نطاق النظام وحدوده وواجهاته مع الخدمات المسندة — اعتماد الإدارة العليا
- بناء جرد أصول المعلومات مع التصنيف والملكية — مالكو الأصول وأمناء البيانات
- تقييم تهديدات أمن المعلومات واختيار خيارات المعالجة — مالكو المخاطر ولجنة الأمن
- تصميم بيان قابلية التطبيق الذي يبرر كل قرار بشأن ضوابط Annex A — المدققون وجهات منح الشهادات
- اختبار فاعلية الضوابط عبر المقاييس والتدقيق الداخلي — مراجعة الإدارة
- تطبيق روتين الإجراءات التصحيحية والتحسين المستمر — مالك النظام ومالكو العمليات

مصطلحات تطبيق نظام إدارة أمن المعلومات وتشغيله الأساسية

- نظام إدارة أمن المعلومات — السياسات والعمليات والأدوار والضوابط التي تحمي بها المنشأة سرية معلوماتها وسلامتها وتوافرها.
- بيان قابلية التطبيق — وثيقة تسرد كل ضابط من الملحق وتبين هل طبق مع مبرر إدراجه أو استبعاده.
- معالجة المخاطر — قرار تعديل التهديد أو الاحتفاظ به أو تجنبه أو مشاركته، موثقا مع الضوابط التي تنفذه.
- الملحق Annex A — المجموعة المرجعية لضوابط أمن المعلومات في ISO/IEC 27001:2022 موزعة على محاور تنظيمية وبشرية ومادية وتقنية.
- مراجعة الإدارة — اجتماع مجدول تفحص فيه الإدارة العليا أداء النظام ونتائج التدقيق والتغييرات وتقرر التحسينات والموارد.
- عدم المطابقة — إخفاق في تلبية متطلب من المعيار أو من نظام المنشأة نفسه يستدعي تصحيحا ومعالجة للسبب الجذري.

تطبيق نظام إدارة أمن المعلومات وتشغيله يوما بيوم

اليوم 1: مبررات النظام الحي

- بنية بنود ISO/IEC 27001:2022 — متطلبات نظام الإدارة مقابل الضوابط
- دورة التخطيط والتنفيذ والفحص والتصحيح — إيقاع تشغيل النظام
- خريطة الأطراف المعنية — التوقعات الأمنية الواجب تلبيتها
- تقييم الفجوات مقابل المعيار — حجم الجهد المبدئي وأولوياته
- أدلة دعم القيادة — الأدوار المطلوبة من الإدارة العليا

اليوم 2: النطاق والسياق

- صياغة بيان النطاق — المواقع والخدمات والاستثناءات
- تحليل القضايا الداخلية والخارجية — عوامل تشكل الأهداف الأمنية
- الواجهات مع مزودي السحابة والخدمات المسندة — مسؤوليات الحدود
- إطار سياسات أمن المعلومات — التوجه الأعلى والسياسات الموضوعية
- الأهداف الأمنية ومقاييسها — ما يجب أن يحققه النظام

اليوم 3: أصول المعلومات وتصنيفها

- أساليب جرد الأصول — المعلومات والأنظمة والأفراد والموردون
- تعيين ملكية الأصول — المساءلة عن قرارات الحماية
- تصميم مخطط التصنيف — الوسوم وقواعد التداول
- الاستخدام المقبول وإعادة الأصول — ضوابط انضمام الموظفين ومغادرتهم
- أدوات إدارة الإعدادات والأصول — إبقاء الجرد محدثا

اليوم 4: منهجية تقييم التهديدات

- معايير التقييم ومستويات القبول — نتائج متسقة وقابلة للتكرار
- الأساليب القائمة على الأصول مقابل السيناريوهات — اختيار النهج
- تحديد التهديدات ونقاط الضعف — مدخلات الاحتمالية
- مقاييس الأثر على السرية والسلامة والتوافر — تصنيف العواقب
- توقيع مالك التهديد — المساءلة عن التعرض المتبقي

اليوم 5: المعالجة وبيان قابلية التطبيق

- اختيار خيار المعالجة — التعديل أو الاحتفاظ أو التجنب أو المشاركة
- ربط ضوابط Annex A — وصل كل تهديد بضماناته
- مبررات بيان قابلية التطبيق — إدراج واستبعاد يقبلهما المدققون
- جدولة خطة المعالجة — المسؤولون والموارد والمواعيد
- وثائق قبول التعرض المتبقي — الموافقة الرسمية من المالكين

اليوم 6: الضوابط التنظيمية والبشرية

- الأدوار والفصل بين المهام وجهات الاتصال — وضوح المسؤوليات الأمنية
- اتفاقيات أمن الموردين — البنود التعاقدية والمتابعة
- الفحص المسبق وشروط التوظيف والإجراءات التأديبية — ضوابط دورة حياة الموظف
- سجلات الوعي والكفاءة — أدلة تدريب الموظفين
- إجراء حوادث أمن المعلومات — الإبلاغ والاستجابة والتعلم

