الدورة التدريبية: تحديات الخصوصية وحماية البيانات في بيئة التحول الرقمي: استراتيجيات الامتثال والأمان

#DT8066

الدورة التدريبية: تحديات الخصوصية وحماية البيانات في بيئة التحول الرقمي: استراتيجيات الامتثال والأمان

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التسارع الهائل للتحول الرقمي الذي يشهده عالمنا اليوم، تبرز تحديات الخصوصية وحماية البيانات كأحد أهم القضايا التي تواجه المؤسسات والأفراد على حد سواء. إن الحفاظ على أمن المعلومات الشخصية والحساسة لم يعد مجرد مسألة تقنية، بل أصبح ركيزة أساسية للثقة والامتثال القانوني. تقدم هذه الدورة التدريبية الشاملة من BIG BEN Training Center برنامجاً متكاملاً مصمماً لتزويد المشاركين بالمعرفة والأدوات اللازمة لفهم مخاطر أمن البيانات، واستراتيجيات الامتثال للخصوصية، وأفضل ممارسات حماية المعلومات. سنتناول كيفية تطبيق إدارة أمن المعلومات، والتعامل مع خروقات البيانات، وتشفير البيانات وحمايتها. ستركز الدورة على أهمية حوكمة البيانات الرقمية، وتأمين البنية التحتية الرقمية، والتدقيق الأمني للبيانات. تهدف الدورة إلى تمكين المهنيين والقادة من تطوير وتنفيذ سياسات وإجراءات فعالة تضمن حماية البيانات في بيئة التحول الرقمي، وتحقيق الامتثال والأمان اللازمين. يؤكد البروفيسور دانيال سولوف (Daniel Solove)، أحد أبرز خبراء الخصوصية في العالم ومؤلف كتاب "Understanding Privacy"، على أن الخصوصية لا تتعلق فقط بالسرية، بل بالتحكم في كيفية استخدام المعلومات، مما يبرز أهمية الفهم الشامل لهذه التحديات. يقدم BIG BEN Training Center هذه الدورة لتمكين المشاركين من فهم تشريعات حماية البيانات، وخصوصية البيانات الشخصية، وأمن المعلومات السحابية، وإدارة المخاطر السيبرانية، وأخلاقيات استخدام البيانات، وبناء ثقافة أمن البيانات، وتقييم أثر حماية البيانات، والاستجابة للحوادث الأمنية، والأمان في التحول الرقمي، وحماية البيانات الحساسة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء أمن المعلومات.
- مسؤولو حماية البيانات (DPOs).
- مدراء تقنية المعلومات.
- مدراء الامتثال والمخاطر.
- المستشارون القانونيون.
- أخصائيو الأمن السيبراني.
- مدراء المشاريع الرقمية.
- المطورون والمهندسون الذين يتعاملون مع البيانات.
- أصحاب الأعمال والمدراء التنفيذيون.
- أي شخص مسؤول عن التعامل مع البيانات الشخصية والحساسة.

القطاعات والصناعات المستهدفة:

- الخدمات المالية والمصرفية.
- الرعاية الصحية.
- الحكومة والقطاع العام.
- الاتصالات.
- التكنولوجيا والبرمجيات.
- التجزئة والتجارة الإلكترونية.
- المحاماة والاستشارات القانونية.
- التعليم.
- التصنيع.
- المنظمات غير الربحية.

الأقسام المؤسسية المستهدفة:

- أمن المعلومات.
- تقنية المعلومات.
- الامتثال والشؤون القانونية.
- إدارة المخاطر.
- الموارد البشرية.
- التسويق.
- العمليات.
- إدارة المنتجات.
- التدقيق الداخلي.
- التطوير والبحث.

أهداف الدورة التدريبية:

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

- فهم تحديات الخصوصية وحماية البيانات في العصر الرقمي.
- تطبيق استراتيجيات الامتثال للخصوصية مع تشريعات حماية البيانات.
- تحديد وتقييم مخاطر أمن البيانات المحتملة.
- تطوير وتنفيذ أفضل ممارسات حماية المعلومات.
- إدارة أمن المعلومات وتأمين الأنظمة الرقمية.
- التعامل الفعال مع خروقات البيانات وخطط الاستجابة.
- تطبيق تقنيات تشفير البيانات وحمايتها.
- وضع سياسات حوكمة البيانات الرقمية الشاملة.
- تأمين البنية التحتية الرقمية بشكل فعال.
- إجراء التدقيق الأمني للبيانات بانتظام.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة التدريبية على منهجية تعليمية تفاعلية وموجهة نحو التطبيق العملي، مصممة لتمكين المشاركين من مواجهة تحديات الخصوصية وحماية البيانات في بيئة التحول الرقمي. تتضمن المنهجية مزيجاً من المحاضرات المتعمقة التي تغطي تشريعات حماية البيانات وخصوصية البيانات الشخصية، ودراسات حالة واقعية لخروقات البيانات وكيفية التعامل معها، وورش عمل تطبيقية تتيح للمشاركين فرصة لتطبيق استراتيجيات الامتثال للخصوصية، وتشفير البيانات وحمايتها، وإدارة المخاطر السيبرانية. سيتم التركيز على أمن المعلومات السحابية، وبناء ثقافة أمن البيانات، وتقييم أثر حماية البيانات. يقدم المدربون الخبراء، من ذوي الخبرة الواسعة في مجال الأمن السيبراني والخصوصية، إرشادات عملية وتغذية راجعة بناءة. تهدف المنهجية إلى تمكين المتدربين من فهم عميق لأخلاقيات استخدام البيانات، والاستجابة للحوادث الأمنية، والأمان في التحول الرقمي، وحماية البيانات الحساسة، مما يؤهلهم لتعزيز الامتثال والأمان في مؤسساتهم.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أسس الخصوصية وحماية البيانات في التحول الرقمي

