

# € TRAINING

إدارة المخاطر في أمن المعلومات

23 فبراير - 6 مارس 2025  
شرم الشيخ (مصر)



## إدارة المخاطر في أمن المعلومات

رمز الدورة: I1067 تاريخ الإنعقاد: 23 فبراير - 6 مارس 2025 دولة الإنعقاد: شرم الشيخ (مصر) - التكلفة: 6965 يورو

### مقدمة عن البرنامج التدريبي:

تم تصميم البرنامج إدارة المخاطر في أمن المعلومات لتزويد المشاركين بالمعرفة والمهارات اللازمة لتحديد وتقييم وتخفيف المخاطر في بيئات أمن المعلومات. في مشهد التهديدات سريع التطور اليوم ، يعد فهم إدارة المخاطر أمرًا بالغ الأهمية للمؤسسات لحماية بياناتها الحساسة وأنظمتها الحساسة بشكل فعال.

### أهداف البرنامج التدريبي:

في نهاية هذه البرنامج سيكون المشاركون قادرين على:

- فهم المفاهيم الأساسية لإدارة المخاطر في سياق أمن المعلومات.
- تحديد التهديدات ونقاط الضعف المحتملة في أنظمة المعلومات.
- تطبيق منهجيات تقييم المخاطر لتحديد أولويات التدابير الأمنية.
- تنفيذ استراتيجيات وضوابط التخفيف من المخاطر.
- تطوير إطار عمل لإدارة المخاطر مصمم خصيصًا لتلبية الاحتياجات المحددة للمؤسسة

### الفئات المستهدفة:

- متخصصو أمن المعلومات الذين يسعون إلى تعزيز مهاراتهم في إدارة المخاطر.
- مدراء تكنولوجيا المعلومات وصناع القرار المسؤولين عن الإشراف على استراتيجيات أمن المعلومات.
- مسؤولو النظام الذين يهتمون بفهم ومعالجة مخاطر الأمان.
- موظفو الامتثال الذين يهدفون إلى ضمان تلبية المتطلبات التنظيمية.

### محاور البرنامج التدريبي:

#### الوحدة الاولى:

#### مقدمة في إدارة المخاطر

- تعريف إدارة المخاطر وأهميتها في أمن المعلومات
- فهم مكونات إدارة المخاطر: التحديد ، التقييم ، التخفيف ، المراقبة
- استكشاف دورة حياة إدارة المخاطر

#### الوحدة الثانية:

#### التهديدات ونقاط الضعف

- البرامج الضارة وبرامج الفدية
- هجمات التصيد الاحتيالي والهندسة الاجتماعية
- التهديدات الداخلية
- هجمات رفض الخدمة DoS
- التهديدات المستمرة المتقدمة APTs

#### التعرف على نقاط الضعف في نظم المعلومات:

- ثغرات البرامج
- تكوينات خاطئة
- آليات المصادقة الضعيفة
- نقاط ضعف الأمن المادي

## الوحدة الثالثة:

### منهجيات تقييم المخاطر

- تعريف المخاطر
- تحليل المخاطر
- تقييم الخطر

## الوحدة الرابعة:

### تحديد وتصنيف المخاطر

- جلسات العصف الذهني
- تحليل SWOT نقاط القوة والضعف والفرص والتهديدات
- تقييم الأصول وتحديد الأولويات

## إنشاء سجل للمخاطر:

- توثيق المخاطر المحددة
- تحديد الملكية والمسئولية

## الوحدة الخامسة:

### تحليل تأثير واحتمالية المخاطر المحددة:

- التحليل النوعي للمخاطر
- التحليل الكمي للمخاطر

## تحديد أولويات المخاطر على أساس الخطورة والحرارة:

- تصنيف وترتيب المخاطر

## الوحدة السادسة:

### فهم خيارات الاستجابة للمخاطر:

- تجنب المخاطر
- نقل المخاطر
- تخفيف المخاطر
- قبول المخاطر

## تنفيذ ضوابط الأمان لتقليل المخاطر:

- ضوابط الوصول
- التشفير

- تدريب توعية الحراس
- تخطيط استمرارية الأعمال

## الوحدة السابعة:

### بناء إطار إدارة مخاطر مصمم خصيصًا للمؤسسة:

- وضع سياسات إدارة المخاطر
- تحديد الأدوار والمسؤوليات

### دمج إدارة المخاطر في سياسات الأمن الحالية:

- التوافق مع معايير أمن المعلومات ISO 27001 ، NIST ، إلخ.

## الوحدة الثامنة:

### إبلاغ المخاطر بشكل فعال لأصحاب المصلحة:

- تطوير استراتيجيات التواصل بشأن المخاطر
- تقديم معلومات المخاطر إلى الجماهير غير الفنية

### إعداد تقارير المخاطر للإدارة وصنع القرار:

- ملخص تنفيذي للمخاطر
- نتائج وتوصيات تقييم المخاطر

## الوحدة التاسعة:

### إنشاء عملية مراقبة ومراجعة المخاطر:

- تقنيات المراقبة المستمرة
- مؤشرات المخاطر الرئيسية KRIS

### تحديث استراتيجيات إدارة المخاطر حسب الحاجة:

- الاستجابة للتهديدات والحوادث الناشئة

## الوحدة العاشرة:

### تحليل سيناريوهات العالم الحقيقي لتطبيق مفاهيم إدارة المخاطر:

- سيناريوهات الاستجابة للحوادث
- تحليل أثر الأعمال التجارية

### تمارين عملية لتعزيز التعلم والمهارات:

- إجراء تقييم المخاطر لبيئة محاكاة
- تطوير خطة إدارة المخاطر لمنظمة وهمية