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

يونيو ٢٠٢٦ ٠٥ - ٠١

كيب تاون - *

(للشخص الواحد) ٦٠٠٠ €

Ref: #DT4643_563130

مقدمة الدورة التدريبية / لمحة عامة:

يعد كافياً التركيز على أهمية إدارة المخاطر والأمن الرقمي كعنصر حاسم مع تسارع وتيرة التحول الرقمي في المؤسسات، تزداد استراتيجيات قوية لحماية الأصول الرقمية وضمان تبني التقنيات الحديثة، بل يجب أن يترافق ذلك مع لنجاح أي مشروع تحول. لم لتزويد المشاركين بالمعرفة الشاملة من BIG BEN Training Center برنامجاً استمرارية الأعمال. تقدم هذه الدورة التدريبية سنتناول تدابير الأمن السيبراني، وإدارة التهديدات الرقمية والأدوات اللازمة لتقييم المخاطر السيبرانية، تطبيق متكاملاً مصمماً العالمية، ودمج الأمن في تصميم البنية كيفية بناء مرونة سيبرانية، والامتثال للوائح بفعالية عبر جميع مراحل مشاريع التحول.

تهدف التفكير الاستباقي في أمن المعلومات، وحماية التحتية والحلول الرقمية. ستركز الدورة على أهمية والمعايير مع ضمان حماية المؤسسة من الدورة إلى تمكين القادة والمهنيين من قيادة مشاريع البيانات، والاستجابة للحوادث السيبرانية. خبير الأمن السيبراني والرئيس(Howard Schmidt) التهديدات المتزايدة. يؤكد البروفيسور هوارد شميدت التحول الرقمي بثقة، مبادرة رقمية، وليس الأمريكي، في أعماله على أن الأمن يجب أن يكون السابق للمجلس الاستشاري للأمن السيبراني للرئيس، الدورة لتمكين المشاركين من فهم الأمن مجرد إضافة لاحقة. يقدم BIG BEN Training Center جزءاً لا يتجزأ من التخطيط لأي السيبرانية للشركات، وحماية البيانات الرقمية، والامتثال الأمني السيبراني المؤسسي، وإدارة مخاطر التحول الرقمي، هذه الجديدة، والمرونة

والاستراتيجيات التحتية الرقمية، والسياسات الأمنية للتحول الرقمي، والاستجابة للحوادث السيبرانية، وأمن البنية للتقنيات الدفاعية الرقمية. والتهديدات السيبرانية الناشئة،

لـ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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 ٤.٠).
- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

التحول الرقمي الوحدة الأولى: أسس الأمن الرقمي وإدارة المخاطر في

- الرقمي.ٔ مقدمة إلى الأمن الرقمي وإدارة المخاطر في العصر
- تحديات وفرص التحول الرقمي من منظور الأمن.ٔ
- مفاهيم المخاطر السيبرانية والتهديدات الشائعة.ٔ
- الأصول الرقمية الحيوية وكيفية تحديدها.ٔ
- الرقمية.ٔ أهمية دمج الأمن منذ بداية التخطيط للمشاريع
- مبادئ حماية البيانات والخصوصية.ٔ
- .ٔ(ISO ٢٧٠٠١ اللوائح والمعايير الدولية للأمن السيبراني (GDPR,

الأمن السيبراني الوحدة الثانية: تقييم المخاطر وتطوير استراتيجيات

- .ٔ(Assessment منهجيات تقييم المخاطر السيبرانية (Risk
- 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.ٔ

الرقمية الوحدة الثالثة: حماية البنية التحتية والبيانات

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

والمرونة السيبرانية الوحدة الرابعة: الامتثال، الاستجابة للحوادث،

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

المؤسسي الوحدة الخامسة: قيادة الأمن الرقمي وثقافة الأمن

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

الأسئلة المتكررة:ا

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

لا توجد شروط مسبقة.ا

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

التوازن الأمثل بين الابتكار الناشئة وتعقيد مشاريع التحول الرقمي، كيف يمكن في ظل التطور المتسارع للتهديدات السيبرانية

مستويات عالية من الأمن السيبراني المؤسسي، مع ضمان السريع في تبني التقنيات الجديدة والحفاظ على للمؤسسات تحقيق

الفعالة على المدى الطويل؟ استمرارية الأعمال وبناء المرونة السيبرانية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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