

رقم الدورة 1921

دورة تقييم المخاطر السييرانية للمتخصصين في قطاع التأمين

التأمين السيبراني
التأمين وإدارة المخاطر

طريقة التقديم

حضور

المدة

5 أيام



نظرة عامة على الدورة

تقدم دورة تقييم المخاطر السيرية للمتخصصين في قطاع التأمين إطاراً عملياً واستراتيجياً متكاملًا لتحديد المخاطر السيرية وتقييمها وتحليلها وإدارتها داخل شركات التأمين. وتركز الدورة على فهم تأثير التهديدات السيرية في العمليات التأمينية وبيانات العملاء والاختتاب والمطالبات والخدمات الرقمية والعلاقات مع الأطراف الخارجية واستمرارية الأعمال والمرونة المؤسسية.

يتعرف المشاركون على مشهد المخاطر السيرية في قطاع التأمين، بما يشمل التهديدات والثغرات ونقاط الضعف والسيناريوهات المحتملة للهجمات والتعرض للبيانات والاعتماد على التقنيات الحديثة وتعطل العمليات والمخاطر المرتبطة بالأطراف الخارجية والمخاطر الرقمية الناشئة. وتركز الدورة على تقييم المخاطر من منظور الأعمال والمخاطر المؤسسية دون الحاجة إلى التخصص التقني المتعمق في الأمن السيرياني.

كما تتناول الدورة منهجيات تقييم المخاطر السيرية، وتحديد المخاطر وتصنيفها، وتقييم احتمالية الحدوث والأثر، وبناء سيناريوهات المخاطر، وتقييم فعالية الضوابط، وتحديد المخاطر المتبقية، وربطها بشهية المخاطر واستراتيجيات المعالجة. ويتعلم المشاركون كيفية تحويل النتائج التقنية إلى معلومات واضحة مرتبطة بالأعمال لدعم الإدارة وصناع القرار وتخصيص الموارد.

وتركز الدورة كذلك على آثار المخاطر السيرية على التأمين، وحماية البيانات والخصوصية، والاستجابة للحوادث، واستمرارية الأعمال، ومخاطر الأطراف الخارجية، والمرونة السيرية، والحوكمة. ومن خلال التمارين العملية ودراسات الحالة وورش تقييم المخاطر وتحليل السيناريوهات، يطور المشاركون منهجية متكاملة لتقييم وإدارة المخاطر السيرية في بيئة التأمين.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل مشهد المخاطر السيرية المؤثرة في شركات التأمين.
- تحديد التهديدات والثغرات والأصول والاعتماديات التشغيلية المرتبطة بالمخاطر السيرية.

- تقييم المخاطر السيبرانية عبر العمليات والخدمات والمنصات الرقمية في قطاع التأمين.
- تطبيق منهجيات منظمة لتحديد المخاطر السيبرانية وتقييمها.
- تحليل احتمالية المخاطر السيبرانية وتأثيراتها والتعرض لها ونتائجها المحتملة على الأعمال.
- تطوير سيناريوهات مخاطر سيبرانية مرتبطة بطبيعة أعمال شركات التأمين.
- تقييم فعالية الضوابط الأمنية وتحديد الفجوات ونقاط الضعف.
- تحديد وتفسير مستوى المخاطر المتأصلة والمخاطر المتبقية.
- تطوير معايير لتصنيف المخاطر السيبرانية وترتيب أولوياتها.
- موازنة تقييم المخاطر السيبرانية مع شهية المخاطر وأطر الحوكمة المؤسسية.
- تقييم المخاطر السيبرانية المرتبطة بالأطراف الخارجية ومقدمي الخدمات التقنية.
- تحليل المخاطر المتعلقة ببيانات العملاء والخدمات التأمينية الرقمية.
- تطوير استراتيجيات مناسبة لمعالجة المخاطر السيبرانية والحد منها.
- دمج معلومات المخاطر السيبرانية في إدارة المخاطر المؤسسية واتخاذ القرارات.
- إعداد إطار عملي متكامل لتقييم المخاطر السيبرانية في شركة التأمين.

الفئة المستهدفة

تستهدف الدورة القيادات التنفيذية والمديرين والمتخصصين في إدارة المخاطر ومسؤولي الالتزام والحوكمة وصناع القرار المسؤولين عن المخاطر التشغيلية والتقنية والمعلوماتية والمخاطر الناشئة. وتناسب بشكل خاص العاملين في إدارة المخاطر المؤسسية، والأمن السيبراني، وأمن المعلومات، والالتزام، والتدقيق الداخلي، وتقنية المعلومات، والتحول الرقمي، والعمليات، والمطالبات، والاكتاب، وخدمات العملاء.

