الدورة التدريبية: إدارة عقود الأمن السيبراني وحماية البيانات: التحديات والحلول القانونية والتقنية



09 - 13 نوفمبر 2026
الدار البيضاء
4500 € (للشخص الواحد)
Ref: #CM3860_418608

مقدمة الدورة التدريبية / لمحة عامة:

في العصر الرقمي الحالي، حيث تتزايد التهديدات السيبرانية وتُصبح حماية البيانات أمرًا حيويًا لبقاء ونجاح أي مؤسسة، تُعد إدارة عقود الأمن السيبراني من التخصصات بالغة الأهمية. إن التعقيد المتزايد للهجمات الإلكترونية، وتنامي حجم البيانات الحساسة التي تتم معالجتها، والتشريعات الصارمة مثل اللائحة العامة لحماية البيانات (GDPR)، جعلت من الضروري للشركات إتقان الجوانب القانونية والتقنية لعقود الأمن السيبراني وحماية البيانات. تقدم هذه الدورة التدريبية الشاملة من BIG BEN Training Center منهجًا متكاملًا لإدارة عقود الأمن السيبراني وحماية البيانات، بدءًا من صياغة اتفاقيات الخدمة الأمنية، مرورًا بالتعامل مع بنود الامتثال للوائح حماية البيانات، وصولًا إلى إدارة الاستجابة للحوادث السيبرانية ومسؤولية الأطراف. سيتعلم المشاركون كيفية هيكلة عقود الأمن السيبراني، والتفاوض على الشروط الأساسية، وتطبيق أفضل الممارسات لضمان حماية الأصول الرقمية والامتثال القانوني، مع تحقيق أقصى درجات الأمان والفعالية. تستند هذه الدورة إلى أحدث المعايير الدولية في الأمن السيبراني وقانون حماية البيانات، مستلهمة من أعمال خبراء مرموقين مثل البروفيسور دانييل ج. سولوف (Daniel J. Solove)، الذي يُعد مرجعًا في مجال قانون الخصوصية والبيانات. يهدف BIG BEN Training Center من خلال هذه الدورة إلى تمكين المهنيين من إتقان إدارة عقود الأمن السيبراني وحماية البيانات، وتعزيز المرونة السيبرانية، وضمان الامتثال القانوني في بيئة رقمية متغيرة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء الأمن السيبراني.
- المستشارون القانونيون في تكنولوجيا المعلومات.
- مدراء العقود والمشتريات في الشركات التقنية.
- مدراء تكنولوجيا المعلومات.
- خبراء حماية البيانات (DPOs).
- المسؤولون عن الامتثال وحوكمة الشركات.
- مدراء المخاطر.
- المدراء التنفيذيون في الشركات التي تتعامل مع بيانات حساسة.
- المهندسون الأمنيون.
- المدققون في مجال تكنولوجيا المعلومات.

القطاعات والصناعات المستهدفة:

- قطاع تكنولوجيا المعلومات والاتصالات.
- الخدمات المصرفية والمالية.
- الرعاية الصحية والصيدلانية.
- الحكومة والقطاع العام.
- قطاع التجزئة والتجارة الإلكترونية.
- شركات التأمين.
- صناعة الطاقة والمرافق.
- قطاع الخدمات الاستشارية.
- شركات تطوير البرمجيات.
- المؤسسات التعليمية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- الإدارة القانونية.
- إدارة تكنولوجيا المعلومات.
- إدارة العقود.
- إدارة المخاطر.
- الامتثال وحوكمة الشركات.
- التدقيق الداخلي.
- إدارة المشتريات.
- إدارة البيانات.
- إدارة المشاريع.

أهداف الدورة التدريبية:

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

- فهم عميق لمفاهيم الأمن السيبراني وأطر حماية البيانات.
- صياغة عقود الأمن السيبراني واتفاقيات معالجة البيانات.
- إدارة دورة حياة عقود الأمن السيبراني.
- تحديد وإدارة المخاطر القانونية والتشغيلية في الأمن السيبراني.
- التفاوض على شروط عقود الأمن السيبراني بفعالية.
- ضمان الامتثال للوائح حماية البيانات (مثل GDPR).
- التعامل مع حوادث الأمن السيبراني والاستجابة لها.
- فهم مسؤولية الأطراف في عقود الأمن السيبراني.
- تقييم مزودي خدمات الأمن وإدارة أدائهم.
- حماية الأصول الرقمية والبيانات الحساسة للمؤسسة.

منهجية الدورة التدريبية:

يُقدم BIG BEN Training Center هذه الدورة بمنهجية تدريبية عملية ومُتخصصة، مُصممة لتمكين المشاركين من إتقان إدارة عقود الأمن السيبراني وحماية البيانات. تعتمد المنهجية على محاضرات تفاعلية تُقدم المفاهيم القانونية، والتقنية، والاستراتيجية المتعلقة بالأمن السيبراني وحماية البيانات، مصحوبة بورش عمل تطبيقية مكثفة تتيح للمشاركين ممارسة صياغة بنود عقود الخدمات الأمنية، وتحليل اتفاقيات معالجة البيانات، وتطوير خطط الاستجابة للحوادث السيبرانية. تُقدم دراسات حالة واقعية ومتعمقة لانتهاكات بيانات كبرى وهجمات سيبرانية معقدة، تُحلل فيها أسباب الاختراق، والآثار القانونية والمالية، والدروس المستفادة من هذه التجارب، بما في ذلك قضايا الاحتيال السيبراني، والابتزاز الإلكتروني، والنزاعات حول المسؤولية عن البيانات. تُشجع الجلسات التفاعلية على النقاش وتبادل الخبرات بين المتدربين من مختلف الخلفيات القانونية والتقنية، مما يُعزز من فهمهم للتحديات المتعددة الأبعاد في هذا المجال. يُقدم المدربون الخبراء في BIG BEN Training Center، وهم من ذوي الخبرة الواسعة في قانون الأمن السيبراني وحماية البيانات، تغذية راجعة بناءة ومستمرة لضمان التطور المستمر للمشاركين في مجال عقود الأمن السيبراني وحماية البيانات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في الأمن السيبراني وحماية البيانات

