إدارة مخاطر تكنولوجيا المعلومات وحوكمة المؤسسات

ITM007

وصف البرنامج

برنامج «إدارة مخاطر تكنولوجيا المعلومات وحوكمة المؤسسات» هو برنامج تدريبي شامل يهدف إلى توفير المعرفة والمهارات الضرورية لفهم وتطبيق إدارة مخاطر تكنولوجيا المعلومات وتعزيز حوكمة المؤسسات بشكل فعال. يتناول البرنامج مجموعة واسعة من المحاور المتعلقة بالمفاهيم الأساسية والأدوات العملية التي يحتاجها المشاركون لتحقيق أهدافهم في مجال التكنولوجيا والأمان.

يهدف البرنامج إلى تحقيق عدة أهداف رئيسية، منها فهم مفاهيم إدارة المخاطر التكنولوجية وتقييمها، وتطوير المهارات العملية لتطبيق استراتيجيات الإدارة الفعالة. كما يسعى البرنامج إلى تعزيز الوعي الأمني والامتثال للتشريعات واللوائح ذات الصلة، وتحسين التواصل والتعاون بين المشاركين.

يتضمن برنامج الدورة محاوراً تشمل فهم المخاطر التكنولوجية وتصنيفها، وإطار عمل إدارة المخاطر مثل ISO 27001، وتقييم المخاطر وتحليل الثغرات، بالإضافة إلى تطوير استراتيجيات مخاطر مخصصة وتطبيق ممارسات حوكمة تكنولوجيا المعلومات. يختتم البرنامج بمحورين يركزان على مراقبة وتقييم الأداء وتعزيز الثقافة الأمنية.

تستهدف الفئات المشاركة في البرنامج مديري تكنولوجيا المعلومات ومسؤولي الأمن، ومديري المشاريع التكنولوجية، ومسؤولي الأمن السيبراني، بالإضافة إلى مسؤولي الامتثال والتنظيم والمدراء التنفيذيين والموظفين الفنيين والمختصين في تكنولوجيا المعلومات.

بشكل عام، يقدم برنامج «إدارة مخاطر تكنولوجيا المعلومات وحوكمة المؤسسات» فرصة فريدة لتحسين المهارات اللازمة لإدارة المخاطر وتحقيق حوكمة فعّالة في بيئة التكنولوجيا، مما يساهم في تحقيق الأهداف الأمنية والاستقرارية للمؤسسات.

الأهداف التفصيلية

في نهاية هذه الدورة سيكون المشارك قادرا على:

- فهم مفاهيم إدارة مخاطر تكنولوجيا المعلومات: يتعلم المشاركون المفاهيم الأساسية لإدارة مخاطر تكنولوجيا المعلومات، بما في ذلك تحليل وتقييم المخاطر وتطبيق أدوات وتقنيات الإدارة الفعالة.
- تطوير المهارات العملية: يوفر البرنامج تدريباً عملياً لتطوير مهارات إدارة المخاطر وتطبيقها على سيناريوهات واقعية.
- فهم أفضل لحوكمة المؤسسات: يساعد البرنامج في فهم أفضل لمفهوم حوكمة المؤسسات وكيفية تطبيقها في سياق تكنولوجيا المعلومات.
- تطوير إستراتيجيات الحوكمة وإدارة المخاطر: يهدف البرنامج إلى تمكين المشاركين من تطوير استراتيجيات فعّالة لإدارة المخاطر وتعزيز الحوكمة في منظماتهم.
- تعزيز الامتثال والتنظيم: يساعد البرنامج في توجيه المشاركين حول كيفية الامتثال للتشريعات واللوائح ذات الصلة في مجال تكنولوجيا المعلومات وكيفية تنفيذ أفضل الممارسات.
- تعزيز الوعي الأمني: يعزز البرنامج الوعي بأهمية الأمن في تكنولوجيا المعلومات ويوفر نظرة عامة على التهديدات الأمنية وكيفية التعامل معها بشكل فعال.
- تحقيق هذه الأهداف يساعد في بناء قدرات فعّالة في إدارة مخاطر تكنولوجيا المعلومات وتعزيز حوكمة المؤسسات، وبالتالي يسهم في تحقيق أهداف الأمان والاستقرار والامتثال للمؤسسة.

