

رقم الدورة 1925

دورة قياس المخاطر السييرانية كمياً لقطاع التأمين

التأمين السييراني
التأمين وإدارة المخاطر

طريقة التقديم

حضور

المدة

5 أيام



نظرة عامة على الدورة

تقدم دورة قياس المخاطر السيبرانية كمياً لقطاع التأمين إطاراً عملياً وتحليلياً متقدماً لقياس المخاطر السيبرانية وتحويلها إلى مؤشرات مالية قابلة للتحليل واتخاذ القرار. وتهدف الدورة إلى تمكين المتخصصين في قطاع التأمين من الانتقال من التقييمات الوصفية للمخاطر السيبرانية إلى تقديرات كمية للخسائر المحتملة، بما يدعم الاكتتاب والتسعير وإدارة المحافظ وإعادة التأمين.

يتعرف المشاركون على العلاقة بين التهديدات السيبرانية والثغرات والضوابط الأمنية والاعتماديات التشغيلية والآثار المالية. كما يتناول البرنامج كيفية تحويل الحوادث السيبرانية، مثل هجمات الفدية وتسريب البيانات وانقطاع الأعمال والأعطال التقنية وانقطاع الخدمات السحابية والهندسة الاجتماعية والحوادث المرتبطة بالأطراف الخارجية، إلى سيناريوهات خسائر قابلة للقياس لأغراض التأمين.

تركز الدورة على منهجيات التقييم الكمي للمخاطر، بما يشمل تحليل تكرار الخسائر وشدتها، والقياس القائم على السيناريوهات، وتوزيعات الخسائر، وتقدير الاحتمالات، ونمذجة الآثار المالية، وتحليل الحساسية، واختبارات التحمل، وتحليل التجمع والتراكم. كما تتناول تحديات محدودية البيانات التاريخية، وسرعة تغير التهديدات السيبرانية، وتربط الأحداث، والمخاطر السيبرانية النظامية، وعدم اليقين في تقديرات الخسائر.

كما يتعلم المشاركون كيفية استخدام النتائج الكمية للمخاطر السيبرانية في الاكتتاب والتسعير وتحديد الحدود والتحملات وقرارات إعادة التأمين وتخطيط رأس المال وتحسين المحافظ وتحديد شهية المخاطر. ومن خلال التمارين العملية ودراسات الحالة والسيناريوهات المالية، يطور المشاركون منهجية متكاملة لقياس المخاطر السيبرانية وترجمة النتائج التحليلية إلى قرارات تأمينية قابلة للتنفيذ.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل مبادئ وتطبيقات القياس الكمي للمخاطر السيبرانية في قطاع التأمين.
- تحديد المحركات الرئيسية للمخاطر السيبرانية وآثارها المالية المحتملة.

- تحويل التهديدات والثغرات السيبرانية إلى سيناريوهات خسائر قابلة للقياس.
- تقييم تكرار الخسائر السيبرانية وشدتها باستخدام الأساليب الكمية.
- تطوير نماذج للآثار المالية الناتجة عن الحوادث السيبرانية الكبرى.
- تطبيق تحليل السيناريوهات على مخاطر هجمات الفدية وتسريب البيانات وانقطاع الأعمال.
- تقييم الآثار المالية للحوادث السيبرانية المرتبطة بالأطراف الخارجية والخدمات السحابية.
- تطبيق تحليل الاحتمالات وعدم اليقين والحساسية في تقديرات المخاطر السيبرانية.
- تطوير توزيعات للخسائر وتقدير نطاقات الخسائر المحتملة.
- قياس مخاطر التراكم والتجمع والمخاطر السيبرانية النظامية.
- استخدام المعلومات الكمية للمخاطر في دعم قرارات الاكتتاب والتسعير.
- تقييم الحدود التأمينية والتحملات وهياكل نقل المخاطر المناسبة.
- دمج القياس الكمي للمخاطر السيبرانية في قرارات إدارة المحافظ وإعادة التأمين.
- تطبيق اختبارات التحمل على السيناريوهات السيبرانية شديدة التأثير.
- عرض نتائج القياس الكمي للمخاطر السيبرانية بوضوح أمام القيادات وصناع القرار.

