€TRAINING

التدقيق في مجال تكنولوجيا المعلومات

التدقيق في مجال تكنولوجيا المعلومات

مقدمة عن البرنامج التدريبي:

يُعتبر التدقيق في مجال تكنولوجيا المعلومات أمرًا حيويًا لأي منظمة تعتمد على التكنولوجيا في عملياتها. يهدف هذا البرنامج التدريبي إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتقديم تقييم شامل لنظام المعلومات في منظمتهم وتحديد الفجوات والمخاطر المحتملة وتوصيات لتحسين الأداء العام.

اهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرون على:

- معرفة المهارات اللازمة لتنفيذ عمليات التدقيق في مجال تكنولوجيا المعلومات بفعالية.
- تقييم أمان وكفاءة الأنظمة والتقنيات المستخدمة في المؤسسة.
- تحديد المخاطر والفجوات الأمنية والمحاسبية.
- تعزيز الأمان والموثوقية والامتثال في بيئة تكنولوجيا المعلومات.

الفئات المستهدفة:

- مدققو تكنولوجيا المعلومات الداخليون والخارجيون.
- مسؤولو أمان المعلومات والحماية.
- مديرو تكنولوجيا المعلومات ومسؤولو اتخاذ القرار.
- محللو أمان المعلومات وخبراء أمان الشبكات.
- مسؤولو الامتثال والتشريعات القانونية المتعلقة بتكنولوجيا المعلومات.

محاور البرنامج التدريبي:

الوحدة الأولى:

مقدمة في تكنولوجيا المعلومات وأساسيات التدقيق الداخلي والخارجي:

- مفهوم تكنولوجيا المعلومات وأهميتها في المؤسسات.
- دور التدقيق الداخلي والخارجي في ضمان الامتثال والأمان.
- إطار عمل تدقيق تكنولوجيا المعلومات وأفضل الممارسات.
- استعراض الأنظمة الأساسية المستخدمة في التدقيق الداخلي والخارجي.
- التحديات والصعوبات التي تواجه التدقيق في بيئة تكنولوجيا المعلومات.

الوحدة الثانية:

تقييم الأمان والمخاطر في تكنولوجيا المعلومات:

- تحديد وتقييم المخاطر الأمنية والتحديات المتعلقة بأمان المعلومات.
- تحليل الثغرات الأمنية المحتملة والتعرف على الهجمات الشائعة.
- تقييم الجاهزية للاستجابة للطوارئ واختبار أنظمة الحماية.
- استراتيجيات تعزيز الأمن السيبراني والوقاية من التهديدات الرقمية.
- أهمية التدريب المستمر والتوعية الأمنية للموظفين.

الوحدة الثالثة:

التدقيق المحاسبي والتحقق من التزام الامتثال:

- فحص العمليات المحاسبية والمالية المرتبطة بتكنولوجيا المعلومات.
- التحقق من الامتثال للمعايير والتشريعات القانونية المتعلقة بالمعلوماتية وحماية البيانات.
- تقييم العمليات الداخلية للحد من المخاطر المالية والتحايل.
- أساليب استخدام أدوات التدقيق المتقدمة لتحليل ومراجعة البيانات المالية.
- تعزيز الشفافية والمساءلة في التقارير المالية.

الوحدة الرابعة:

تحقيق أمان تكنولوجيا المعلومات وأفضل الممارسات:

- تحديد السياسات والإجراءات الأمنية الفعالة وتطبيقها.
- حماية الأصول الرقمية والتصدي للتهديدات الأمنية.
- تأمين الشبكات والاتصالات وحماية البيانات الحساسة.
- مراجعة وتحديث الأنظمة الأمنية لتلبية المتطلبات الجديدة.
- تطبيق معايير الأمان العالمية لضمان الحماية الكاملة.

الوحدة الخامسة:

التقارير والتوصيات وجلسات المراجعة:

- إعداد التقارير التفصيلية عن نتائج التدقيق والاستنتاجات المستخلصة.
- تقديم التوصيات الملائمة لتحسين أمان تكنولوجيا المعلومات.
- أهمية عقد جلسات مراجعة ونقاش للتأكد من فهم الجميع للنتائج والتحسينات المقترحة.
- استخدام التغذية الراجعة من الجلسات لتحسين العمليات الأمنية المستقبلية.
- تطوير خطط العمل الاستراتيجية بناءً على التوصيات ونتائج التقارير.