QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1944

# دورة إدارة مخاطر الأمن السيبراني المتقدمة

**الأمن السيبراني وأمن المعلومات**
**تقنية المعلومات والأمن السيبراني**

المدة
**5 أيام**

طريقة التقديم
**حضوري**

## نظرة عامة على الدورة

تقدم دورة إدارة مخاطر الأمن السيبراني المتقدمة منهجية متقدمة واستراتيجية وعملية لإدارة المخاطر السيبرانية في البيئات المؤسسية المعقدة. وتتجاوز الدورة أساليب تحديد المخاطر الأساسية لتتناول قياس المخاطر كمياً، وترتيب الأولويات الاستراتيجية، والحوكمة، والمرونة السيبرانية، واتخاذ القرارات، ودمج مخاطر الأمن السيبراني ضمن منظومة إدارة المخاطر المؤسسية.

يتعرف المشاركون على كيفية تحديد المخاطر السيبرانية المتطورة وتقييم أثرها المحتمل على الأعمال، وتحديد شهية المخاطر وحدود التحمل، واتخاذ قرارات مدروسة بشأن معالجة المخاطر والاستثمارات الأمنية. كما تتناول الدورة المخاطر التقنية والتشغيلية والمالية والتنظيمية ومخاطر الأطراف الثالثة والحوسبة السحابية والبيانات والمخاطر السيبرانية الناشئة.

تركز الدورة على الربط بين مخاطر الأمن السيبراني وصنع القرار التنفيذي، حيث يتعلم المشاركون كيفية تحويل الثغرات التقنية ومعلومات التهديدات إلى سيناريوهات مخاطر مؤسسية، وقياس الخسائر المحتملة عند الحاجة، وتطوير مؤشرات مخاطر ذات قيمة إدارية، والتواصل الفعال بشأن مستوى التعرض السيبراني مع الإدارة العليا ومجالس الإدارة.

ومن خلال السيناريوهات المتقدمة وتمارين التحليل الكمي وورش تقييم المخاطر ومحاكاة المخاطر السيبرانية وأنشطة تحديد أولويات الاستثمارات والتخطيط الاستراتيجي، يطور المشاركون القدرات اللازمة لبناء برامج ناضجة لإدارة مخاطر الأمن السيبراني وتعزيز قدرة المؤسسة على الصمود أمام التهديدات السيبرانية المتطورة.

## أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل المفاهيم المتقدمة لإدارة مخاطر الأمن السيبراني وأثرها على الاستراتيجية المؤسسية.
- تقييم المخاطر السيبرانية المعقدة عبر الجوانب التقنية والتشغيلية والمالية والتنظيمية ومخاطر الأطراف الثالثة.

- تطوير منهجيات متقدمة لتقييم وقياس مخاطر الأمن السيبراني.
- تقييم المخاطر السيبرانية وفق الاحتمالية والأثر ومستوى التعرض وسيناريوهات الخسائر.
- تحديد شهية المخاطر السيبرانية وحدود التحمل ومستويات التصعيد.
- ترتيب أولويات المخاطر السيبرانية وفق أهمية الأعمال والأثر المحتمل.
- تطوير استراتيجيات متقدمة لمعالجة المخاطر والحد منها.
- تقييم الاستثمارات الأمنية باستخدام مبادئ اتخاذ القرار القائم على المخاطر.
- دمج مخاطر الأمن السيبراني مع إدارة المخاطر المؤسسية.
- تطوير مؤشرات مخاطر سيبرانية فعالة ولوحات متابعة للإدارة العليا.
- تقييم المخاطر السيبرانية الناشئة والنظامية والمترابطة.
- تعزيز إدارة مخاطر الأطراف الثالثة وسلاسل التوريد والحوسبة السحابية والتقنيات الحديثة.
- تطوير استراتيجيات المرونة السيبرانية المتوافقة مع الخدمات المؤسسية الحيوية.
- تحسين التقارير التنفيذية وتقارير مجالس الإدارة المتعلقة بمخاطر الأمن السيبراني.
- بناء نموذج تشغيل متقدم لإدارة مخاطر الأمن السيبراني وخارطة طريق لتطويره.

## الفئة المستهدفة

تستهدف الدورة مديري الأمن السيبراني وأمن المعلومات، ومتخصصي مخاطر الأمن السيبراني، ومديري المخاطر المؤسسية، ومهندسي الأمن، ومتخصصي الحوكمة والالتزام، وقادة عمليات الأمن السيبراني، ومتخصصي مخاطر التقنية، ومديري تقنية المعلومات.

