الدورة التدريبية: إدارة مخاطر الأمن السيبراني: التقييم، التحليل، والمعالجة الشاملة



19 - 23 اكتوبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #SM5748_424097

مقدمة الدورة التدريبية / لمحة عامة:

في ظل المشهد الرقمي المتغير باستمرار، أصبحت إدارة مخاطر الأمن السيبراني: التقييم، التحليل، والمعالجة الشاملة ضرورة حتمية للمؤسسات التي تسعى لحماية أصولها وبياناتها الحساسة. هذه الدورة التدريبية المتعمقة مصممة لتزويد المشاركين بالمعرفة والمهارات المتقدمة لتحديد، تقييم، تحليل، ومعالجة المخاطر السيبرانية بشكل استباقي وفعال. من خلال التركيز على أحدث المنهجيات والأطر العالمية، سيتعلم المتدربون كيفية بناء برنامج شامل لإدارة المخاطر السيبرانية يتوافق مع أهداف الأعمال ويقلل من التعرض للتهديدات. تستند الدورة إلى أعمال خبراء رواد في مجال إدارة المخاطر، مثل الدكتور Carl Pritchard Carl Pritchard، الذي يقدم رؤى قيمة حول التخطيط للمخاطر وإدارتها. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من تطوير استراتيجيات قوية لإدارة المخاطر، وتنفيذ ضوابط أمنية فعالة، واتخاذ قرارات مستنيرة لحماية البنية التحتية الرقمية للمؤسسة. سنركز على الجوانب العملية، مع تقديم أمثلة واقعية ودراسات حالة تساعد المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم لتعزيز مرونة الأمن السيبراني.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو المخاطر الأمنية.
- محللو الأمن السيبراني.
- مديرو أمن المعلومات.
- مسؤولو الامتثال.
- مدققو أمن المعلومات.
- مهندسو الأمن.
- القادة وصناع القرار في تقنية المعلومات.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الرعاية الصحية.
- الحكومة والدفاع.
- قطاع الطاقة والمرافق.
- شركات الاتصالات.
- الشركات التكنولوجية.
- الاستشارات الأمنية.
- الشركات الصناعية الكبرى.

الأقسام المؤسسية المستهدفة:

- إدارة المخاطر.
- إدارة أمن المعلومات.
- إدارة تقنية المعلومات.
- قسم التدقيق الداخلي.
- قسم الامتثال.
- الإدارة العليا.
- إدارة العمليات.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- تحديد المخاطر السيبرانية المحتملة وتقييمها بدقة.
- تحليل تأثير المخاطر على العمليات التجارية والأصول.
- تطوير استراتيجيات فعالة لمعالجة المخاطر (القبول، التجنب، التخفيف، النقل).
- تنفيذ ضوابط أمنية لتقليل التعرض للمخاطر.
- مراقبة وتقييم المخاطر بشكل مستمر.
- بناء إطار عمل شامل لإدارة المخاطر السيبرانية.
- التعامل مع المخاطر الناشئة والتهديدات المتطورة.
- إعداد تقارير المخاطر وتقديم التوصيات للإدارة.

منهجية الدورة التدريبية:

تتبنى هذه الدورة التدريبية منهجية تفاعلية وعملية تهدف إلى تزويد المشاركين بفهم عميق ومهارات تطبيقية في مجال إدارة مخاطر الأمن السيبراني: التقييم، التحليل، والمعالجة الشاملة. تبدأ الدورة بمحاضرات متعمقة يقدمها خبراء متخصصون في إدارة المخاطر السيبرانية، تليها مناقشات جماعية بناءة لتبادل الأفكار والتحديات. يتم التركيز بشكل مكثف على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل سيناريوهات مخاطر سيبرانية معقدة، وتحديد العوامل المؤثرة، واقتراح استراتيجيات معالجة. تتضمن المنهجية ورش عمل تطبيقية تتيح للمتدربين استخدام أدوات تقييم المخاطر، وإعداد مصفوفات المخاطر، وتطوير خطط تخفيف المخاطر. يشجع BIG BEN Training Center المشاركة النشطة والعمل الجماعي لتعزيز التفكير النقدي وقدرات حل المشكلات. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مجهزون بالمعرفة والأدوات اللازمة لإدارة المخاطر السيبرانية بفعالية وكفاءة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مفاهيم وأسس إدارة مخاطر الأمن السيبراني

