البيانات الدورة التدريبية: تدقيق الأمن السيبراني وحماية

Ref: #GRC9339

مقدمة الدورة التدريبية / لمحة عامة:

العملية اللازمة لضمان السيبراني وحماية البيانات لتزويد المشاركين تم تصميم هذه الدورة التدريبية في تدقيق الأمن خلال الدورة، سيكتسب المتدربون فهمًا أمن المعلومات وتحقيق حماية فعالة للبيانات في بالمعرفة العميقة والمهارات كيفية التقنية، وتحليل الفجوات الأمنية وفق معايير معترف شاملاً لتقييم المخاطر السيبرانية، وتدقيق الضوابط المؤسسات. التنظيمية مثل.GDPR إعداد تقارير تدقيق مفصلة تشمل توصيات لتعزيز حماية بها مثل ISO ٢٧٠٠٧ و .NISTسيتعلم المشاركون مما يضمن قدرة المشاركين على تُقدم الدورة بأسلوب تفاعلي يجمع بين دراسة الحالات البيانات وامتثالها للمتطلبات تقدم BIG BEN Training Center هذه الدورة تنفيذ إجراءات فعالة لحماية البيانات داخل بيئاتهم الواقعية والمحاكاة، مثل لتعزيز حوكمة أمن المعلومات وتحقيق الامتثال بطريقة احترافية موجهة للشركات والمؤسسات التي تسعى المؤسسية. تحليل نقاط الضعف والمراجعة الفنية المتقدمة. التنظيمي، مع التركيز على الجوانب الفريدة

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:

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

- إجراء تدقيق الأمن السيبراني باستخدام معاييرISO ٢٧٠٠٧.
- تحليل المخاطر وتقييم الضوابط الأمنية.
- البيانات. إعداد تقارير تدقيق فنية شاملة وحلول حماية
- 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:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

وحماية البيانات: الوحدة الأولى: أساسيات تدقيق الأمن السيبراني

- تعريف تدقيق الأمن السيبراني والحوكمة.
- معايير ISO ٢٧٠٠٧ 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.

الأمان: الوحدة الثانية: تدقيق الضوابط التقنية وتقنيات

- 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.

القانونية: الوحدة الثالثة: تدقيق الامتثال والتشريعات

- 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.

المتقدمة: الوحدة الرابعة: استجابة الحوادث وتحليل المخاطر

- 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.

التنفيذية: الوحدة الخامسة: التكامل المؤسسي والتوصيات

- 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:

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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تجمع بين الأمور النظرية السيبراني وحماية البيانات بتقديم تجربة تعليمية تتميز هذه الدورة التدريبية في تدقيق الأمن تحليل المخاطر السيبرانية وتقييم الضوابط التقنية. والتطبيق العملي الفوري اعتمادًا على كلمات مثل مصممة خصيصًا للشركات، الجوانب الفنية مثل ISO ٢٧٠٠٧ وNIST، مع تقديم دراسات حالة حقيقية تركز الدورة على استخدام معايير معترف بها دوليًا إعداد تقارير تدقيق تنفيذية وتوصيات والتنظيمية. تقدم BIG BEN Training Center مشهدًا من بيئات شركات فعلية تشمل لتدريب التهديدات، بل تصميم وتنفيذ إجراءات حماية فعّالة. قابلة للتطبيق، مما □□□□ للمشاركين ليس فقط فهم شاملاً يشمل تعتمد على مؤشرات الفرق على رد الفعل السريع والتعافي، مع تطوير خطة علاوة على ذلك، تُجرى محاكاة حوادث واقعية مباشرة إلى المؤسسة، دون الاعتماد أداء واضحة. كل هذا يتم ضمن منهج تطبيقي يضمن مستدامة لحوكمة أمن المعلومات دفاع سيبراني متكامل وقابل للتكيف مع تطورات البيئة على أدوات، بل باستخدام رؤى عملية تؤهل الفرق لبناء انتقال المعرفة الرقمية.