الدورة التدريبية: إدارة المخاطر والأمن الرقمي في مشاريع التحول: بناء المرونة والثقة



19 - 23 اكتوبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #DT4643_421049

مقدمة الدورة التدريبية / لمحة عامة:

مع تسارع وتيرة التحول الرقمي في المؤسسات، تزداد أهمية إدارة المخاطر والأمن الرقمي كعنصر حاسم لنجاح أي مشروع تحول. لم يعد كافياً التركيز على تبني التقنيات الحديثة، بل يجب أن يترافق ذلك مع استراتيجيات قوية لحماية الأصول الرقمية وضمان استمرارية الأعمال. تقدم هذه الدورة التدريبية الشاملة من BIG BEN Training Center برنامجاً متكاملاً مصمماً لتزويد المشاركين بالمعرفة والأدوات اللازمة لتقييم المخاطر السيبرانية، تطبيق تدابير الأمن السيبراني، وإدارة التهديدات الرقمية بفعالية عبر جميع مراحل مشاريع التحول. سنتناول كيفية بناء مرونة سيبرانية، والامتثال للوائح والمعايير العالمية، ودمج الأمن في تصميم البنية التحتية والحلول الرقمية. ستركز الدورة على أهمية التفكير الاستباقي في أمن المعلومات، وحماية البيانات، والاستجابة للحوادث السيبرانية. تهدف الدورة إلى تمكين القادة والمهنيين من قيادة مشاريع التحول الرقمي بثقة، مع ضمان حماية المؤسسة من التهديدات المتزايدة. يؤكد البروفيسور هوارد شميدت (Howard Schmidt)، خبير الأمن السيبراني والرئيس السابق للمجلس الاستشاري للأمن السيبراني للرئيس الأمريكي، في أعماله على أن الأمن يجب أن يكون جزءاً لا يتجزأ من التخطيط لأي مبادرة رقمية، وليس مجرد إضافة لاحقة. يقدم BIG BEN Training Center هذه الدورة لتمكين المشاركين من فهم الأمن السيبراني المؤسسي، وإدارة مخاطر التحول الرقمي، وحماية البيانات الرقمية، والامتثال الأمني للتقنيات الجديدة، والمرونة السيبرانية للشركات، والاستجابة للحوادث السيبرانية، وأمن البنية التحتية الرقمية، والسياسات الأمنية للتحول الرقمي، والتهديدات السيبرانية الناشئة، والاستراتيجيات الدفاعية الرقمية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء تقنية المعلومات (CIOs).
- مدراء الأمن السيبراني (CISOs).
- مدراء المشاريع الرقمية.
- محللو المخاطر.
- مهندسو الأمن.
- مدراء الامتثال والتدقيق.
- أعضاء فرق التحول الرقمي.
- المدراء التنفيذيون المعنيون بالاستراتيجيات الرقمية.
- استشاريو الأمن وتقنية المعلومات.
- أي شخص مسؤول عن حماية الأصول الرقمية للمؤسسة.

القطاعات والصناعات المستهدفة:

- جميع القطاعات والصناعات التي تمر بتحول رقمي.
- القطاع المصرفي والمالي.
- قطاع الاتصالات.
- قطاع الرعاية الصحية.
- الجهات الحكومية والمؤسسات العامة.
- شركات التكنولوجيا والبرمجيات.
- قطاع التصنيع (الصناعة 4.0).
- شركات الخدمات اللوجستية.
- قطاع الطاقة.
- شركات التأمين.

الأقسام المؤسسية المستهدفة:

- قسم تقنية المعلومات.
- قسم الأمن السيبراني.
- إدارة المخاطر.
- قسم الامتثال والتدقيق.
- إدارة المشاريع.
- إدارة التحول الرقمي.
- القسم القانوني.
- إدارة العمليات.
- الموارد البشرية (في سياق التوعية الأمنية).
- إدارة الاستمرارية والأزمات.

أهداف الدورة التدريبية:

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

- فهم العلاقة بين التحول الرقمي والأمن الرقمي.
- تحديد وتقييم المخاطر السيبرانية المرتبطة بمشاريع التحول.
- تطبيق أفضل الممارسات في حماية البيانات الرقمية والأصول الحيوية.
- وضع سياسات أمنية للتحول الرقمي تضمن الامتثال للوائح.
- بناء المرونة السيبرانية للشركات والاستعداد للاستجابة للحوادث.
- إدارة التهديدات السيبرانية الناشئة بشكل استباقي.
- دمج اعتبارات الأمن في تصميم البنية التحتية الرقمية.
- تطوير خطط الاستجابة للحوادث السيبرانية والتعافي من الكوارث.
- تعزيز ثقافة الأمن السيبراني المؤسسي بين الموظفين.
- قيادة مشاريع التحول الرقمي مع التركيز على الأمن السيبراني كأولوية.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة التدريبية على منهجية تعليمية مكثفة وتطبيقية، تجمع بين الجوانب النظرية والتجارب العملية لضمان فهم عميق لإدارة المخاطر والأمن الرقمي في مشاريع التحول. تتضمن المنهجية جلسات تفاعلية، وتحليل دراسات حالة واقعية لانتهاكات أمنية ومشاريع تحول، وورش عمل عملية تتيح للمشاركين فرصة تقييم المخاطر السيبرانية، وتصميم تدابير الأمن السيبراني، وتطوير خطط الاستجابة للحوادث السيبرانية. سيتم التركيز على حماية البيانات الرقمية، والامتثال الأمني للتقنيات الجديدة، والمرونة السيبرانية للشركات. يقدم المدربون الخبراء، من ذوي الخبرة الواسعة في الأمن السيبراني والتحول الرقمي، إرشادات مستمرة وتغذية راجعة بناءة. تهدف المنهجية إلى تمكين المتدربين من فهم عميق لأمن البنية التحتية الرقمية، والسياسات الأمنية للتحول الرقمي، والتهديدات السيبرانية الناشئة، والاستراتيجيات الدفاعية الرقمية، مما يؤهلهم لقيادة مشاريع التحول بثقة وأمان.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أسس الأمن الرقمي وإدارة المخاطر في التحول الرقمي

