

رقم الدورة 1926

دورة أساسيات التأمين السيبراني وإدارة المخاطر

التأمين السيبراني
التأمين وإدارة المخاطر

طريقة التقديم

حضور

المدة

5 أيام



نظرة عامة على الدورة

تقدم دورة أساسيات التأمين السيراني وإدارة المخاطر أساساً مهنياً متكاملاً لفهم التأمين السيراني وطبيعة المخاطر السيرانية ومبادئ إدارتها من منظور تأميني وإدارة المخاطر المؤسسية. وتهدف الدورة إلى تمكين المتخصصين في قطاع التأمين ومديري المخاطر والقيادات التنفيذية من فهم كيفية تحول التهديدات السيرانية إلى مخاطر مالية وتشغيلية ورقابية وقانونية ومرتبطة بالسمعة.

يتعرف المشاركون على مشهد المخاطر السيرانية، بما يشمل هجمات الفدية، وتسريب البيانات، وحوادث الخصوصية، وانقطاع الأعمال، والأعطال التقنية، والهندسة الاجتماعية، والاعتماد على الخدمات السحابية، ونقاط ضعف سلاسل التوريد، والمخاطر السيرانية المرتبطة بالأطراف الخارجية. ويركز البرنامج على العلاقة بين هذه التهديدات وآليات التأمين المستخدمة لتحديد المخاطر وتقييمها ونقلها وإدارتها.

تغطي الدورة أساسيات منتجات التأمين السيراني ومكونات التغطية الرئيسية وهيكل الوثائق واعتبارات الاكتتاب والاستثناءات والحدود والتحملات وإجراءات المطالبات واستراتيجيات نقل المخاطر. كما يتعرف المشاركون على العلاقة بين الضوابط الأمنية ومستوى نضج إدارة المخاطر السيرانية وقرارات التأمين والتسعير وشروط الوثائق.

كما تتناول الدورة حوكمة المخاطر السيرانية وتقييم المخاطر والاستعداد للحوادث واستمرارية الأعمال والمرونة ومخاطر الأطراف الخارجية والمتطلبات الرقابية والمخاطر السيرانية الناشئة. ومن خلال دراسات الحالة وتمارين تقييم المخاطر والسيناريوهات التأمينية، يطور المشاركون أساساً عملياً قوياً لإدارة المخاطر السيرانية واتخاذ قرارات أكثر فاعلية بشأن التأمين السيراني ونقل المخاطر.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح أساسيات التأمين السيراني ودوره الاستراتيجي في إدارة المخاطر.
- تحليل تطور مشهد المخاطر السيرانية وتأثيره على المؤسسات.

- تحديد أبرز المخاطر السيبرانية التي قد تؤدي إلى خسائر مالية قابلة للتأمين.
- تقييم مخاطر هجمات الفدية وتسريب البيانات وانقطاع الأعمال والأعطال التقنية.
- تحليل العلاقة بين الضوابط الأمنية وقرارات التأمين السيبراني.
- فهم هياكل التغطية التأمينية السيبرانية ومكونات الوثائق الرئيسية.
- تقييم الحدود التأمينية والتحملات والاستثناءات والحدود الفرعية وشروط الوثائق.
- تطبيق منهجيات منظمة لتقييم وإدارة المخاطر السيبرانية.
- تقييم مخاطر الأطراف الخارجية وسلاسل التوريد والخدمات السحابية والاعتماد على التقنية.
- تطوير استراتيجيات مناسبة للحد من المخاطر السيبرانية ونقلها.
- فهم دور الاكتتاب والتسعير والمطالبات وإعادة التأمين في التأمين السيبراني.
- تقييم حوكمة المخاطر السيبرانية والمسؤوليات المؤسسية.
- تطبيق تحليل السيناريوهات على الحوادث السيبرانية المهمة.
- تعزيز الاستعداد للحوادث السيبرانية واستمرارية الأعمال.
- تطوير إطار متكامل لإدارة المخاطر والتأمين السيبراني.