- مفهوم الأمن السيبراني وأهميته للمؤسسات.
- أنواع التهديدات السيبرانية (برمجيات خبيثة، تصيد، هجمات حجب الخدمة).
- مفاهيم حماية البيانات والخصوصية.
- أهمية الإطار القانوني للأمن السيبراني وحماية البيانات.
- مقدمة إلى اللوائح الدولية (GDPR, CCPA).
- أصول المعلومات وكيفية تصنيفها.
- تأثير الأمن السيبراني على استمرارية الأعمال.

الوحدة الثانية: صياغة عقود الأمن السيبراني والخدمات الأمنية

- صياغة بنود عقود الأمن السيبراني وخدمات الحماية.
- تحديد بنود نطاق الخدمة الأمنية ومستويات الحماية.
- صياغة اتفاقيات مستوى الخدمة (SLAs) في الأمن السيبراني.
- التعامل مع بنود المسؤولية والتعويضات في حالة الاختراق.
- أهمية الوضوح في بنود التدقيق الأمني والاختبار.
- بنود السرية وعدم الإفصاح (NDAs).
- المتطلبات التقنية في العقود الأمنية.

الوحدة الثالثة: عقود حماية البيانات والامتثال القانوني

- صياغة بنود اتفاقيات معالجة البيانات (DPAs).
- تحديد بنود حماية البيانات الشخصية والبيانات الحساسة.
- الامتثال للائحة العامة لحماية البيانات (GDPR).
- التزامات معالجي البيانات ومراقبي البيانات.
- حقوق الأفراد بموجب قوانين حماية البيانات.
- نقل البيانات عبر الحدود والآليات القانونية.
- التعامل مع طلبات الوصول إلى البيانات والتصحيح.

الوحدة الرابعة: إدارة المخاطر السيبرانية والاستجابة للحوادث

- تحديد وتقييم المخاطر السيبرانية.
- استراتيجيات تخفيف المخاطر والتحكم بها.
- خطط الاستجابة للحوادث السيبرانية وإدارة الأزمات.
- الإبلاغ عن انتهاكات البيانات للجهات التنظيمية.
- دور التأمين السيبراني في إدارة المخاطر.
- التدريبات العملية على سيناريوهات الاختراق.
- التحقيق الجنائي الرقمي في الحوادث الأمنية.

الوحدة الخامسة: المراجعة والتدقيق والاتجاهات المستقبلية في الأمن السيبراني

- تدقيق عقود الأمن السيبراني وحماية البيانات.
- تقييم فعالية الضوابط الأمنية.
- أهمية مراجعة العقود الدورية.
- التهديدات السيبرانية الناشئة (الذكاء الاصطناعي، إنترنت الأشياء).
- التحديات القانونية للذكاء الاصطناعي والأمن السيبراني.
- مستقبل الأمن السيبراني والتغيرات التشريعية المتوقعة.
- أهمية بناء ثقافة أمنية 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 المعتمدة على الذكاء الاصطناعي، والزيادة الهائلة في حجم البيانات الشخصية التي يتم جمعها ومعالجتها، كيف يمكن لعقود الأمن السيبراني وحماية البيانات أن تضمن المرونة والقدرة على التكيف مع هذه الهجمات المتطورة، وما هي الابتكارات التعاقدية التي يمكن تبنيها لضمان حماية فعالة ومستقبلية للبيانات تتجاوز الأطر القانونية الحالية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة من BIG BEN Training Center بتقديمها منظورًا شاملاً وعمليًا لإدارة عقود الأمن السيبراني وحماية البيانات، مما يجعلها ضرورية لكل من يسعى لحماية الأصول الرقمية والامتثال للوائح الصارمة. نحن لا نكتفي بتقديم المفاهيم النظرية، بل نغوص في التفاصيل الدقيقة لصياغة اتفاقيات الخدمة الأمنية، والتعامل مع بنود حماية البيانات، وإدارة الاستجابة للحوادث السيبرانية بأسلوب احترافي. تُقدم الدورة رؤى عملية حول كيفية تخفيف المخاطر السيبرانية، وضمان الامتثال القانوني، وتقييم مزودي خدمات الأمن، مما يُسهم في حماية المؤسسة من الاختراقات وتعزيز الثقة الرقمية. يخرج المتدرب من هذه الدورة وهو يمتلك القدرة على قيادة وإدارة العمليات التعاقدية للأمن السيبراني وحماية البيانات بفعالية، مما يُسهم بشكل مباشر في نجاح استراتيجيات الأمن الرقمي وحماية سمعة المؤسسة. إنها دورة مصممة خصيصًا لمن يسعى للتميز في إدارة عقود الأمن السيبراني وحماية البيانات.