المستفيدون من البرنامج

- مديري تكنولوجيا المعلومات ومسؤولي الأمن: الذين يتولون مسؤولية تطبيق وتنفيذ إستراتيجيات إدارة المخاطر وحوكمة المؤسسات في البنية التحتية التكنولوجية للمؤسسة.
- مديري المشاريع التكنولوجية: الذين يعملون على تطوير وتنفيذ مشاريع تكنولوجيا المعلومات ويحتاجون إلى فهم عميق للمخاطر المرتبطة بهذه المشاريع وكيفية إدارتها بشكل فعال.
- مسؤولي الأمن السيبراني: الذين يعملون على حماية البنية التحتية التكنولوجية والمعلومات من التهديدات السيبرانية ويحتاجون إلى تحديث مهاراتهم ومعرفتهم بأحدث الاتجاهات والتقنيات.
- مسؤولي الامتثال والتنظيم: الذين يعملون على ضمان أن تلتزم المؤسسة بالقوانين واللوائح المتعلقة بتكنولوجيا المعلومات والحفاظ على معايير الأمان والخصوصية.
- المدراء التنفيذيين ومسؤولي صنع القرار: الذين يحتاجون إلى فهم استراتيجي للمخاطر التكنولوجية وحوكمة المؤسسات لاتخاذ القرارات الصحيحة فيما يتعلق بالاستثمارات التكنولوجية والسياسات الأمنية.
- الموظفين الفنيين والمختصين في تكنولوجيا المعلومات: الذين يحتاجون إلى تطوير مهاراتهم في مجال إدارة المخاطر وحوكمة المؤسسات لتطبيقها في أعمالهم اليومية.

مدة البرنامج

٥ أيام عمل

الخطوط العريضة

١. فهم المخاطر التكنولوجية
   - مقدمة في مفهوم إدارة مخاطر تكنولوجيا المعلومات.
   - تحليل أنواع المخاطر التكنولوجية وتصنيفها.
   - تحليل تأثير المخاطر على أهداف المؤسسة وأنشطتها.

٢. إطار عمل إدارة المخاطر
   - مراجعة الإطار القياسي لإدارة المخاطر مثل ISO 27001.
   - تطبيق نماذج إدارة المخاطر مثل COSO ERM أو NIST Cybersecurity Framework.
   - تعزيز الوعي بأهمية التوافق مع التشريعات واللوائح المتعلقة بالأمن والخصوصية.

٣. تقييم المخاطر وتحليل الثغرات
   - تطبيق تقنيات تقييم المخاطر مثل تحليل الثغرات وتقييم الأثر.
   - تحليل الثغرات الأمنية والضعف في البنية التحتية التكنولوجية والعمليات.

٤. تطوير استراتيجيات مخاطر مخصصة
   - وضع استراتيجيات لتقليل المخاطر وتحسين الأمن التكنولوجي.
   - تصميم وتنفيذ آليات للكشف عن الانتهاكات والاستجابة لها.
   - تحسين ممارسات إدارة الهوية والوصول والحماية من البرمجيات الخبيثة والهجمات السيبرانية.

٥. حوكمة المؤسسات من منظور تكنولوجيا المعلومات

- فهم مفهوم حوكمة تكنولوجيا المعلومات وعلاقتها بإدارة المخاطر.
- وضع إطار للحوكمة يدعم تحقيق أهداف المؤسسة ويحافظ على التوافق والأمان.
- تطبيق ممارسات حوكمة تكنولوجيا المعلومات مثل ITIL.

٦. مراقبة وتقييم الأداء

- تطبيق أدوات مراقبة الأمن التكنولوجي لرصد الأنشطة والتهديدات.
- تقييم فعالية استراتيجيات إدارة المخاطر وحوكمة تكنولوجيا المعلومات.
- تحليل البيانات لتحديد المجالات التي تحتاج إلى تحسين وتطوير.

٧. التوعية وتعزيز الثقافة الأمنية

- تعزيز الوعي بأهمية الأمن التكنولوجي وإدراك المخاطر المحتملة.
- تنظيم جلسات تدريبية وورش عمل للموظفين حول ممارسات الأمان وسلامة المعلومات.
- تطوير برامج تحفيزية لتشجيع المشاركة الفعّالة في جهود الأمان التكنولوجي.