الدورة التدريبية: إدارة المخاطر السيبرانية والامتثال التنظيمي للمؤسسات



28 ديسمبر 2026 - 01 يناير 2027
بوسطن
7500 € (للشخص الواحد)
Ref: #IT6473_375775

مقدمة الدورة التدريبية / لمحة عامة:

في المشهد الرقمي المعاصر، أصبحت إدارة المخاطر السيبرانية والامتثال التنظيمي من أهم الأولويات الاستراتيجية للمؤسسات على اختلاف أحجامها وقطاعاتها. مع التطور المستمر للتهديدات السيبرانية وتزايد حجم التعقيدات القانونية والتنظيمية، تواجه الشركات تحدياً متزايداً في حماية أصولها الرقمية وضمان الالتزام بالمعايير والمتطلبات. هذه الدورة التدريبية مصممة لتزويد المشاركين بالمعرفة والأدوات اللازمة لفهم وتقييم وإدارة المخاطر السيبرانية بفعالية، بالإضافة إلى بناء برامج امتثال قوية تضمن تلبية المتطلبات التنظيمية المحلية والدولية. سنغطي منهجيات تحديد المخاطر، تحليل الثغرات، ووضع خطط للتخفيف من حدتها، مع التركيز على أهمية الحوكمة الرشيدة في هذا المجال. يؤكد البروفيسور ويليام إدواردز ديمينج (W. Edwards Deming)، أحد رواد إدارة الجودة، أن "التحسين المستمر ليس أمراً اختيارياً، بل هو ضرورة للبقاء في عالم اليوم". يلتزم BIG BEN Training Center بتقديم تدريب متكامل يجمع بين النظريات المتقدمة والتطبيقات العملية، لتمكين قادة الأمن ومتخصصي الامتثال من بناء بيئات رقمية آمنة، وتقليل التعرض للمخاطر، وتعزيز الثقة والشفافية في عملياتهم.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء أمن المعلومات.
- مسؤولو المخاطر والامتثال.
- مدققو نظم المعلومات.
- المستشارون في الأمن السيبراني.
- مدراء تقنية المعلومات.
- مدراء الحوكمة المؤسسية.
- المحامون والمتخصصون القانونيون في المجال الرقمي.
- المتخصصون في إدارة استمرارية الأعمال.
- قادة الأعمال والمدراء التنفيذيون.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الاتصالات وتقنية المعلومات.
- القطاع الحكومي والجهات التنظيمية.
- قطاع الرعاية الصحية.
- شركات التأمين.
- شركات الطاقة والمرافق.
- الشركات الكبرى والمتعددة الجنسيات.
- شركات الاستشارات الأمنية والقانونية.
- الشركات الناشئة التقنية.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات.
- أقسام إدارة المخاطر.
- أقسام الامتثال (Compliance).
- أقسام التدقيق الداخلي والخارجي.
- الأقسام القانونية.
- أقسام تقنية المعلومات.
- أقسام الحوكمة المؤسسية.
- أقسام التخطيط الاستراتيجي.

أهداف الدورة التدريبية:

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

- تحديد وتقييم وإدارة المخاطر السيبرانية للمؤسسة.
- فهم وتطبيق الأطر والمعايير الدولية لإدارة المخاطر.
- بناء وتطبيق برامج الامتثال التنظيمي الفعالة.
- التعامل مع التشريعات واللوائح المتعلقة بأمن المعلومات والخصوصية.
- إعداد وتنفيذ خطط الاستجابة للحوادث الأمنية.
- تحليل الثغرات الأمنية ونقاط الضعف في الأنظمة.
- تطوير سياسات وإجراءات أمنية متوافقة مع المتطلبات.
- قياس فعالية برامج إدارة المخاطر والامتثال.
- تعزيز ثقافة الوعي بالمخاطر الأمنية داخل المؤسسة.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة التدريبية على منهجية متقدمة تجمع بين الفهم النظري العميق لإدارة المخاطر السيبرانية والامتثال التنظيمي والتطبيق العملي المكثف. تتضمن المنهجية محاضرات تفاعلية يقدمها خبراء في الأمن السيبراني وإدارة المخاطر والقانون الرقمي، مع التركيز على أحدث التهديدات وأفضل الممارسات. سيشارك المتدربون في ورش عمل عملية تستعرض سيناريوهات واقعية لتقييم المخاطر، وتحليل الثغرات، وتطوير خطط المعالجة. كما سيتم التطرق إلى دراسات حالة لأمثلة ناجحة وفاشلة في إدارة المخاطر والامتثال، مما يمنح المشاركين رؤى عملية حول التحديات وكيفية التغلب عليها. يتم تشجيع العمل الجماعي والمناقشات لتبادل الخبرات وتطوير حلول مبتكرة. الهدف هو تزويد المشاركين بالقدرة على تحديد وتقييم المخاطر، ووضع استراتيجيات فعالة للتخفيف منها، وضمان الامتثال الصارم للمتطلبات التنظيمية، مما يعزز المرونة الأمنية للمؤسسات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات المخاطر السيبرانية وإطارها العام.