كما تناسب المتخصصين العاملين في التأمين السيبراني، وتقييم المخاطر، وإدارة مخاطر الأطراف الخارجية، واستمرارية الأعمال، وحماية البيانات، وحوكمة التقنية، والمخاطر الرقابية، ممن يحتاجون إلى فهم أعمق للمخاطر

السيرانية من منظور الأعمال وقطاع التأمين.

وتعد الدورة مناسبة بشكل خاص لشركات التأمين التي تسعى إلى تعزيز المرونة السيرية، وتحسين وضوح المخاطر، وحماية بيانات العملاء الحساسة، وتقوية حوكمة المخاطر التقنية، واتخاذ قرارات أكثر دقة بشأن التعرض للمخاطر السيرية وسبل الحد منها.

مخرجات التعلم

- بنهاية الدورة، سيتمكن المشاركون من:
- بناء منهجية منظمة لتقييم المخاطر السيرية داخل شركة التأمين.
- تحديد الأصول المعلوماتية والأنظمة والعمليات والاعتماديات التشغيلية الحرجة.
- تحديد التهديدات والثغرات السيرية المؤثرة في العمليات التأمينية.
- تطوير سيناريوهات واقعية للمخاطر السيرية وتقييم نتائجها المحتملة.
- تقييم المخاطر وفق احتمالية الحدوث والأثر والتعرض وفعالية الضوابط.
- التمييز بين المخاطر المتأصلة والمخاطر الخاضعة للضوابط والمخاطر المتبقية.
- تحديد نقاط الضعف والفجوات في الضوابط الأمنية.
- تطوير تصنيفات وألويات للمخاطر السيرية.
- تقييم المخاطر السيرية المرتبطة بالأطراف الخارجية ومقدمي الخدمات.
- تحليل المخاطر المتعلقة ببيانات العملاء والمنصات والخدمات الرقمية.
- إعداد خطط لمعالجة المخاطر والحد منها.
- موازنة إدارة المخاطر السيرية مع شهية المخاطر وإدارة المخاطر المؤسسية.
- دعم الإدارة وصناع القرار بمعلومات واضحة عن المخاطر السيرية.

- دمج المخاطر السيبرانية في خطط استمرارية الأعمال والمرونة المؤسسية.
- تعزيز الحوكمة والمساءلة عن المخاطر السيبرانية.
- إعداد خارطة طريق عملية لتطوير تقييم وإدارة المخاطر السيبرانية.
- المحاوّر التدريبية

محاوّر الدورة

اليوم الأول

مشهد المخاطر السيبرانية في قطاع التأمين

- مفهوم المخاطر السيبرانية وأهميتها الاستراتيجية لشركات التأمين.
- تطور التهديدات السيبرانية المؤثرة في قطاع التأمين.
- أبرز التهديدات والثغرات ونقاط الدخول السيبرانية.
- تحديد الأصول المعلوماتية والاعتماديات التقنية الحرجة.
- المخاطر السيبرانية في الاكتتاب والمطالبات وإدارة الوثائق والمدفوعات وخدمة العملاء.
- المخاطر المرتبطة بالمنصات والخدمات التأمينية الرقمية.
- مخاطر تعرض بيانات العملاء للسرقة أو التسريب.
- الآثار المالية والتشغيلية والرقابية والقانونية والسمعة الناتجة عن الحوادث السيبرانية.
- بناء ثقافة مؤسسية واعية بالمخاطر السيبرانية.
- تطبيق عملي: تحديد الأصول والعمليات والاعتماديات والتهديدات السيبرانية الرئيسية داخل نموذج لشركة تأمين.

اليوم الثاني

تحديد المخاطر السيبرانية ومنهجيات تقييمها

- مبادئ تحديد المخاطر السيبرانية وتقييمها.
- أساليب التقييم القائمة على الأصول والسيناريوهات.
- تحديد التهديدات والثغرات والأحداث المسببة للمخاطر.
- تطوير سيناريوهات مخاطر سيبرانية متخصصة في قطاع التأمين.
- تقييم احتمالية وقوع المخاطر والأثر المحتمل.
- تحليل الآثار المالية والتشغيلية والرقابية والمتعلقة بالعملاء والسمعة.
- إعداد مصفوفات ونماذج لتصنيف المخاطر السيبرانية.
- تقييم فعالية الضوابط الحالية.
- تحديد المخاطر المتأصلة والمخاطر المتبقية.
- ترتيب أولويات المخاطر وفق مستوى التعرض وأهمية الأعمال.
- تطبيق عملي: تنفيذ تقييم منظم للمخاطر السيبرانية لعدد من العمليات التأمينية وتحديد مستويات المخاطر وأولويات المعالجة.

