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

اغسطس ٢٠٢٦ ٢١ - ١٧

بروكسل

(للشخص الواحد) € ٤٤٠٠

Ref: #CM3860_212783

مقدمة الدورة التدريبية / لمحة عامة:

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

بيئة رقمية متغيرة.

لـ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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.
- بيانات حساسة. المدراء التنفيذيون في الشركات التي تتعامل مع
- 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:

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

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

منهجية الدورة التدريبية:ا

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

البيانات الوحدة الأولى: مقدمة في الأمن السيبراني وحماية

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

والخدمات الأمنية الوحدة الثانية: صياغة عقود الأمن السيبراني

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

القانوني الوحدة الثالثة: عقود حماية البيانات والامتثال

- صياغة بنود اتفاقيات معالجة البيانات (DPAs).
- الحساسة. تحديد بنود حماية البيانات الشخصية والبيانات
- 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.

والاستجابة للحوادث الوحدة الرابعة: إدارة المخاطر السيبرانية

- 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.

المستقبلية في الأمن السيبراني الوحدة الخامسة: المراجعة والتدقيق والاتجاهات

- تدقيق عقود الأمن السيبراني وحماية البيانات.
- تقييم فعالية الضوابط الأمنية.
- أهمية مراجعة العقود الدورية.
- إنترنت الأشياء). التهديدات السيبرانية الناشئة (الذكاء الاصطناعي،
- السيبراني. التحديات القانونية للذكاء الاصطناعي والأمن
- المتوقعة. مستقبل الأمن السيبراني والتغيرات التشريعية
- أهمية بناء ثقافة أمنية في المؤسسة.

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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:

الشخصية التي يتم جمعها المعتمدة على الذكاء الاصطناعي، والزيادة الهائلة في ظل التطور المتسارع للتهديدات السيبرانية البيانات أن تضمن المرونة والقدرة على التكيف مع ومعالجتها، كيف يمكن لعقود الأمن السيبراني وحماية في حجم البيانات تتجاوز الأطر القانونية الحالية؟ التعاقدية التي يمكن تبنيها لضمان حماية فعالة هذه الهجمات المتطورة، وما هي الابتكارات ومستقبلية للبيانات

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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