المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Cybersecurity Risk Management Training

فكرة الدورة

أصبحت مخاطر الأمن السيبراني جزءاً أساسياً من منظومة المخاطر المؤسسية، مع توسع الخدمات الرقمية، وتزايد الاعتماد على الأنظمة المتصلة، وارتفاع تأثير الحوادث الأمنية على الاستمرارية والسمعة والامتثال. لذلك تحتاج المؤسسات إلى منهجية واضحة لتحديد المخاطر، وتحليلها، وترتيب أولوياتها، واختيار الضوابط المناسبة لمعالجتها ضمن إطار حوكمة متماسك.

يركز هذا البرنامج التدريبي من AINFCT على تمكين المشاركين من فهم دورة إدارة مخاطر الأمن السيبراني من منظور عملي، يشمل تحديد الأصول، وفهم التهديدات، وتحليل الثغرات، وتقدير الأثر، وبناء سجل المخاطر، وربط المعالجات بالضوابط والسياسات والمتابعة المستمرة. كما يتناول البرنامج العلاقة بين إدارة المخاطر، والامتثال، واستمرارية الأعمال، وسلاسل التوريد الرقمية.

يوفر البرنامج قيمة مهنية واضحة من خلال تحويل مفاهيم المخاطر إلى ممارسات قابلة للتطبيق، تساعد المشاركين على دعم قرارات أمنية أكثر نضجاً داخل مؤسساتهم.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- شرح مفاهيم مخاطر الأمن السيبراني بوضوح مهني.
- تحديد الأصول والتهديدات والثغرات ذات الأولوية.
- تحليل احتمالية المخاطر وأثرها المؤسسي.

- اختيار معالجات وضوابط أمنية مناسبة.
- إعداد سجل مخاطر سيبراني قابل للمتابعة.
- ربط المخاطر بالحوكمة والامتثال والاستمرارية.

منهجية الدورة

- عروض تفاعلية مدعومة بأمثلة واقعية.
- تمارين عملية لبناء سجل مخاطر.
- تحليل حالات وسيناريوهات تهديد مؤسسية.
- مناقشات جماعية حول قرارات المعالجة والقبول.
- مراجعات قصيرة لترسيخ المفاهيم الرئيسية.

أثر الدورة على المنظمة

يمكن تعزيز فاعلية إدارة المخاطر السيبرانية المؤسسية من خلال:

- تحسين رؤية الإدارة للمخاطر السيبرانية الحرجة.
- دعم قرارات أمنية مبنية على الأولويات.
- تقليل فجوات الضوابط والامتثال الأمني.
- تعزيز جاهزية المؤسسة للتعامل مع الحوادث.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- استخدام منهجيات عملية لتقييم المخاطر.
- ترتيب المخاطر وفق الأثر والاحتمالية.
- صياغة معالجات أمنية قابلة للتنفيذ.
- التواصل المهني مع أصحاب المصلحة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المهنيين الذين يشاركون في تقييم المخاطر السيبرانية أو معالجتها أو متابعتها داخل المؤسسة. كما يفيد العاملين الذين يحتاجون إلى ربط الأمن السيبراني بالحوكمة والامتثال واستمرارية الأعمال.

- مختصو الأمن السيبراني وأمن المعلومات.
- مسؤولو المخاطر والحوكمة والامتثال.
- مديرو تقنية المعلومات والبنية التحتية.
- محللو المخاطر والضوابط الأمنية.
- فرق التدقيق الداخلي واستمرارية الأعمال.

موضوعات الدورة

اليوم الأول: مدخل إلى إدارة مخاطر الأمن السيبراني

- مفهوم الخطر السيبراني وعلاقته بالمخاطر المؤسسية.

- الفروق بين التهديدات والثغرات والأثر والاحتمالية.
- دور إدارة المخاطر في حماية القيمة المؤسسية.
- العلاقة بين الحوكمة والضوابط وإدارة المخاطر.
- مبادئ التفكير القائم على المخاطر في الأمن السيبراني.

اليوم الثاني: حوكمة المخاطر والأدوار والمسؤوليات

- بناء نموذج حوكمة واضح للمخاطر السيبرانية.
- مسؤوليات الإدارة العليا ومالكي المخاطر والفرق التقنية.
- تحديد شهية المخاطر وحدود القبول المؤسسي.
- ربط المخاطر السيبرانية بأهداف الأعمال والامتثال.
- آليات التقارير والتصعيد واتخاذ القرار.

اليوم الثالث: تحديد الأصول ونطاق التقييم

- تحديد الأصول المعلوماتية والأنظمة والخدمات الحرجة.
- تصنيف الأصول حسب القيمة والحساسية والاعتمادية.
- تحديد حدود النطاق وأصحاب المصلحة المعنيين.
- فهم الاعتماديات الداخلية والخارجية بين الأصول.
- توثيق الأصول في سياق تقييم المخاطر.

اليوم الرابع: تحليل التهديدات ومصادر المخاطر

- أنواع التهديدات السيبرانية الداخلية والخارجية.
- تحليل الجهات المهددة والدوافع والقدرات.
- مصادر المخاطر التقنية والبشرية والتنظيمية.
- التهديدات المرتبطة بالموردين والخدمات السحابية.
- استخدام سيناريوهات التهديد في بناء التقييم.

اليوم الخامس: تحليل الثغرات ونقاط الضعف

- مفهوم الثغرة وعلاقتها بالضوابط والعمليات.