اليوم الثالث

الضوابط السيبرانية ومخاطر الأطراف الخارجية وحماية البيانات

- فهم الضوابط الوقائية والكاشفة والتصحيحية للأمن السيبراني.
- تقييم فعالية الضوابط الأمنية الحالية.
- تحديد نقاط الضعف والفجوات وأولويات المعالجة.
- المخاطر السيبرانية المرتبطة بمقدمي الخدمات والأطراف الخارجية.
- تقييم مخاطر الموردين والاستعانة بمصادر خارجية والخدمات السحابية.

اليوم الثالث — تابع

- حماية بيانات العملاء ومخاطر الخصوصية.
- المخاطر المرتبطة بالمنصات والتطبيقات الرقمية للعملاء.
- إدارة مخاطر الوصول والتحقق من الهوية وأمن البيانات وحماية المعلومات.
- تقييم المرونة السيبرانية لدى مقدمي الخدمات الحيوية.
- دمج مخاطر الأطراف الخارجية في تقييم المخاطر المؤسسية.
- تطبيق عملي: تقييم المخاطر السيبرانية لمقدم خدمة خارجي رئيسي وإعداد خطة متكاملة لمعالجة المخاطر.

اليوم الرابع

معالجة المخاطر السيبرانية والمرونة والآثار التأمينية

- تطوير استراتيجيات معالجة المخاطر السيبرانية.
- تجنب المخاطر والحد منها ونقلها وقبولها ومعالجتها.
- موازنة معالجة المخاطر مع شهية المخاطر.
- الاستجابة للحوادث السيبرانية وآليات التصعيد.
- استمرارية الأعمال والتعافي من الكوارث الناتجة عن الحوادث السيبرانية.
- المرونة السيبرانية واستعادة الخدمات التأمينية الحرجة.
- آثار المخاطر السيبرانية على الاكتتاب واختيار المخاطر التأمينية.
- فهم التعرض للمخاطر السيبرانية واعتبارات نقل المخاطر.
- تحليل السيناريوهات واختبارات التحمل للمخاطر السيبرانية.
- تطوير مؤشرات الإنذار المبكر للمخاطر السيبرانية الناشئة.
- تطبيق عملي: تحليل سيناريو حادث سيبراني كبير يؤثر في شركة تأمين وإعداد خطة متكاملة للاستجابة والمعالجة وتعزيز المرونة.

اليوم الخامس

حوكمة المخاطر السيبرانية وإعداد التقارير والتنفيذ

- حوكمة المخاطر السيبرانية وتحديد المسؤوليات.
- أدوار الإدارة التنفيذية وإدارة المخاطر والتقنية والأمن والالتزام والتدقيق الداخلي.
- دمج المخاطر السيبرانية ضمن إدارة المخاطر المؤسسية.
- شهية المخاطر وحدود تحمل المخاطر السيبرانية.
- تطوير مؤشرات المخاطر السيبرانية ولوحات المعلومات الإدارية.
- إعداد تقارير المخاطر السيبرانية للإدارة العليا وصناع القرار.
- متابعة المخاطر السيبرانية الناشئة وتغيرات بيئة التهديدات.
- إنشاء عمليات مستمرة لتقييم المخاطر السيبرانية.
- ترتيب الاستثمارات في الأمن السيبراني وفق مستوى التعرض للمخاطر.
- بناء إطار مستدام لإدارة المخاطر السيبرانية.
- إعداد خارطة طريق لتطبيق وتطوير تقييم المخاطر السيبرانية.
- ورشة ختامية: تطوير إطار متكامل لتقييم المخاطر السيبرانية لشركة تأمين، يشمل الأصول الحرجة، وسيناريوهات التهديدات، وتصنيف المخاطر، وتقييم الضوابط، والمخاطر المتبقية، ومخاطر الأطراف الخارجية، واستراتيجيات المعالجة، والحوكمة، والتقارير، وخارطة طريق التنفيذ.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

<https://quest-training.com/courses/cyber-risk-assessment-for-insurance-professionals-training-course>الموقع الإلكتروني: <https://quest-training.com>البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440