تقييم وإدارة مخاطر الأمن السيبراني



لندن - المملكة المتحدة

07 - Dec 2026 - 11 - Dec 2026

$6,000

GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

المقدمة

في المشهد الرقمي المتطور باستمرار، تشكل التهديدات السيبرانية تحديًا مستمرًا للمؤسسات من جميع الأحجام. يعد اتباع نهج استباقي لتقييم وإدارة مخاطر الأمن السيبراني أمرًا ضروريًا لحماية البيانات الحساسة، وحماية البنية التحتية الحيوية، وضمان استمرارية الأعمال. يزود هذا البرنامج المكثف الذي يستمر خمسة أيام، والذي يقدمه مركز جينتكس للتدريب، المشاركين بالمعرفة والمهارات العملية اللازمة لتقييم مخاطر الأمن السيبراني بشكل فعال، وتطوير استراتيجيات تخفيف قوية، وتنفيذ إطار شامل لإدارة المخاطر. ومن خلال الاستكشاف الشامل لمنهجيات تقييم المخاطر الرئيسية وأفضل ممارسات الصناعة والتمارين العملية، يكتسب المشاركون القدرة على تحديد نقاط الضعف وتحديد أولويات المخاطر وبناء وضع قوي للأمن السيبراني داخل مؤسساتهم.

أهداف دورة تقييم وإدارة مخاطر الأمن السيبراني:

- إتقان المبادئ الأساسية لتقييم وإدارة مخاطر الأمن السيبراني.
- فهم مشهد التهديدات السيبرانية والأنواع المختلفة من الهجمات السيبرانية التي تواجهها المؤسسات.
- تحديد وتحليل نقاط الضعف في الأمن السيبراني داخل البنية التحتية لتكنولوجيا المعلومات وأنظمة البيانات في المؤسسة.
- تطبيق منهجيات تقييم المخاطر المتوافقة مع معايير الصناعة لتقييم احتمالية التهديدات السيبرانية وتأثيرها.
- وضع خطة شاملة لإدارة المخاطر لتحديد أولويات المخاطر وتخصيص الموارد وتنفيذ استراتيجيات التخفيف.

GENTEX® TRAINING CENTER

- استكشف أفضل الممارسات للاستجابة للحوادث والتعافي من الكوارث و التخطيط لاستمرارية الأعمال في حالة وقوع هجوم إلكتروني.

- الاستفادة من الأطر القانونية والتنظيمية ذات الصلة بإدارة مخاطر الأمن السيبراني.

- تحليل دراسات الحالة الواقعية لممارسات إدارة مخاطر الأمن السيبراني الناجحة وغير الناجحة.

- قم بصياغة خطة عمل مخصصة لتقييم وإدارة مخاطر الأمن السيبراني داخل مؤسستك.

منهجية الدورة

يستخدم هذا البرنامج التفاعلي نهجا يركز على المشاركين. فهو يمزج بين محاضرات خبراء الأمن السيبراني وورش العمل التفاعلية ودراسات الحالة الواقعية والمناقشات الجماعية والتمارين العملية. يشارك المشاركين بنشاط في إجراء تقييمات المخاطر، وتطوير خطط إدارة المخاطر، ومحاكاة سيناريوهات الاستجابة للحوادث، وصياغة خطط عمل لمعالجة مخاطر الأمن السيبراني المحددة داخل مؤسساتهم. من خلال التعلم التجريبي، يكتسب المشاركون المهارات العملية والمعرفة النظرية اللازمة ليصبحوا أبطال إدارة مخاطر الأمن السيبراني داخل مؤسساتهم، مما يضمن بيئة رقمية أكثر أمانًا ومرونة.

الفئات المستهدفة

- يسعى متخصصو أمن تكنولوجيا المعلومات ومسؤولو الأنظمة ومهندسو الشبكات إلى تعزيز مهاراتهم في تقييم مخاطر الأمن السيبراني وإدارتها.

- مديرو الأعمال ومديرو المشاريع وصناع القرار المسؤولون عن حماية الأصول التنظيمية والتخفيف من مخاطر الأمن السيبراني.

GENTEX® TRAINING CENTER

- يسعى مسؤولو الامتثال ومتخصصو إدارة المخاطر إلى دمج اعتبارات الأمن السيبراني في أطر إدارة المخاطر الشاملة الخاصة بهم.

- أي شخص مهتم بالفهم والمساهمة في بناء وضع قوي للأمن السيبراني لمؤسسته.

