€TRAINING

إدارة المخاطر في أمن المعلومات

إدارة المخاطر في أمن المعلومات

مقدمة البرنامج التدريبي:

يهدف هذا البرنامج إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لإدارة مخاطر أمن المعلومات بفعالية داخل المؤسسات. يغطي البرنامج المبادئ الأساسية، والاستراتيجيات العملية، والتقنيات المتقدمة اللازمة لحماية الأصول الرقمية وضمان استمرارية الأعمال.

أهداف البرنامج التدريبي:

في نهاية هذا البرنامج سيكون المشاركون قادرين على:

- فهم أساسيات إدارة المخاطر في مجال أمن المعلومات.
- تحديد وتقييم المخاطر باستخدام منهجيات متبعة على مستوى الصناعة.
- تطوير وتنفيذ استراتيجيات للحد من التهديدات المحتملة.
- إعداد خطط استجابة للحوادث وخطط استمرارية الأعمال للحد من التوقفات.
- الامتثال للمتطلبات القانونية والتنظيمية المتعلقة بأمن المعلومات.

الفئات المستهدفة:

- مدراء وضباط أمن المعلومات.
- مدراء ومحللو المخاطر.
- محترفو أمن المعلومات.
- مدققو نظم المعلومات وضباط الامتثال.
- مسؤولو النظام ومهندسو الشبكات.

محاور البرنامج التدريبي:

الوحدة الأولى:

مقدمة في إدارة مخاطر أمن المعلومات:

- التعرف على أساسيات إدارة المخاطر في مجال أمن المعلومات.
- استعراض دور التقييمات والمخططات الأمنية.
- تحديد أصحاب المصلحة في عملية إدارة المخاطر.
- نظرة عامة على أطر ومعايير إدارة المخاطر.

الوحدة الثانية:

تحديد وتقييم المخاطر:

- تقنيات تحديد مخاطر أمن المعلومات.
- إجراء التقييمات الأمنية وتقييم نقاط الضعف.
- ترتيب المخاطر حسب الأولوية بناءً على احتمالية التأثير.
- استخدام أدوات ومنهجيات تقييم المخاطر.
- توثيق النتائج والتوصيات المتعلقة بالمخاطر.

الوحدة الثالثة:

استراتيجيات معالجة المخاطر:

- استراتيجيات للتخفيف من المخاطر أو قبولها.
- تنفيذ الضوابط لتقليل المخاطر المكتشفة.
- تطوير خطط لمعالجة المخاطر.
- دمج إدارة المخاطر في العمليات التجارية.

الوحدة الرابعة:

إدارة الحوادث واستمرارية الأعمال:

- إعداد خطط الاستجابة للحوادث والإجراءات اللازمة.
- إنشاء قنوات الاتصال أثناء الحوادث.
- اختبار وتحديث خطط الاستجابة للحوادث.
- ضمان استمرارية الأعمال عند وقوع الحوادث الأمنية.

الوحدة الخامسة:

الجوانب القانونية والتنظيمية لأمن المعلومات:

- فهم الأطر القانونية المتعلقة بأمن المعلومات.
- متطلبات الامتثال وتأثيرها على إدارة المخاطر.
- دور العقود والتأمين في تخفيف المخاطر.
- التعامل مع قوانين حماية البيانات والخصوصية الدولية.

الوحدة السادسة:

الضوابط الأمنية والتقنيات:

- تنفيذ الضوابط التقنية الأمنية التشفير والتحكم في الوصول.
- نشر تقنيات للكشف عن التهديدات ومنعها.
- دمج الضوابط الأمنية في البنية التحتية للنظام والشبكة.
- تقييم التقنيات الناشئة لأمن المعلومات.
- دراسات حالة حول التنفيذ الناجح للضوابط الأمنية.

الوحدة السابعة:

التواصل والإبلاغ عن المخاطر:

- أهمية التواصل الفعّال مع أصحاب المصلحة بشأن المخاطر.
- إعداد تقارير المخاطر ولوحات المعلومات Dashboard لصنع القرار.
- تقديم تقييمات المخاطر والتوصيات بشكل فعّال.
- مواجهة تحديات التواصل في إدارة المخاطر.
- أهمية تدريب الموظفين على الوعي بالمخاطر.

الوحدة الثامنة:

الاعتبارات الأخلاقية والاجتماعية في إدارة المخاطر:

- الاعتبارات الأخلاقية في إدارة مخاطر أمن المعلومات.
- التوازن بين التدابير الأمنية وخصوصية المستخدمين.

- الهندسة الاجتماعية والعوامل البشرية في أمن المعلومات.
- بناء ثقافة تنظيمية واعية بأمن المعلومات.

الوحدة التاسعة:

التهديدات الناشئة واتجاهات أمن المعلومات:

- التعرف على التهديدات الحالية والناشئة لأمن المعلومات.
- مراقبة الاتجاهات في التهديدات الإلكترونية ووسائل الهجوم.
- تكيف استراتيجيات إدارة المخاطر مع التهديدات المتطورة.
- الاستفادة من معلومات التهديدات لإدارة المخاطر بشكل استباقي.
- استراتيجيات التعامل مع التهديدات الداخلية والهندسة الاجتماعية.

الوحدة العاشرة:

التحسين المستمر ومستقبل إدارة المخاطر:

- تقييم فعالية برامج إدارة المخاطر.
- تنفيذ حلقات التغذية الراجعة والدروس المستفادة.
- التخطيط للتحديات المستقبلية والتقدم في أمن المعلومات.
- المسارات المهنية والتطور المهني في إدارة المخاطر.
- الاتجاهات التي تشكل مستقبل إدارة مخاطر أمن المعلومات.