الفئة المستهدفة

تستهدف الدورة القيادات التنفيذية والمتخصصين في الاكتتاب ومديري المطالبات ومديري المخاطر والمتخصصين في التأمين السيبراني والمسؤولين عن تقييم وإدارة المخاطر السيبرانية. كما تناسب المهنيين الذين يحتاجون إلى فهم شامل للتأمين السيبراني دون الحاجة إلى خلفية تقنية متعمقة في الأمن السيبراني.

وتناسب الدورة أيضاً المتخصصين في إدارة المخاطر المؤسسية والالتزام والحوكمة والتدقيق الداخلي وأمن المعلومات ومخاطر التقنية واستمرارية الأعمال ووسطاء التأمين وإعادة التأمين والمتخصصين الاكتواريين والمستشارين القانونيين والعاملين في برامج التأمين المؤسسية.

وتعد الدورة مناسبة بشكل خاص للجهات التي تسعى إلى رفع الوعي بالمخاطر السيبرانية، وتحسين جاهزية التأمين، وفهم آليات نقل المخاطر السيبرانية، وتعزيز المرونة المؤسسية، وبناء تنسيق فعال بين الأمن السيبراني وإدارة المخاطر والتأمين ووحدات الأعمال.

مخرجات التعلم

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح المفاهيم والمبادئ الأساسية للتأمين السيبراني.
- تحديد أبرز التهديدات السيبرانية وآثارها المحتملة على الأعمال.
- تقييم المخاطر السيبرانية الرئيسية من منظور تأميني.
- التمييز بين أنواع التغطيات المختلفة في التأمين السيبراني.
- تقييم الحدود والتحملات والاستثناءات وشروط التغطية.
- تحليل دور الضوابط الأمنية في قرارات التأمين السيبراني.
- تحديد المعلومات الأساسية المطلوبة لتقييم المخاطر السيبرانية.
- تقييم مستوى نضج إدارة المخاطر والأمن السيبراني في المؤسسة.
- تحليل مخاطر الأطراف الخارجية والخدمات السحابية وسلاسل التوريد.
- تطوير استراتيجيات عملية للحد من المخاطر السيبرانية.
- تقييم الأساليب المناسبة لنقل المخاطر السيبرانية.
- فهم العلاقة بين الاكتتاب والمطالبات والتسعير وإعادة التأمين.
- تطبيق تحليل السيناريوهات على الحوادث السيبرانية المحتملة.
- تعزيز جاهزية الحوادث وترتيبات استمرارية الأعمال.

- دعم الإدارة في اتخاذ قرارات التأمين وشهية المخاطر السيبرانية.
- تطوير إطار عملي لدمج التأمين السيبراني ضمن إدارة المخاطر المؤسسية.
- المحاوّر التدريبية

محاوّر الدورة

اليوم الأول

مشهد المخاطر السيبرانية وأساسيات التأمين السيبراني

- مفهوم المخاطر السيبرانية والتأمين السيبراني.
- تطور التهديدات السيبرانية وأنماط المخاطر الناشئة.
- هجمات الفدية والبرمجيات الضارة والتصيد والهندسة الاجتماعية.
- تسريب البيانات والمخاطر المرتبطة بالخصوصية.
- مخاطر انقطاع الأعمال والأعطال التقنية.
- مخاطر الخدمات السحابية والاعتماد على التقنيات الرقمية.
- مخاطر الأطراف الخارجية وسلاسل التوريد.
- الآثار المالية والتشغيلية والرقابية والقانونية والمرتبطة بالسمعة.
- دور التأمين السيبراني ضمن إدارة المخاطر المؤسسية.
- الأطراف الرئيسية المشاركة في إدارة المخاطر والتأمين السيبراني.
- تطبيق عملي: تحليل مجموعة من الحوادث السيبرانية وتحديد آثارها المالية والتشغيلية والتأمينية المحتملة.