- مصادر اكتشاف الثغرات الفنية والتنظيمية.
- تحليل ضعف التكوينات والإعدادات والصلاحيات.
- الثغرات الناتجة عن العمليات والسلوك البشري.
- تقييم قابلية الاستغلال ضمن سياق المؤسسة.

اليوم السادس: تقييم الاحتمالية والأثر

- مناهج تقدير احتمالية حدوث المخاطر.
- تحليل الأثر المالي والتشغيلي والسمعي والتنظيمي.
- تحديد مستويات شدة المخاطر وتصنيفها.
- استخدام مصفوفة المخاطر في التقييم العملي.
- تجنب الانحيازات الشائعة في تقدير المخاطر.

اليوم السابع: أساليب تقييم المخاطر السيبرانية

- التقييم النوعي والكمي وشبه الكمي للمخاطر.
- اختيار المنهج المناسب حسب نضج المؤسسة.
- جمع البيانات المطلوبة للتقييم الموثوق.
- تحليل السيناريوهات الأمنية حسب الأولوية.
- توثيق الافتراضات والقيود أثناء التقييم.

اليوم الثامن: بناء سجل المخاطر السيبرانية

- عناصر سجل المخاطر ومكوناته الأساسية.
- صياغة وصف واضح ومحدد للمخاطر.
- تحديد مالك الخطر وخطة المعالجة.
- تحديث حالة المخاطر ومؤشرات المتابعة.
- استخدام السجل في التقارير واتخاذ القرار.

اليوم التاسع: معالجة المخاطر واختيار الضوابط

- خيارات معالجة المخاطر: التخفيف والقبول والنقل والتجنب.

- اختيار الضوابط وفق الأولوية والجدوى.
- الربط بين المخاطر والضوابط الوقائية والكاشفة.
- تقدير المخاطر المتبقية بعد المعالجة.
- توثيق قرارات القبول والاستثناءات الأمنية.

اليوم العاشر: المخاطر والامتثال والسياسات

- العلاقة بين المتطلبات التنظيمية وإدارة المخاطر.
- تحويل الالتزامات إلى ضوابط قابلة للقياس.
- إدارة الاستثناءات والانحرافات عن السياسات.
- استخدام المراجعات الداخلية لدعم إدارة المخاطر.
- تجهيز الأدلة المطلوبة للتدقيق والامتثال.

اليوم الحادي عشر: مؤشرات المخاطر والتقارير

- تصميم مؤشرات المخاطر الرئيسية للأمن السيبراني.
- التمييز بين مؤشرات الأداء ومؤشرات المخاطر.
- بناء تقارير تنفيذية واضحة ومختصرة.
- عرض المخاطر بلغة مناسبة للإدارة العليا.
- تتبع الاتجاهات والتغيرات في مستوى المخاطر.

اليوم الثاني عشر: مخاطر الأطراف الثالثة وسلاسل التوريد

- تحديد مخاطر الموردين والشركاء ومقدمي الخدمات.
- تقييم الضوابط الأمنية لدى الأطراف الخارجية.
- إدارة المخاطر التعاقدية ومتطلبات الخدمة.
- متابعة الامتثال المستمر للموردين الحرجين.
- التعامل مع مخاطر البرمجيات والخدمات السحابية.

اليوم الثالث عشر: المخاطر واستمرارية الأعمال

- ربط المخاطر السيبرانية باستمرارية الأعمال.

- تحليل أثر الأعمال للخدمات والأنظمة الحرجة.
- تحديد أولويات التعافي حسب مستويات المخاطر.
- مخاطر التوقف وفقدان البيانات وتعطل الخدمات.
- اختبار خطط الاستمرارية من منظور سيبراني.

اليوم الرابع عشر: المراقبة المستمرة وتحسين النضج

- مراقبة المخاطر والضوابط بشكل دوري.
- تحديث التقييمات عند تغير البيئة أو التهديدات.
- استخدام نتائج الحوادث في تحسين التقييم.
- قياس نضج إدارة المخاطر السيبرانية.
- بناء خارطة طريق لتحسين الضوابط.

اليوم الخامس عشر: تطبيق عملي وتكامل المنهجية

- تحليل حالة مؤسسية متكاملة لإدارة المخاطر.
- إعداد سجل مخاطر مبسط لمجموعة أصول.
- اختيار معالجات وضوابط حسب الأولوية.
- عرض نتائج التقييم لأصحاب المصلحة.
- مراجعة الدروس المهنية وخطة التطوير اللاحقة.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للموضوع السابق، ثم عرض للمحور الرئيسي، يليه تطبيق عملي أو نقاش موجه، وينتهي اليوم بخلاصة مركزة تربط المفاهيم بممارسات العمل. يوازن الجدول بين الشرح، والتحليل، والتطبيق، والمراجعة، بما يدعم استيعاب المشاركين للمنهجية الكاملة لإدارة مخاطر الأمن السيبراني.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، وتحليل الحالات، ومراجعة مخرجات سجل المخاطر والمعالجات المقترحة. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- إدارة مخاطر الأمن السيبراني.
- تحليل التهديدات والثغرات.
- تقييم الأثر والاحتمالية.
- بناء سجل المخاطر.
- اختيار الضوابط والمعالجات.
- التواصل مع أصحاب المصلحة.

مكتب القاهرة الرئيسي

القاهرة، جمهورية مصر العربية

7 شارع وهران، الطيران، مدينة نصر

+201152466358

info@ainfct.com

ainfct.com

رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي

مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد

training@ainfct.com

ainfct.com