- مقدمة إلى إدارة المخاطر السيبرانية ودورها الاستراتيجي.
- أهمية تقييم المخاطر في تحديد الأولويات الأمنية.
- مفاهيم التهديد، الثغرة، والأثر.
- نماذج إدارة المخاطر (مثل NIST CSF، ISO 27005).
- مكونات إطار عمل إدارة المخاطر الشامل.
- التحديات الشائعة في إدارة المخاطر السيبرانية.
- دمج إدارة المخاطر مع أهداف الأعمال.

الوحدة الثانية: تحديد وتقييم المخاطر السيبرانية

- تحديد الأصول الهامة وتقدير قيمتها.
- تحديد التهديدات ونقاط الضعف المحتملة.
- منهجيات تقييم المخاطر (الكمية والنوعية).
- أدوات وتقنيات جمع البيانات للمخاطر.
- تحليل احتمالية وقوع الحوادث.
- تقدير الأثر المالي والتشغيلي والأخلاقي للمخاطر.
- تصنيف المخاطر وتحديد مستوياتها.

الوحدة الثالثة: تحليل المخاطر وتطوير استراتيجيات المعالجة

- تحليل المخاطر بناءً على الاحتمالية والأثر.
- تقنيات تحليل الثغرات الأمنية واختبار الاختراق.
- خيارات معالجة المخاطر (القبول، التجنب، التخفيف، النقل).
- تصميم وتنفيذ الضوابط الأمنية لتقليل المخاطر.
- تطوير خطط الاستجابة للحوادث كجزء من المعالجة.
- تحليل التكلفة والفائدة للضوابط الأمنية.
- بناء خطة شاملة لمعالجة المخاطر.

الوحدة الرابعة: مراقبة المخاطر وإعداد التقارير

- المراقبة المستمرة للمخاطر وتحديد المخاطر الناشئة.
- مؤشرات الأداء الرئيسية (KPIs) ومؤشرات المخاطر الرئيسية (KRIs).
- إعداد تقارير المخاطر للإدارة العليا وأصحاب المصلحة.
- التواصل الفعال حول حالة المخاطر.
- مراجعة وتقييم فعالية خطط معالجة المخاطر.
- إدارة سجلات المخاطر وتحديثها.
- أهمية التغذية الراجعة في دورة إدارة المخاطر.

الوحدة الخامسة: إدارة المخاطر المتقدمة والامتثال

- إدارة مخاطر سلسلة التوريد والأطراف الثالثة.
- إدارة مخاطر الامتثال للوائح (مثل GDPR، CCPA).
- أتمتة إدارة المخاطر (GRC tools).
- التعامل مع المخاطر البشرية والأمن السلوكي.
- مخاطر التقنيات الناشئة (الذكاء الاصطناعي، إنترنت الأشياء، الحوسبة السحابية).
- دراسات حالة متقدمة في إدارة المخاطر السيبرانية.
- التخطيط للمستقبل في مواجهة التهديدات المتغيرة.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

كيف يمكن للمؤسسات أن تضمن أن عملية إدارة المخاطر السيبرانية ليست مجرد وظيفة متفاعلة مع التهديدات، بل هي محرك استباقي للابتكار والنمو الآمن في البيئة الرقمية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل والعميق على إدارة مخاطر الأمن السيبراني: التقييم، التحليل، والمعالجة الشاملة، مما يميزها عن الدورات التي تقدم نظرة سطحية. نحن لا نكتفي بتقديم المفاهيم، بل نتعمق في المنهجيات والأدوات التي تمكن المشاركين من تطبيق إدارة المخاطر بفعالية في مؤسساتهم. تعتمد الدورة على نهج عملي مكثف، يتضمن دراسات حالة واقعية وورش عمل تفاعلية، مما يسمح للمتدربين بممارسة تقييم المخاطر، وتحليلها، وصياغة خطط معالجتها. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على دراية بأحدث التحديات والحلول في هذا المجال الحيوي. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء في إدارة المخاطر السيبرانية، قادرين على حماية أصول مؤسساتهم واتخاذ قرارات مستنيرة لتعزيز مرونة الأمن.