الفئة المستهدفة

تستهدف الدورة القيادات التنفيذية ومديري الاكتتاب وكبار المكتبيين والمتخصصين الاكتواريين ومديري المخاطر والمتخصصين في التأمين السيبراني ومديري المحافظ والعاملين في التقييم المالي للمخاطر السيبرانية.

كما تناسب المتخصصين في المطالبات والتسعير وإعادة التأمين وإدارة المخاطر المؤسسية ومخاطر التقنية والأمن السيبراني وتحليل البيانات والمخاطر المالية والالتزام والحوكمة، ممن يشاركون في تقييم التعرض السيبراني والخسائر المالية المحتملة.

وتعد الدورة مناسبة بشكل خاص لشركات التأمين التي تسعى إلى تعزيز قدراتها في القياس الكمي للمخاطر

السيبرانية، وتحسين الاكتتاب والتسعير القائم على المخاطر، وتقييم مخاطر تراكم المحافظ، ودعم قرارات إعادة التأمين، وتزويد الإدارة العليا برؤية مالية أكثر وضوحاً حول التعرض للمخاطر السيبرانية.

مخرجات التعلم

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح دور التقييم الكمي للمخاطر السيبرانية في قطاع التأمين.
- تحديد البيانات اللازمة لقياس المخاطر السيبرانية كمياً.
- تطوير سيناريوهات منظمة للخسائر السيبرانية.
- تقدير الخسائر المالية المحتملة الناتجة عن الحوادث السيبرانية.
- تحليل تكرار الخسائر وشدتها.
- تقييم الآثار المالية المباشرة وغير المباشرة للحوادث السيبرانية.
- قياس خسائر انقطاع الأعمال والاعتماد على التقنيات والخدمات الرقمية.
- تقييم مخاطر الأطراف الخارجية ومخاطر التركيز في الخدمات السحابية.
- تطبيق أساليب الاحتمالات وعدم اليقين في تقديرات المخاطر.
- إجراء تحليل الحساسية للعوامل والافتراضات الرئيسية.
- تطوير رؤية كمية لمخاطر التراكم والمخاطر السيبرانية النظامية.
- استخدام اختبارات التحمل لتقييم السيناريوهات السيبرانية شديدة التأثير.
- تطبيق نتائج القياس الكمي في قرارات الاكتتاب والتسعير.
- دعم قرارات الحدود والتحملات وإعادة التأمين ونقل المخاطر.
- تفسير نتائج القياس الكمي للمخاطر السيبرانية أمام الإدارة وصناع القرار.

- تطوير إطار عملي للقياس الكمي للمخاطر السيبرانية في التطبيقات التأمينية.
- المحاوّر التدريبية

محاوّر الدورة

اليوم الأول

أسس القياس الكمي للمخاطر السيبرانية في قطاع التأمين

- مفهوم القياس الكمي للمخاطر السيبرانية وأهدافه.
- الفرق بين التقييم النوعي والتقييم الكمي للمخاطر السيبرانية.
- التهديدات والثغرات والضوابط والتعرض المالي للمخاطر.
- تحديد الأصول والأنظمة والعمليات والاعتماديات الحرجة.
- سيناريوهات هجمات الفدية وتسريب البيانات وانقطاع الأعمال والأعطال التقنية.
- الآثار المالية المباشرة وغير المباشرة للحوادث السيبرانية.
- محركات المخاطر السيبرانية في القطاعات ونماذج الأعمال المختلفة.
- البيانات المطلوبة للتحليل الكمي للمخاطر السيبرانية.
- تحديات البيانات غير المكتملة والمتغيرة باستمرار.
- تحديد الافتراضات وحدود نماذج القياس الكمي.
- تطبيق عملي: إعداد ملف منظم للمخاطر السيبرانية وتحديد المتغيرات الرئيسية اللازمة لقياس الخسائر التأمينية المحتملة.

اليوم الثاني

تكرار الخسائر وشدتها ونمذجة الآثار المالية

- مبادئ تحليل تكرار الخسائر السيبرانية وشدتها.
- تحديد الأحداث ومتغيرات التعرض ذات الصلة.
- تقدير احتمالية وقوع الحوادث السيبرانية.
- تقييم شدة الخسائر المحتملة.
- نمذجة خسائر هجمات الفدية والابتزاز السيبراني.
- قياس خسائر تسريب البيانات والخصوصية.
- نمذجة خسائر انقطاع الأعمال.
- تقييم تكاليف استعادة الأنظمة والبيانات والمصروفات الإضافية.
- تحليل خسائر انقطاع الأعمال الناتج عن الأطراف الخارجية.
- بناء افتراضات وسيناريوهات الخسائر المالية.
- تطبيق عملي: بناء نموذج افتراضي للخسائر السيبرانية يشمل التكرار والشدة والخسائر المباشرة وانقطاع الأعمال والمصروفات الإضافية.