اليوم 7: الضوابط المادية والتقنية

- المناطق الآمنة وحماية المعدات — قرارات المحيط المادي
- التحكم في الوصول وإدارة الهويات — مبدأ الحد الأدنى من الصلاحيات في التطبيق
- التسجيل والمراقبة واستخبارات التهديدات — نطاق الكشف
- الإعداد الآمن ومعالجة الثغرات — وتيرة التصحيح والتحصين
- النسخ الاحتياطي والتكرار ومنع تسرب البيانات — ضمانات التوافر ومنع الإفشاء

اليوم 8: التوثيق والأدلة التشغيلية

- ضبط المعلومات الموثقة — الإصدارات والاعتماد والاحتفاظ
- تصميم الإجراءات وتعليمات العمل — إرشاد عملي للمشغلين
- المقاييس الأمنية ولوحات المتابعة — قياس فاعلية الضوابط
- دمج إدارة التغيير — فحوص أمنية في تغييرات التقنية
- حالات تطبيق في الرعاية الصحية والخدمات اللوجستية — دروس قطاعية

اليوم 9: التدقيق الداخلي ومراجعة الإدارة

- تخطيط برنامج التدقيق الداخلي — تغطية البنود والضوابط
- أخذ عينات الأدلة وإجراء المقابلات — اختبار التشغيل لا الورق
- تصنيف حالات عدم المطابقة والإبلاغ عنها — نتائج واضحة للمالكين
- مدخلات مراجعة الإدارة ومخرجاتها — قرارات الموارد والتغيير
- الإجراء التصحيحي وأساليب السبب الجذري — منع التكرار

اليوم 10: ممارسة خطة تطبيق نظام إدارة أمن المعلومات

- تطبيق النطاق والسياق على منشأة حالة — حدود قابلة للدفاع
- تمرين المعالجة وقابلية التطبيق — اختيار الضوابط تحت القيود
- محاكاة التدقيق والرد على النتائج — الجاهزية للتقييم الخارجي
- خارطة التحسين المستمر — الدورة التالية لأول شهادة
- استكمال خطة تطبيق نظام إدارة أمن المعلومات — المراحل والمسؤولون ومحطات الأدلة

تطبيق نظام إدارة أمن المعلومات وتشغيله بعد الدورة

- إجراء تقييم فجوات للنظام الحالي مقابل بنود ISO/IEC 27001:2022 وعرض الفجوات ذات الأولوية على الإدارة العليا
- مراجعة بيان قابلية التطبيق مع مالكي الضوابط وإضافة فحص فاعلية قابل للقياس لكل ضابط مطبق

أسئلة حول تطبيق نظام إدارة أمن المعلومات وتشغيله

ما تطبيق نظام إدارة أمن المعلومات وتشغيله ولماذا يهم الآن؟

تطبيق نظام إدارة أمن المعلومات وتشغيله هو بناء النظام وإدارته بما يلبي متطلبات ISO/IEC 27001:2022. ويهم الآن لأن العملاء والشركاء يطلبون أدلة على ضوابط عاملة لا سياسات فحسب قبل الوثوق بالمنشأة.

من يستفيد أكثر من دورة تطبيق نظام إدارة أمن المعلومات وتشغيله؟

يستفيد أكثر مالكو النظام ومديرو أمن المعلومات وقادة الامتثال والمدققون الداخليون. وتزداد فائدتك إن كنت تملك بيان قابلية التطبيق أو تشغل الضوابط أو تحتاج إلى إثبات عمل النظام بين التقييمات.

كيف تختلف دورة تطبيق نظام إدارة أمن المعلومات وتشغيله عن دورة التعريف بالمعيار ISO/IEC 27001؟

تتجاوز الدورة شرح المتطلبات إلى بناء كل جزء من النظام وتشغيله. فأنت تمارس تحديد النطاق والمعالجة واختيار الضوابط والتدقيق الداخلي ومراجعة الإدارة، وتغادر بخطة لمنشأتك لا بلمحة عامة.

ماذا تعود به من دورة تطبيق نظام إدارة أمن المعلومات وتشغيله؟

تعود بخطة مرحلية لتطبيق نظامك أو تعزيزه. وتحدد النطاق ومنهجية التقييم وأولويات الضوابط وجدول التدقيق ومحطات الأدلة، مع مسؤول مسمى لكل مرحلة.

تطبيق نظام إدارة أمن المعلومات وتشغيله: الطريق إلى الأمام

توجه خطة تطبيق نظام إدارة أمن المعلومات أولا قرار الإدارة العليا بشأن حدود النطاق ومنهجية التقييم. ويقودها مالكو النظام، وينفذ مالكو الضوابط مراحلها، ويبني عليها المدققون الداخليون خطة التغطية. وبعد أول دورة تدقيق داخلي يستحق بيان قابلية التطبيق مراجعة جديدة، إذ تكشف الأدلة ضوابط طبقت على الورق ولم تعمل بعد.