كما تناسب المدققين الداخليين، ومتخصصي استمرارية الأعمال والمرونة المؤسسية، ومديري أمن الحوسبة السحابية، ومتخصصي مخاطر الأطراف الثالثة، ومتخصصي ضمان التقنية، والقيادات التنفيذية المشاركة في حوكمة الأمن السيبراني والإشراف على المخاطر وقرارات الاستثمار والمرونة المؤسسية.

وتكتسب الدورة أهمية خاصة للمؤسسات التي تسعى إلى الانتقال من تقييمات مخاطر الأمن السيبراني التقليدية إلى منهجية ناضجة ومرتبطة بالأعمال، قادرة على دعم القرارات الاستراتيجية وترتيب أولويات الاستثمارات وتحقيق المتطلبات الرقابية وتعزيز المرونة المؤسسية.

## مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- تقييم المخاطر السيبرانية المعقدة ضمن إطار إدارة المخاطر المؤسسية.
- تطوير منهجيات متقدمة لتقييم مخاطر الأمن السيبراني.
- تحليل سيناريوهات المخاطر السيبرانية والنتائج المحتملة على الأعمال.
- تطبيق الأساليب الكمية والنوعية في تحليل المخاطر السيبرانية.
- تقدير الخسائر المالية والتشغيلية المحتملة الناتجة عن المخاطر السيبرانية الرئيسية.
- تحديد شهية المخاطر السيبرانية وإطار حدود التحمل.
- ترتيب المخاطر وفق أهمية الأعمال ومستوى التعرض والاحتمالية والأثر.
- تطوير استراتيجيات لمعالجة المخاطر السيبرانية ذات الأولوية.
- تقييم فعالية الضوابط الأمنية ومستوى المخاطر المتبقية.
- دمج معلومات التهديدات في قرارات إدارة المخاطر السيبرانية.
- تقييم مخاطر الأطراف الثالثة وسلاسل التوريد والحوسبة السحابية والمخاطر الناشئة.
- تطوير مؤشرات مخاطر الأمن السيبراني والتقارير التنفيذية.
- مواءمة الاستثمارات الأمنية مع أولويات المخاطر المؤسسية.
- تعزيز المرونة السيبرانية وحماية الخدمات المؤسسية الحيوية.

- دعم قرارات الإدارة العليا ومجالس الإدارة المتعلقة بالمخاطر السيبرانية.
- إعداد خارطة طريق متقدمة لتطوير وتحول إدارة مخاطر الأمن السيبراني.
- المحاور التدريبية

## محاور الدورة

**اليوم الأول**

### استراتيجية وحوكمة إدارة مخاطر الأمن السيبراني المتقدمة

- تطور إدارة مخاطر الأمن السيبراني.
- مخاطر الأمن السيبراني باعتبارها مخاطر مؤسسية وتجارية.
- المخاطر السيبرانية الاستراتيجية والتشغيلية والمالية والتنظيمية والسمعة.
- هياكل حوكمة مخاطر الأمن السيبراني.
- أدوار ومسؤوليات الإدارة العليا ومالكي المخاطر وفرق الأمن.
- شهية المخاطر وحدود التحمل السيبراني.
- ملكية المخاطر والمساءلة.
- آليات تصعيد المخاطر واتخاذ القرارات.
- دمج الأمن السيبراني مع إدارة المخاطر المؤسسية.
- نماذج نضج إدارة مخاطر الأمن السيبراني.
- بناء برنامج لإدارة مخاطر الأمن السيبراني مرتبط بأهداف الأعمال.
- التطبيق العملي: تقييم مستوى نضج برنامج إدارة مخاطر الأمن السيبراني في مؤسسة افتراضية وإعداد خطة استراتيجية لتحسينه.

اليوم الثاني

## التقييم المتقدم وقياس مخاطر الأمن السيبراني

- منهجيات التقييم المتقدم لمخاطر الأمن السيبراني.
- أهمية الأصول وتحليل أثر الأعمال.
- تحليل التهديدات والثغرات ومستوى التعرض والنتائج المحتملة.
- تطوير سيناريوهات متقدمة للمخاطر السيبرانية.
- الأساليب النوعية والكمية لتقييم المخاطر.
- نمذجة الاحتمالية والأثر.
- تقدير الخسائر المالية والتشغيلية المحتملة.
- القياس الكمي للمخاطر بناءً على السيناريوهات.
- تحليل المخاطر المتبقية.
- تجميع المخاطر وتحليل المخاطر المترابطة.
- نماذج تصنيف وترتيب أولويات المخاطر السيبرانية.
- إعداد سجلات متقدمة لمخاطر الأمن السيبراني.
- التطبيق العملي: تطوير وقياس مجموعة من سيناريوهات المخاطر السيبرانية وإعداد سجل متقدم للمخاطر المؤسسية مرتب حسب الأولوية.

