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

Information Security Manager-CISM

فكرة الدورة

تواجه المؤسسات اليوم تحديات متزايدة في إدارة أمن المعلومات نتيجة توسع الاعتماد على الخدمات الرقمية، وتداخل المتطلبات التنظيمية، وارتفاع مستوى التهديدات السيبرانية التي تؤثر في العمليات والسمعة واستمرارية الأعمال. ولم يعد أمن المعلومات وظيفة تقنية منفصلة، بل أصبح مسؤولية إدارية تتطلب مواءمة واضحة بين الاستراتيجية، والمخاطر، والموارد، والضوابط، ومؤشرات الأداء.

يركز هذا البرنامج التدريبي من AINFCT على تأهيل المشاركين لفهم الدور الإداري والقيادي لمدير أمن المعلومات وفق منظور مهني شامل. ويتناول البرنامج حوكمة أمن المعلومات، وإدارة المخاطر، وبناء البرامج الأمنية، وقياس الفاعلية، وإدارة الحوادث، والتواصل مع أصحاب المصلحة، بما يدعم اتخاذ قرارات أمنية متوازنة ومرتبطة بأهداف المؤسسة.

يوفر البرنامج قيمة عملية للمشاركين من خلال ربط مفاهيم CISM بالمسؤوليات اليومية لقادة أمن المعلومات، مع التركيز على التفكير الإداري، وإدارة الأولويات، وتحويل المتطلبات الأمنية إلى برامج قابلة للتنفيذ والقياس.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحليل حوكمة أمن المعلومات ضمن السياق المؤسسي.
- مواءمة الاستراتيجية الأمنية مع أهداف الأعمال.
- إدارة مخاطر أمن المعلومات وفق منهجية واضحة.
- تطوير برامج أمنية قابلة للتنفيذ والقياس.
- تحسين جاهزية إدارة الحوادث الأمنية.
- تعزيز التقارير الأمنية لأصحاب المصلحة.

منهجية الدورة

- عروض تفاعلية تربط مفاهيم CISM بالبيئة المؤسسية.
- تمارين تطبيقية في تقييم المخاطر وإدارة البرامج.
- مناقشات موجهة حول قرارات أمنية تنفيذية.
- حالات عملية لإدارة الحوادث والتقارير الأمنية.
- مراجعات معرفية قصيرة في نهاية المحاور الرئيسية.

أثر الدورة على المنظمة

يمكن رفع نضج إدارة أمن المعلومات المؤسسية من خلال:

- تحسين مواءمة الأمن مع الحوكمة المؤسسية.
- دعم قرارات المخاطر بمؤشرات واضحة.
- تعزيز فعالية البرامج الأمنية والضوابط.
- تقليل أثر الحوادث على استمرارية الأعمال.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم مسؤوليات مدير أمن المعلومات.
- قيادة برامج أمنية مرتبطة بالمخاطر.
- تحليل الحوادث من منظور إداري.
- تقديم تقارير أمنية تنفيذية فعالة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المهنيين الذين يتولون أو يستعدون لتولي مسؤوليات إدارية وقيادية في أمن المعلومات. كما يفيد المشاركين المعنيين بربط الأمن بالمخاطر والحوكمة والأهداف المؤسسية.

- مديرو ومسؤولو أمن المعلومات.
- قادة فرق الأمن السيبراني وتقنية المعلومات.
- مختصو الحوكمة والمخاطر والامتثال.
- مسؤولو البرامج والمشروعات الأمنية.
- المرشحون لتطوير مسار مهني مرتبط بـ CISM.

موضوعات الدورة

اليوم الأول: مدخل إلى دور مدير أمن المعلومات

- تطور وظيفة أمن المعلومات من التقنية إلى الإدارة.
- مسؤوليات مدير أمن المعلومات داخل المؤسسة.
- العلاقة بين الأمن السيبراني وإدارة الأعمال.
- أصحاب المصلحة وتأثيرهم في القرارات الأمنية.
- مبادئ المهنية والحوكمة في قيادة الأمن.

اليوم الثاني: حوكمة أمن المعلومات

- مفهوم الحوكمة الأمنية وأهدافها المؤسسية.
- هياكل الحوكمة واللجان والأدوار والمسؤوليات.
- السياسات والمعايير والإجراءات الأمنية.
- التكامل بين الحوكمة المؤسسية وحوكمة الأمن.
- مؤشرات قياس فاعلية الحوكمة الأمنية.

اليوم الثالث: استراتيجية أمن المعلومات

- بناء استراتيجية أمنية مرتبطة بأهداف المؤسسة.
- تحليل البيئة الداخلية والخارجية للأمن.
- تحديد المبادرات الأمنية ذات الأولوية.
- إعداد خارطة طريق أمنية قابلة للتنفيذ.
- إدارة الميزانية والموارد الداعمة للاستراتيجية.

اليوم الرابع: المتطلبات القانونية والتنظيمية والتعاقدية

- تحديد المتطلبات التنظيمية المؤثرة في أمن المعلومات.
- إدارة الالتزامات التعاقدية مع الأطراف الخارجية.
- ربط الامتثال بإدارة المخاطر والضوابط.

