الدورة التدريبية: تدقيق الأمن السيبراني وحماية البيانات



28 ديسمبر 2026 - 01 يناير 2027
بوسطن
7500 € (للشخص الواحد)
Ref: #GRC9339_384577

مقدمة الدورة التدريبية / لمحة عامة:

تم تصميم هذه الدورة التدريبية في تدقيق الأمن السيبراني وحماية البيانات لتزويد المشاركين بالمعرفة العميقة والمهارات العملية اللازمة لضمان أمن المعلومات وتحقيق حماية فعالة للبيانات في المؤسسات. خلال الدورة، سيكتسب المتدربون فهمًا شاملاً لتقييم المخاطر السيبرانية، وتدقيق الضوابط التقنية، وتحليل الفجوات الأمنية وفق معايير معترف بها مثل ISO 27007 وNIST. سيتعلم المشاركون كيفية إعداد تقارير تدقيق مفصلة تشمل توصيات لتعزيز حماية البيانات وامتثالها للمتطلبات التنظيمية مثل GDPR. تُقدم الدورة بأسلوب تفاعلي يجمع بين دراسة الحالات الواقعية والمحاكاة، مما يضمن قدرة المشاركين على تنفيذ إجراءات فعالة لحماية البيانات داخل بيئاتهم المؤسسية. تقدم BIG BEN Training Center هذه الدورة بطريقة احترافية موجهة للشركات والمؤسسات التي تسعى لتعزيز حوكمة أمن المعلومات وتحقيق الامتثال التنظيمي، مع التركيز على الجوانب الفريدة مثل تحليل نقاط الضعف والمراجعة الفنية المتقدمة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو أمن المعلومات.
- مدققو نظم المعلومات.
- مسؤولو امتثال وحوكمة البيانات.
- مسؤولو تقنية المعلومات.
- موظفو الأمن السيبراني.
- محللو المخاطر السيبرانية.
- فرق استجابة الحوادث.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- قطاع الرعاية الصحية.
- شركات تكنولوجيا المعلومات والاتصالات.
- المؤسسات الحكومية والجهات الرقابية.
- الهيئات الحكومية وما في حكمها.

الأقسام المؤسسية المستهدفة:

- قسم تقنية المعلومات.
- قسم نظم المعلومات.
- قسم الامتثال والسلامة التنظيمية.
- قسم إدارة المخاطر وحوكمة البيانات.
- قسم الأمن والسجلات.

أهداف الدورة التدريبية:

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

- إجراء تدقيق الأمن السيبراني باستخدام معايير ISO 27007.
- تحليل المخاطر وتقييم الضوابط الأمنية.
- إعداد تقارير تدقيق فنية شاملة وحلول حماية البيانات.
- تطبيق إجراءات تدقيق امتثال GDPR والسياسات.
- تنفيذ تقييمات نقاط الضعف واستخدام إطار NIST.
- تصميم خطة استجابة للحوادث السيبرانية.
- مراجعة أمن الشبكات وقواعد البيانات داخل المؤسسات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على أساليب فعّالة في التعلم تشمل دراسات حالة حقيقية في مجال حماية البيانات وتقييم الأمان، وأنشطة جماعية لتحليل مخاطر المؤسسات، وجلسات تفاعلية لاستكشاف الضوابط التقنية، بالإضافة إلى جلسات تغذية راجعة من خبراء أمن المعلومات. تُستخدم أدوات تحليل الضوابط والحماية العملية لضمان نقل المعرفة بشكل تطبيقي، وتعزيز قدرات المشاركين على تنمية ثقافة أمنية مؤسسية قوية، مما يعزز التفاعل والفائدة للجهات المشاركة ويضمن نتائج ملموسة معتمدة على تقنيات تدقيق معترف بها دولياً.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات تدقيق الأمن السيبراني وحماية البيانات:

- تعريف تدقيق الأمن السيبراني والحوكمة.
- معايير ISO 27007 وأهميتها في تقييم الأمان.
- فهم إطار NIST للأمن السيبراني.
- تحليل المخاطر وتقييم الضوابط الأساسية.
- حماية البيانات الشخصية وامتثال GDPR.
- عمليات مراجعة حماية قواعد البيانات.
- كيفية إعداد تقرير تدقيق أولي.