اليوم الثاني

تقييم المخاطر السيبرانية وإدارتها

- مبادئ تحديد وتقييم المخاطر السيبرانية.
- تحديد الأصول والأنظمة والعمليات والاعتماديات الحرجة.
- تحليل التهديدات والثغرات ونقاط الضعف.
- تقييم الضوابط الأمنية ومستوى النضج السيبراني.
- تقييم احتمالية المخاطر وتأثيرها ومستوى التعرض لها.
- تصنيف المخاطر السيبرانية وترتيب أولوياتها.
- شهية المخاطر وحدود تحمل المخاطر السيبرانية.
- استراتيجيات الحد من المخاطر وتحسين الضوابط.
- الاستعداد للحوادث وقدرات الاستجابة.
- استمرارية الأعمال والمرونة السيبرانية.
- تطبيق عملي: تنفيذ تقييم منظم للمخاطر السيبرانية لمؤسسة افتراضية وإعداد خطة ذات أولويات لمعالجة المخاطر.

اليوم الثالث

منتجات التأمين السيبراني والتغطيات وهيكل الوثائق

- نظرة عامة على منتجات التأمين السيبراني وهيكل السوق.
- التغطيات المتعلقة بالمخاطر التي يتحملها المؤمن له والأطراف الخارجية.
- تغطية تسريب البيانات وحوادث الخصوصية.
- تغطية انقطاع الأعمال الناتج عن الحوادث السيبرانية.
- تغطية الابتزاز السيبراني وهجمات الفدية.

اليوم الثالث — تابع

- تكاليف استعادة البيانات والاستجابة للحوادث.
- مسؤولية أمن الشبكات والمسؤولية التقنية.
- الحدود التأمينية والتحملات والحدود الفرعية.
- الاستثناءات والشروط والاشتراطات التأمينية.
- فهم محفزات التغطية واستجابة الوثيقة للحوادث.
- العلاقة بين الضوابط السيرانية وشروط التأمين.
- تطبيق عملي: مراجعة وثيقة تأمين سيراني افتراضية وتحديد التغطيات والقيود والاستثناءات ومتطلبات المخاطر الرئيسية.

اليوم الرابع

نقل المخاطر السيرانية والاكتتاب والمطالبات والمخاطر الناشئة

- مبادئ نقل المخاطر السيرانية.
- أساسيات اكتتاب التأمين السيراني.
- المعلومات المطلوبة لتقييم المخاطر لأغراض الاكتتاب.
- اختيار المخاطر وتصنيفها.
- اعتبارات التسعير وعلاقتها بجودة المخاطر.
- دورة حياة المطالبة السيرانية وإدارتها.
- التحقيق في الحوادث وتقييم الخسائر.
- الاحتيال والتضليل ومخاطر المطالبات.
- إعادة التأمين وإدارة مخاطر المحافظ.
- الحوادث السيرانية النظامية ومخاطر التراكم.
- المخاطر السيرانية الناشئة وآثارها على التأمين.

اليوم الرابع — تابع

- تطبيق عملي: تقييم خطر سيرياني افتراضي من مرحلة الاكتتاب إلى المطالبة وتحديد إجراءات نقل المخاطر وإدارتها المناسبة.

اليوم الخامس

حوكمة التأمين السيرياني والمرونة والتنفيذ الاستراتيجي

- حوكمة التأمين السيرياني وتحديد المسؤوليات المؤسسية.
- دمج التأمين السيرياني في إدارة المخاطر المؤسسية.
- شهية المخاطر والاستراتيجية التأمينية السيريانية.
- تطوير إطار جاهزية المؤسسة للتأمين السيرياني.
- التنسيق بين التأمين والأمن السيرياني أثناء الحوادث.
- استمرارية الأعمال والمرونة المؤسسية.
- إدارة مخاطر الأطراف الخارجية وسلاسل التوريد.
- متابعة التغيرات في مستوى التعرض للمخاطر السيريانية.
- التقارير الإدارية ومؤشرات المخاطر السيريانية.
- مراجعة كفاية التغطية والاحتياجات التأمينية.
- بناء استراتيجية مستدامة لإدارة المخاطر والتأمين السيرياني.
- ورشة ختامية: تطوير إطار متكامل للتأمين السيرياني وإدارة المخاطر يشمل تحديد التعرضات السيريانية، وتقييم المخاطر، والضوابط الأمنية، والتغطيات التأمينية، ونقل المخاطر، والاستجابة للحوادث، واستمرارية الأعمال، والحوكمة، وخطة التنفيذ الاستراتيجي.



للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

<https://quest-training.com/courses/cyber-insurance-fundamentals-risk-management-training-course>

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440