- مقدمة إلى الأمن الرقمي وإدارة المخاطر في العصر الرقمي.
- تحديات وفرص التحول الرقمي من منظور الأمن.
- مفاهيم المخاطر السيبرانية والتهديدات الشائعة.
- الأصول الرقمية الحيوية وكيفية تحديدها.
- أهمية دمج الأمن منذ بداية التخطيط للمشاريع الرقمية.
- مبادئ حماية البيانات والخصوصية.
- اللوائح والمعايير الدولية للأمن السيبراني (GDPR, ISO 27001).

الوحدة الثانية: تقييم المخاطر وتطوير استراتيجيات الأمن السيبراني

- منهجيات تقييم المخاطر السيبرانية (Risk Assessment).
- تحديد الثغرات ونقاط الضعف في الأنظمة الرقمية.
- تطوير استراتيجيات الأمن السيبراني المؤسسي.
- تصميم ضوابط الأمن الوقائية والاستكشافية.
- إدارة التهديدات الرقمية ونماذج الهجوم.
- تحليل المخاطر الكمي والنوعي.
- ورشة عمل: بناء مصفوفة مخاطر لمشروع تحول رقمي.

الوحدة الثالثة: حماية البنية التحتية والبيانات الرقمية

- أمن البنية التحتية الرقمية: الشبكات، الخوادم، والخدمات السحابية.
- أمن تطبيقات الويب والهواتف المحمولة.
- حماية البيانات الرقمية في التخزين والنقل.
- التشفير وإدارة المفاتيح.
- أمن الهوية والوصول (IAM).
- التحكم في الوصول والصلاحيات.
- دراسة حالة: تأمين بيئة سحابية لمشروع رقمي.

الوحدة الرابعة: الامتثال، الاستجابة للحوادث، والمرونة السيبرانية

- الامتثال الأمني للتقنيات الجديدة والمتطلبات القانونية.
- خطط الاستجابة للحوادث السيبرانية والتعافي من الكوارث.
- تطوير فرق الاستجابة للحوادث.
- المرونة السيبرانية للشركات (Cyber Resilience).
- إدارة الأزمات الأمنية والتواصل.
- الاختبارات الأمنية (Penetration Testing) والتدقيق.
- سيناريوهات الهجوم والدفاع.

الوحدة الخامسة: قيادة الأمن الرقمي وثقافة الأمن المؤسسي

- دور القيادة في تعزيز الأمن السيبراني المؤسسي.
- بناء ثقافة الأمن الرقمي بين الموظفين.
- برامج التوعية والتدريب على الأمن.
- إدارة أصحاب المصلحة في قضايا الأمن.
- مستقبل التهديدات السيبرانية الناشئة والاستراتيجيات الدفاعية الرقمية.
- الابتكار في الأمن الرقمي.
- صياغة خارطة طريق شاملة لإدارة المخاطر والأمن في المؤسسة.

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 التطور المتسارع للتهديدات السيبرانية الناشئة وتعقيد مشاريع التحول الرقمي، كيف يمكن للمؤسسات تحقيق التوازن الأمثل بين الابتكار السريع في تبني التقنيات الجديدة والحفاظ على مستويات عالية من الأمن السيبراني المؤسسي، مع ضمان استمرارية الأعمال وبناء المرونة السيبرانية الفعالة على المدى الطويل؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية من BIG BEN Training Center بتركيزها الفريد على إدارة المخاطر والأمن الرقمي في مشاريع التحول، مما يجعلها مختلفة عن الدورات العامة في الأمن السيبراني. نحن نقدم نهجاً عملياً يدمج الأمن كعنصر أساسي في كل مراحل التحول الرقمي، مع التركيز على تقييم المخاطر السيبرانية، وحماية البيانات الرقمية، وتطبيق تدابير الأمن السيبراني المتقدمة. لا تكتفي الدورة بتقديم المفاهيم، بل تركز على تزويد المشاركين بأدوات فعالة لإدارة التهديدات الرقمية، وبناء المرونة السيبرانية للشركات، وتطوير خطط الاستجابة للحوادث السيبرانية. إن هذا المزيج الفريد من المحتوى العميق، والمنهجية التطبيقية، ودراسات الحالة الواقعية، بالإضافة إلى التركيز على أمن البنية التحتية الرقمية والسياسات الأمنية للتحول الرقمي، يجعلها الخيار الأمثل للمحترفين الذين يسعون لقيادة مشاريع التحول الرقمي بأمان وفعالية.