- توثيق السياسات لدعم المساءلة المؤسسية.
- التعامل مع التعارض بين المتطلبات والقدرات التشغيلية.

اليوم الخامس: إدارة مخاطر أمن المعلومات

- المفاهيم الأساسية للمخاطر والتهديدات ونقاط الضعف.
- تحديد الأصول والعمليات الحرجة.
- تحليل الاحتمالية والأثر ومستوى المخاطر.
- تحديد شهية المخاطر وحدود القبول.
- توثيق سجل المخاطر الأمنية وتحديثه.

اليوم السادس: تقييم المخاطر والاستجابة لها

- اختيار منهجيات تقييم المخاطر المناسبة.
- تحليل الضوابط القائمة وفجوات الحماية.
- خيارات معالجة المخاطر وتحديد الأولويات.
- تعيين مالكي المخاطر والضوابط.
- متابعة خطط المعالجة ورفع التقارير.

اليوم السابع: تصميم برنامج أمن المعلومات

- مكونات برنامج أمن المعلومات المؤسسي.
- تحديد نطاق البرنامج وأهدافه ومخرجاته.
- بناء السياسات والضوابط والإجراءات التشغيلية.
- دمج الأمن في العمليات والمشروعات.
- إدارة التغيير داخل البرنامج الأمني.

اليوم الثامن: إدارة الموارد والقدرات الأمنية

- تخطيط الموارد البشرية والتقنية والمالية.
- بناء فرق أمن المعلومات وتوزيع المسؤوليات.
- تطوير المهارات والوعي الأمني داخل المؤسسة.

- إدارة الموردين ومقدمي الخدمات الأمنية.
- متابعة الكفاءة التشغيلية للموارد الأمنية.

اليوم التاسع: إدارة الضوابط وقياس الفاعلية

- اختيار الضوابط الأمنية وفق المخاطر.
- دمج الضوابط داخل العمليات المؤسسية.
- اختبار الضوابط وتقييم مستوى النضج.
- استخدام مؤشرات الأداء والمخاطر الأمنية.
- تحسين الضوابط بناءً على نتائج القياس.

اليوم العاشر: إدارة الطرف الثالث وسلاسل التوريد

- مخاطر الموردين والشركاء ومقدمي الخدمات.
- متطلبات الأمن في العقود واتفاقيات الخدمة.
- تقييم ضوابط الطرف الثالث ومراقبة الأداء.
- إدارة المخاطر المستمرة للعلاقات الخارجية.
- معالجة المخاطر المشتركة في الخدمات السحابية.

اليوم الحادي عشر: إدارة الحوادث الأمنية

- مفهوم الحادث الأمني وأثره المؤسسي.
- بناء سياسة وإجراءات إدارة الحوادث.
- تصنيف الحوادث وتحديد مستويات الخطورة.
- تحديد أدوار الاستجابة والتصعيد.
- إدارة التواصل الداخلي أثناء الحوادث.

اليوم الثاني عشر: الاستجابة والتعافي بعد الحوادث

- مراحل الاستجابة من الاكتشاف إلى التعافي.
- التنسيق بين الفرق التقنية والإدارية والقانونية.
- إدارة القرارات تحت ضغط الحوادث.

- حفظ الأدلة ودعم التحقيقات الداخلية.
- استخلاص الدروس وتحسين الجاهزية.

اليوم الثالث عشر: التقارير الأمنية والتواصل التنفيذي

- تصميم تقارير أمنية مناسبة للإدارة العليا.
- تحويل البيانات الأمنية إلى رسائل تنفيذية.
- عرض المخاطر بلغة الأعمال والتأثير.
- بناء لوحات متابعة للأداء والمخاطر.
- إدارة التوقعات مع أصحاب المصلحة.

اليوم الرابع عشر: التكامل مع الأطر والمعايير المهنية

- استخدام ISO/IEC 27001 في إدارة أمن المعلومات.
- الاستفادة من ISO/IEC 27005 في إدارة المخاطر.
- ربط NIST Cybersecurity Framework بالبرامج الأمنية.
- الاستفادة من COBIT في الحوكمة والرقابة.
- اختيار الأطر المناسبة حسب نضج المؤسسة.

اليوم الخامس عشر: مراجعة تطبيقية وتكامل المجالات

- ربط الحوكمة والمخاطر والبرنامج والحوادث.
- تحليل حالات إدارية متعددة في أمن المعلومات.
- مراجعة أهم المفاهيم المرتبطة بـ CISM.
- بناء خطة تطوير مهني بعد البرنامج.
- مناقشة أفضل الممارسات القيادية في أمن المعلومات.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة مركزة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه نقاش تطبيقي أو تمرين مهني، وينتهي اليوم بخلاصة تربط المفاهيم بمسؤوليات مدير أمن المعلومات داخل المؤسسة. يوازن الجدول بين الشرح، والتحليل، والنقاش، والتطبيق، والمراجعة المعرفية.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، وتحليل الحالات، والمراجعات القصيرة المرتبطة بمحاور البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- حوكمة أمن المعلومات.
- إدارة المخاطر الأمنية.
- قيادة البرامج الأمنية.
- قياس الأداء الأمني.
- إدارة الحوادث الأمنية.
- التواصل التنفيذي الأمني.

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