اليوم الثالث

## معلومات التهديدات والمخاطر الناشئة والتحليل المتقدم

- دمج معلومات التهديدات في إدارة المخاطر.
- قدرات الجهات المهاجمة ودوافعها وأهدافها.
- التهديدات المتقدمة والموجهة.

اليوم الثالث — تابع

- المخاطر القائمة على الهوية والصلاحيات.
- مخاطر الحوسبة السحابية والتحول الرقمي.
- مخاطر التطبيقات والبيانات.
- مخاطر الأطراف الثالثة وسلاسل التوريد.
- مخاطر الذكاء الاصطناعي والتقنيات الحديثة.
- التقنيات الناشئة وأس surfaces الهجوم الجديدة.
- المخاطر السيبرانية النظامية والمترابطة.
- تحليل السيناريوهات والتنبؤ بالمخاطر السيبرانية.
- تحديد التغيرات في مستوى التعرض السيبراني للمؤسسة.
- التطبيق العملي: تحليل سيناريو متقدم لتهديد سيبراني باستخدام معلومات التهديدات وتحديد أثره المحتمل على الخدمات المؤسسية الحيوية ومستوى التعرض للمخاطر.

**اليوم الرابع**

## معالجة المخاطر والاستثمار والمرونة السيبرانية

- استراتيجيات معالجة المخاطر السيبرانية المتقدمة.
- تجنب المخاطر وتقليلها ونقلها وقبولها.
- اختيار الضوابط الأمنية وفق المخاطر والقيمة المؤسسية.
- تقييم فعالية الضوابط الأمنية.
- إدارة المخاطر السيبرانية المتبقية.
- ترتيب أولويات الاستثمارات في الأمن السيبراني.
- تحليل التكلفة والعائد للضوابط الأمنية.
- اتخاذ القرارات المتعلقة بالبنية الأمنية وفق المخاطر.

اليوم الرابع — تابع

- المرونة السيبرانية وحماية الخدمات المؤسسية الحيوية.
- مخاطر الاستجابة للحوادث والتعافي منها.
- دمج استمرارية الأعمال والتعافي من الكوارث.
- تطوير محافظ متكاملة لمعالجة المخاطر السيبرانية.
- التطبيق العملي: ترتيب محفظة استثمارات للأمن السيبراني وفق مستوى التعرض للمخاطر وأثر الأعمال وفعالية الضوابط والموارد المتاحة.

**اليوم الخامس**

## التقارير التنفيذية والقياس والتحول في إدارة المخاطر

- إعداد تقارير مخاطر الأمن السيبراني للإدارة العليا ومجالس الإدارة.
- تحويل النتائج الفنية إلى لغة مخاطر مؤسسية.
- مؤشرات المخاطر الرئيسية ومؤشرات الأداء الأمني.
- لوحات المتابعة التنفيذية وعرض المخاطر بصورة واضحة.
- اتجاهات المخاطر وحدود التصعيد ومؤشرات الإنذار المبكر.
- مراقبة التغيرات في مستوى التعرض للمخاطر السيبرانية.
- ضمان مخاطر الأمن السيبراني والاستعداد للتدقيق.
- دمج مخاطر الأمن السيبراني في الحوكمة المؤسسية.
- قياس مستوى نضج إدارة مخاطر الأمن السيبراني.
- بناء نموذج التشغيل المستهدف.
- التحسين المستمر والإدارة الاستراتيجية للمخاطر.
- إعداد خارطة طريق للتحول في إدارة مخاطر الأمن السيبراني.

اليوم الخامس — تابع

- الورشة الختامية: إعداد إطار متكامل ومتقدم لإدارة مخاطر الأمن السيبراني يشمل الحوكمة، وشهية المخاطر، والتقييم، والقياس الكمي، ومعلومات التهديدات، والمخاطر الناشئة، ومعالجة المخاطر، وترتيب الاستثمارات، والمرونة السيبرانية، والتقارير التنفيذية، والقياس، وتقييم النضج، وخارطة طريق استراتيجية للتنفيذ والتطوير.

## للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: https://quest-training.com/courses/advanced-cybersecurity-risk-management-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440