اليوم الثالث

تحليل السيناريوهات والاحتمالات وعدم اليقين

- القياس الكمي للمخاطر باستخدام السيناريوهات.
- تطوير سيناريوهات سيبرانية شديدة ولكن معقولة.
- تقدير الاحتمالات والخسائر المحتملة.
- فهم مصادر عدم اليقين في نماذج المخاطر السيبرانية.
- تحليل الحساسية والافتراضات الرئيسية.

اليوم الثالث — تابع

- تحليل سيناريوهات هجمات الفدية واسعة التأثير.
- نمذجة انقطاع الخدمات السحابية ومقدمي الخدمات التقنية.
- تقييم المخاطر السيبرانية المرتبطة بسلاسل التوريد.
- اختبارات التحمل للتعرضات السيبرانية.
- تفسير نطاقات الخسائر المحتملة ومستويات الثقة.
- تطبيق عملي: قياس آثار حادث سيبراني كبير باستخدام عدة سيناريوهات وتحليل تأثير تغير الافتراضات الرئيسية على تقديرات الخسائر.

اليوم الرابع

التراكم والمخاطر النظامية والقياس الكمي للمخاطر

- مخاطر التراكم والتجمع في التأمين السيبراني.
- الأحداث السيبرانية المترابطة والمتزامنة.
- المخاطر السيبرانية النظامية والأعطال التقنية واسعة النطاق.
- تحليل التعرض على مستوى المحفظة.
- مقدمو الخدمات التقنية المشتركة ومخاطر التركيز.
- تقدير الخسائر الإجمالية عبر عدة مؤمن لهم.
- اختبارات التحمل للمخاطر باستخدام السيناريوهات.
- تقييم الأحداث المحتملة ذات الخسائر الكبيرة.
- استخدام نتائج القياس الكمي في قرارات إعادة التأمين ونقل المخاطر.
- دعم تخطيط رأس المال وشهية المخاطر.
- تحسين المحافظ باستخدام البيانات الكمية للمخاطر.

اليوم الرابع — تابع

- تطبيق عملي: تحليل محفظة تأمينية افتراضية معرضة لحدث سيرياني نظامي وقياس الأثر المالي الإجمالي المحتمل.

اليوم الخامس

تطبيق القياس الكمي في الاكتتاب والتسعير والقرارات الاستراتيجية

- استخدام القياس الكمي للمخاطر في الاكتتاب السيرياني.
- ربط حجم التعرض الكمي بقرارات التسعير.
- دعم قرارات الحدود التأمينية والتحملات.
- دمج القياس الكمي للمخاطر في إدارة المحافظ.
- توظيف النتائج الكمية في استراتيجية إعادة التأمين.
- متابعة التغيرات في التعرض السيرياني طوال دورة الوثيقة.
- حوكمة النماذج والتحقق منها وتوثيق حدودها.
- إدارة عدم اليقين وتجنب الاعتماد المفرط على مخرجات النماذج.
- عرض نتائج المخاطر الكمية على الإدارة العليا.
- تطوير مؤشرات وتقارير كمية للمخاطر السيريانية.
- بناء إطار مستدام للقياس الكمي للمخاطر السيريانية.
- ورشة ختامية: تطوير إطار متكامل للقياس الكمي للمخاطر السيريانية لمحفظة تأمينية، يشمل تحليل التعرض، وسيناريوهات الخسائر، وتكرار الخسائر وشدها، ونمذجة الأثر المالي، وعدم اليقين، واختبارات التحمل، والتراكم، وتطبيقات الاكتتاب والتسعير، واعتبارات إعادة التأمين، وإعداد التقارير التنفيذية.



للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: <https://quest-training.com/courses/cyber-risk-quantification-for-insurance-training-course>

الموقع الإلكتروني: <https://quest-training.com>

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440