- مقدمة في المخاطر السيبرانية وأنواعها.
- مفاهيم التهديد، ونقاط الضعف، والأثر.
- منهجيات تقييم المخاطر (Qualitative and Quantitative).
- تحديد الأصول الحيوية للمؤسسة.
- مراحل دورة حياة إدارة المخاطر.
- تحليل سيناريوهات المخاطر السيبرانية.
- أهمية سجل المخاطر.

الوحدة الثانية: أطر إدارة المخاطر السيبرانية والمعايير الدولية.

- إطار NIST للتحكم في الأمن السيبراني.
- معيار ISO 27005 لإدارة مخاطر أمن المعلومات.
- إطار COBIT لإدارة وحوكمة تكنولوجيا المعلومات.
- إدارة مخاطر الطرف الثالث (Third-Party Risk Management).
- أدوات وتقنيات تقييم المخاطر.
- التحكم في المخاطر: التخفيف، القبول، التحويل، التجنب.
- قياس مؤشرات الأداء الرئيسية (KPIs) للمخاطر.

الوحدة الثالثة: الامتثال التنظيمي وقوانين حماية البيانات.

- مقدمة في الامتثال التنظيمي وأهميته.
- اللائحة العامة لحماية البيانات (GDPR) ومتطلباتها.
- قوانين حماية البيانات والخصوصية المحلية والدولية.
- الامتثال لمعايير الصناعة (PCI DSS، HIPAA).
- دور الهيئات التنظيمية والتدقيق.
- إعداد برامج الامتثال الداخلية.
- سياسات وإجراءات الامتثال.

الوحدة الرابعة: تنفيذ برامج إدارة المخاطر والامتثال.

- بناء فريق إدارة المخاطر والامتثال.
- دمج إدارة المخاطر في دورة حياة التطوير.
- إعداد خطط الاستجابة للحوادث السيبرانية.
- التدقيق الأمني واختبار الاختراق.
- التوعية والتدريب على الأمن السيبراني.
- إدارة التغيير في بيئة المخاطر والامتثال.
- التقارير والإبلاغ عن المخاطر.

الوحدة الخامسة: التحديات المتقدمة والاتجاهات المستقبلية.

- المخاطر السيبرانية في الحوسبة السحابية.
- الذكاء الاصطناعي في إدارة المخاطر والامتثال.
- مخاطر إنترنت الأشياء (IoT).
- سلاسل الكتل (Blockchain) وأثرها على الأمن.
- التحديات القانونية والتنظيمية الجديدة.
- تطور الهجمات السيبرانية (APTs، Ransomware).
- المرونة السيبرانية (Cyber Resilience).

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:

في ظل مشهد التهديدات السيبرانية المتطور باستمرار والمتطلبات التنظيمية المتزايدة، كيف يمكن للمؤسسات أن تبتعد عن نهج الامتثال القائم على "وضع العلامات في المربعات" وتتبنى استراتيجية شاملة لإدارة المخاطر السيبرانية تركز على القيمة وتدعم الابتكار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها منهجاً فريداً يجمع بين إدارة المخاطر السيبرانية والامتثال التنظيمي في سياق متكامل، مما يميزها عن الدورات التي تركز على أحد الجانبين فقط. نحن لا نقدم مجرد معلومات حول التهديدات أو اللوائح، بل نركز على تمكين المشاركين من بناء استراتيجيات شاملة لحماية مؤسساتهم وضمان التزامها. ترتكز الدورة على دراسات حالة واقعية وأمثلة عملية من مختلف القطاعات، مما يمنح المشاركين فهماً عميقاً للتحديات والحلول المطبقة في العالم الحقيقي. كما نغطي أحدث المعايير والأطر العالمية، مع التركيز على كيفية تكييفها مع البيئات المؤسسية المختلفة. إن هذا المزيج الفريد من المعرفة النظرية المتقدمة والتدريب العملي المكثف، بالإضافة إلى التركيز على التفكير الاستراتيجي في الأمن، يضمن للمشاركين اكتساب المهارات اللازمة لقيادة جهود إدارة المخاطر والامتثال بفعالية وثقة.