الوحدة الثانية: تدقيق الضوابط التقنية وتقنيات الأمان:

- تقييم أمان الشبكات والبنية التحتية.
- تحليل نقاط الضعف واستخدام أدوات متخصصة.
- تدقيق نظام إدارة الوصول والتحكم.
- مراجعة التشفير وتطبيقه لحماية البيانات.
- حماية الأنظمة السحابية وتدقيقها.
- تحليل التحكم في الهوية وإدارة الحقوق.
- إعداد توصيات لتحسين الضوابط التقنية.

الوحدة الثالثة: تدقيق الامتثال والتشريعات القانونية:

- إطار GDPR وحماية الخصوصية.
- متطلبات التوافق التنظيمي والدوري.
- تقييم سياسة حماية البيانات في المؤسسات.
- مراجعة حوكمة البيانات والضمان الرقابي.
- تحليل الاتفاقيات مع الأطراف الخارجية.
- إدارة التوثيق أثناء عمليات التدقيق.
- إعداد تقييم شامل للامتثال القانوني.

الوحدة الرابعة: استجابة الحوادث وتحليل المخاطر المتقدمة:

- تصميم خطة استجابة للحوادث السيبرانية.
- تقنيات التحقيق الرقمي وتحليل الأدلة.
- مراجعة عمليات الكشف المبكر عن التهديدات.
- تحليل سيناريوهات الاختراق والتعافي.
- تقييم جاهزية SOC للرد على الحوادث.
- إعداد تقرير تحليل الحوادث وخطة التعافي.
- جلسة محاكاة واقعية للحوادث السيبرانية.

الوحدة الخامسة: التكامل المؤسسي والتوصيات التنفيذية:

- إعداد تقرير تدقيق نهائي للمؤسسة.
- تقديم توصيات تعزيز حماية البيانات.
- وضع خطة تحسين على المدى الطويل.
- مراجعة حالات دراسية متقدمة.
- تحديد مؤشرات الأداء الأمنية (KPIs).
- خطوات متابعة التنفيذ بعد التدقيق.
- خريطة طريق لحوكمة أمن مستدامة.

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 يمكننا قياس فعالية الضوابط الأمنية بعد تطبيقها في بيئة مؤسسية متعددة القنوات؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية في تدقيق الأمن السيبراني وحماية البيانات بتقديم تجربة تعليمية مصممة خصيصًا للشركات، تجمع بين الأمور النظرية والتطبيق العملي الفوري اعتمادًا على كلمات مثل تحليل المخاطر السيبرانية وتقييم الضوابط التقنية. تركز الدورة على استخدام معايير معترف بها دوليًا مثل ISO 27007 وNIST، مع تقديم دراسات حالة حقيقية من بيئات شركات فعلية تشمل الجوانب الفنية والتنظيمية. تقدم BIG BEN Training Center مشهدًا شاملاً يشمل إعداد تقارير تدقيق تنفيذية وتوصيات قابلة للتطبيق، مما [illegible] للمشاركين ليس فقط فهم التهديدات، بل تصميم وتنفيذ إجراءات حماية فعّالة. علاوة على ذلك، تُجرى محاكاة حوادث واقعية لتدريب الفرق على رد الفعل السريع والتعافي، مع تطوير خطة مستدامة لحوكمة أمن المعلومات تعتمد على مؤشرات أداء واضحة. كل هذا يتم ضمن منهج تطبيقي يضمن انتقال المعرفة مباشرة إلى المؤسسة، دون الاعتماد على أدوات، بل باستخدام رؤى عملية تؤهل الفرق لبناء دفاع سيبراني متكامل وقابل للتكيف مع تطورات البيئة الرقمية.