- مقدمة إلى التحول الرقمي وتأثيره على البيانات.
- مفهوم الخصوصية وحماية البيانات وأهميتهما.
- تحديات الخصوصية وحماية البيانات في العصر الرقمي.
- الفرق بين الخصوصية والأمن والسرية.
- أنواع البيانات (شخصية، حساسة) وأهمية حمايتها.
- مبادئ حماية البيانات (مثل تقليل البيانات).
- الوعي بأهمية أمن البيانات.

الوحدة الثانية: تشريعات حماية البيانات واستراتيجيات الامتثال للخصوصية

- أهم تشريعات حماية البيانات العالمية (مثل GDPR, CCPA).
- استراتيجيات الامتثال للخصوصية ومتطلباتها.
- دور مسؤول حماية البيانات (DPO).
- تقييم أثر حماية البيانات (DPIA).
- التعاقد مع الأطراف الثالثة ومعالجي البيانات.
- حوكمة البيانات الرقمية وسياسات الخصوصية.
- دراسة حالة: تطبيق مبادئ GDPR في مؤسسة.

الوحدة الثالثة: إدارة أمن المعلومات ومخاطر أمن البيانات

- مفاهيم إدارة أمن المعلومات.
- مخاطر أمن البيانات الشائعة (هجمات سيبرانية، خروقات).
- تأمين البنية التحتية الرقمية (الشبكات، الخوادم).
- أمن المعلومات السحابية وأفضل الممارسات.
- إدارة الهوية والوصول (IAM).
- إدارة المخاطر السيبرانية وتقييم الضعف.
- ورشة عمل: تحليل سيناريوهات مخاطر البيانات.

الوحدة الرابعة: أفضل ممارسات حماية المعلومات وتشفير البيانات

- أفضل ممارسات حماية المعلومات التقنية والإدارية.
- تشفير البيانات وحمايتها (البيانات في حالة السكون والحركة).
- أمن التطبيقات والبرمجيات.
- أمن الأجهزة الطرفية والمحمولة.
- بناء ثقافة أمن البيانات داخل المؤسسة.
- التدريب والتوعية للموظفين.
- الأمان في التحول الرقمي ومستقبل الأمن السيبراني.

الوحدة الخامسة: التعامل مع خروقات البيانات والاستجابة للحوادث

- خطوات التعامل مع خروقات البيانات.
- خطط الاستجابة للحوادث الأمنية.
- الإبلاغ عن الحوادث والتعاون مع الجهات التنظيمية.
- التحقيق الجنائي الرقمي.
- التعافي من الحوادث واستعادة البيانات.
- المراجعة والتحسين المستمر لسياسات الأمن.
- التدقيق الأمني للبيانات كأداة للتحسين.

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 للتحول الرقمي وتزايد حجم البيانات المتداولة، كيف يمكن للمؤسسات أن تضمن حماية البيانات الحساسة وخصوصية البيانات الشخصية بشكل فعال، مع تحقيق الامتثال والأمان المطلوبين، دون إعاقة الابتكار أو خلق حواجز غير ضرورية أمام تدفق المعلومات اللازم للنمو والتقدم؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية من BIG BEN Training Center بتركيزها الشامل والعملي على تحديات الخصوصية وحماية البيانات في بيئة التحول الرقمي، مقدمةً نهجاً متكاملاً لاستراتيجيات الامتثال والأمان. خلافاً للدورات التي قد تركز على جانب واحد، فإننا نغطي جميع أبعاد مخاطر أمن البيانات، من تشريعات حماية البيانات وخصوصية البيانات الشخصية إلى إدارة أمن المعلومات والتعامل مع خروقات البيانات. نحن نقدم رؤى عملية حول تشفير البيانات وحمايتها، وحوكمة البيانات الرقمية، وتأمين البنية التحتية الرقمية. إن هذا المزيج الفريد من المحتوى العميق، والمنهجية التطبيقية، ودراسات الحالة الواقعية، بالإضافة إلى التركيز على أفضل ممارسات حماية المعلومات والتدقيق الأمني للبيانات، يجعلها الخيار الأمثل للمهنيين الذين يسعون لقيادة مؤسساتهم نحو بيئة رقمية آمنة وموثوقة.