محتوى دورة تقييم وإدارة مخاطر الأمن السيبراني:

اليوم الأول: فهم المشهد: تحديد نقاط الضعف في الأمن السيبراني

- إزالة الغموض عن مخاطر الأمن السيبراني: المفاهيم الأساسية، ومشهد التهديد، وأنواع الهجمات السيبرانية

- تحديد نقاط الضعف وتحليلها: البنية التحتية للشبكة، وأنظمة البيانات، والعوامل البشرية

اليوم الثاني: تقييم المخاطر: منهجيات تقييم المخاطر المتوافقة مع معايير الصناعة

- استكشاف منهجيات تقييم المخاطر: AEMF تحليل وضع الفشل وتأثيره ، FSC TSIN إطار المعهد الوطني للمعايير والتكنولوجيا للأمن السيبراني

- إجراء تقييمات المخاطر وتقييم احتمالية وتأثير التهديدات السيبرانية

اليوم الثالث: بناء دفاع قوي: وضع خطة شاملة لإدارة المخاطر

- تحديد أولويات المخاطر وتخصيص الموارد: وضع خطة لإدارة المخاطر مع استراتيجيات التخفيف
- ضوابط التنفيذ: الضمانات الفنية والإدارية والمادية لمعالجة نقاط الضعف

اليوم الرابع: ما بعد الخرق: الاستجابة للحوادث، والتعافي من الكوارث، واستمرارية الأعمال

- التخطيط لما هو غير متوقع: تطوير خطة الاستجابة للحوادث واستراتيجية التعافي من الكوارث
- ضمان استمرارية الأعمال: تقليل وقت التوقف عن العمل والحفاظ على العمليات الحيوية بعد الهجوم الإلكتروني

اليوم الخامس: بناء مستقبل آمن: الاعتبارات القانونية وأفضل الممارسات وتخطيط العمل

- فهم الأطر القانونية والتنظيمية المتعلقة بالأمن السيبراني
- استكشاف أفضل الممارسات لإدارة المخاطر المستمرة والتحسين المستمر
- صياغة خطة عمل مخصصة لتنفيذ تقييم مخاطر الأمن السيبراني وإدارتها داخل مؤسستك

GENTEX® TRAINING CENTER

الخاتمة:

من خلال إكمال هذا البرنامج الشامل الذي يقدمه مركز جينتكس للتدريب بنجاح، يكتسب المشاركون المعرفة والمهارات العملية اللازمة للتنقل في العالم المعقد لتقييم وإدارة مخاطر الأمن السيبراني. وسيكونون مجهزين لتحديد ومعالجة الخروقات الأمنية المحتملة، وتحديد أولويات المخاطر السيبرانية بشكل فعال، والمساهمة في بناء وضع أمني سيبراني قوي ومرن داخل مؤسساتهم. وتمكنهم هذه المعرفة المعززة من أن يصبحوا مدافعين استباقيين في مكافحة التهديدات السيبرانية، وحماية الأصول القيمة وضمان استمرارية الأعمال في العصر الرقمي اليوم.

الأسئلة الشائعة:

السؤال الأول ما هي دورة تقييم وإدارة مخاطر الأمن السيبراني؟

تركز دورة تقييم وإدارة مخاطر الأمن السيبراني على تحديد وتحليل وإدارة المخاطر السيبرانية. وتشمل الدورة التهديدات السيبرانية، والثغرات الأمنية، ومنهجيات تقييم المخاطر، واستراتيجيات التخفيف، والاستجابة للحوادث، والتعافي من الكوارث، واستمرارية الأعمال، والجوانب القانونية والتنظيمية.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

السؤال الثاني ما هي الفوائد الرئيسية من دورة تقييم وإدارة مخاطر الأمن السيبراني؟

تساعد الدورة المشاركين على تحديد الثغرات الأمنية، وتقييم احتمالية وتأثير التهديدات السيبرانية، وترتيب المخاطر حسب الأولوية، ووضع خطط فعالة للتخفيف منها. كما تعزز قدرة المؤسسات على مواجهة الحوادث والتعافي من الكوارث والحفاظ على استمرارية الأعمال وإدارة المخاطر بشكل مستمر.

السؤال الثالث ما المهارات التي سأكتسبها من دورة تقييم وإدارة مخاطر الأمن السيبراني؟

سيكتسب المشاركون مهارات تقييم مخاطر الأمن السيبراني، وتحليل الثغرات الأمنية، وتخطيط إدارة المخاطر، والاستجابة للحوادث واستمرارية الأعمال. تدعم هذه المهارات تقييم المخاطر، وتحديد نقاط الضعف، ووضع خطط التخفيف، والاستعداد للحوادث، والحفاظ على العمليات الأساسية بعد الهجمات السيبرانية.

GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

السؤال الرابع ما الأدوات أو الأساليب أو المعايير التي تغطيها دورة تقييم وإدارة مخاطر الأمن السيبراني؟

تغطي الدورة منهجية تحليل أنماط وآثار الإخفاق AEMF وإطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا FSC TSIN لتقييم المخاطر. كما تتناول الضوابط التقنية والإدارية والمادية، وتخطيط الاستجابة للحوادث، والتعافي من الكوارث، واستراتيجيات استمرارية الأعمال.

السؤال الخامس كيف يتم تطبيق دورة تقييم وإدارة مخاطر الأمن السيبراني في الواقع العملي؟

يتم تطبيق إدارة المخاطر من خلال تقييمات عملية للمخاطر، وإعداد خطط لإدارتها، ومحاكاة سيناريوهات الاستجابة للحوادث، ودراسات الحالة الواقعية، ووضع خطط عمل. ويتدرب المشاركون على تحديد الثغرات، وتقييم التهديدات، وترتيب المخاطر، وتنفيذ الضوابط، والحفاظ على العمليات بعد الهجمات السيبرانية.

GENTEX®
TRAINING CENTER