المقدمة:

في ظل التحول الرقمي السريع والاعتماد المتزايد على البيانات في مختلف القطاعات، أصبحت قضايا أمن المعلومات وإدارة المخاطر تحديًا جوهريًا يواجه المؤسسات على اختلاف أنواعها. لم تعد حماية البيانات مجرد خيار، بل ضرورة حتمية لضمان استمرارية الأعمال، وحماية السمعة المؤسسية، والامتثال للتشريعات والتنظيمات ذات الصلة.

تهدف دورة "أمن ضوابط نظم المخاطر والمعلومات" إلى تزويد المشاركين بفهم معمق وشامل لكيفية تصميم وتطبيق ضوابط فعالة لأمن المعلومات، بالإضافة إلى تطوير المهارات اللازمة لإدارة المخاطر المتعلقة بالأنظمة والمعلومات بشكل احترافي. تركز الدورة على الدمج المتوازن بين الجوانب التقنية والإدارية، بما يعزز من قدرة المؤسسات على حماية أصولها المعلوماتية من التهديدات المحتملة، وضمان الاستدامة والمرونة التشغيلية.

الفئات المستهدفة:

- مدراء تكنولوجيا المعلومات (CIOs)
- مدراء أمن المعلومات (CISOs)
- محللو وإخصائيو نظم وإدارة المخاطر
- مستشارو أمن المعلومات
- مدراء المشاريع التقنية
- أعضاء فرق الاستجابة للحوادث السيبرانية
- كل من يعمل في مجال حوكمة تقنية المعلومات وأمنها

الأهداف التدريبية:

عند الانتهاء من هذه الدورة، سيكون المشاركون قد اكتسبوا قدرات متقدمة تشمل:

- فهم متكامل للمفاهيم الأساسية والمتقدمة في أمن المعلومات وإدارة المخاطر.
- تصميم وتطبيق ضوابط أمنية تقنية وإدارية فعالة لحماية البيانات والأنظمة الحساسة.
- إجراء تقييم دقيق للمخاطر وتحديد الإجراءات المناسبة للحد منها.
- تطوير آليات فعالة للاستجابة للحوادث الأمنية وضمان استمرارية الأعمال.

- الإلمام بالقوانين واللوائح الدولية والمحلية ذات الصلة بأمن المعلومات، والعمل على تحقيق الامتثال لها.

الكفاءات المستهدفة:

- القدرة على تحليل وتقييم مخاطر المعلومات والتقنيات المرتبطة بها.
- تطوير ضوابط أمنية ملائمة ومبنية على أساس تقييم المخاطر.
- اكتساب الخبرة في تطبيق أدوات وأساليب تقييم أمان المعلومات.
- القدرة على إدارة الحوادث الأمنية والاستجابة الفورية لها.
- الإلمام بالتشريعات والمعايير المعتمدة في مجال أمن المعلومات، مثل ISO 27001 وNIST.

محتوى الدورة:

الوحدة الأولى: مبادئ وأساسيات أمن المعلومات وإدارة المخاطر

- تعريف شامل بأمن المعلومات وأهدافه الأساسية.
- نظرة عامة على مفهوم إدارة المخاطر ودورها في الحوكمة المؤسسية.
- تصنيف المعلومات وفقًا لدرجة حساسيتها وأنواع البيانات الواجب حمايتها.
- استعراض الأطر الدولية لأمن المعلومات مثل: ISO 27001، NIST، COBIT.
- تحليل التهديدات ونقاط الضعف وتأثيراتها المحتملة على البيئة الرقمية.

الوحدة الثانية: تصميم وتنفيذ الضوابط الأمنية

- توضيح أنواع الضوابط الأمنية: الوقائية، الكاشفة، والتصحيحية.
- خطوات منهجية لتصميم ضوابط أمنية فعالة تناسب طبيعة المخاطر المحتملة.
- استخدام الأدوات التقنية الحديثة لتطبيق الضوابط ومراقبة فعاليتها.
- عرض دراسات حالة وأمثلة تطبيقية من واقع العمل في تصميم الضوابط.
- آليات مراجعة وتحديث الضوابط الأمنية بشكل دوري لضمان فعاليتها المستمرة.

الوحدة الثالثة: تقييم وتحليل المخاطر

- شرح مفصل لأنواع تقييم المخاطر: الكمي والنوعي.
- تقديم نماذج وأدوات فعالة في تحليل المخاطر مثل: HACCP، FMEA، SWOT.
- كيفية إجراء تقييم شامل لتحديد مستوى المخاطر وقابليتها للحدوث.
- بناء وتطوير خطط للتقليل من المخاطر وتفادي تأثيراتها.
- وضع آليات للرصد الدوري ومراجعة فعالية أنشطة إدارة المخاطر.

الوحدة الرابعة: الاستجابة للحوادث الأمنية

- إعداد خطة شاملة للاستجابة للحوادث السيبرانية مع تحديد السيناريوهات المحتملة.
- تكوين فرق الاستجابة وتوزيع الأدوار والمسؤوليات بوضوح.
- تطبيق آليات فعالة لرصد الحوادث، التبليغ عنها، والتحقيق في أسبابها.
- استراتيجيات فورية لمعالجة آثار الحوادث واستعادة الأنظمة.
- توثيق الحوادث وتحليلها لاستخلاص الدروس المستفادة وتفادي تكرارها.

الوحدة الخامسة: الامتثال والمعايير القانونية

- مقدمة شاملة حول الامتثال القانوني في مجال أمن المعلومات.
- مراجعة لأبرز القوانين المحلية والدولية مثل: GDPR، HIPAA، والأنظمة الخليجية.
- خطوات تنفيذية لمراقبة الالتزام وتدقيق الإجراءات المؤسسية.
- مناقشة الأثر القانوني لخرق البيانات أو الإخلال بالإجراءات الأمنية.
- تطوير سياسات مراجعة مستمرة لضمان الامتثال للتشريعات المحدثة.