للمؤسسات الدورة التدريبية: إدارة المخاطر السيبرانية والامتثال التنظيمي

Ref: #IT6473

مقدمة الدورة التدريبية / لمحة عامة:

على اختلاف أحجامها السيبرانية والامتثال التنظيمي من أهم الأولويات في المشهد الرقمي المعاصر، أصبحت إدارة المخاطر حجم التعقيدات القانونية والتنظيمية، تواجه وقطاعاتها. مع التطور المستمر للتهديدات السيبرانية الاستراتيجية للمؤسسات بالمعرفة وضمان الالتزام بالمعايير والمتطلبات. هذه الدورة الشركات تحدياً متزايداً في حماية أصولها الرقمية وتزايد السيبرانية بفعالية، بالإضافة إلى بناء برامج والأدوات اللازمة لفهم وتقييم وإدارة المخاطر التدريبية مصممة لتزويد المشاركين للتخفيف من حدتها، مع المحلية والدولية. سنغطي منهجيات تحديد المخاطر، امتثال قوية تضمن تلبية المتطلبات التنظيمية يؤكد البروفيسور ويليام إدواردز ديمينج (W. التركيز على أهمية الحوكمة الرشيدة في هذا المجال. تحليل الثغرات، ووضع خطط يلتزم BIG BEN Training BIG التحسين المستمر ليس أمراً اختيارياً، بل هو ضرورة" ، أحد رواد إدارة الجودة، أن(Edwards Deming المتقدمة والتطبيقات العملية، لتمكين قادة الأمن بتقديم تدريب متكامل يجمع بين النظريات Center للبقاء في عالم اليوم". عملياتهم. وتقليل التعرض للمخاطر، وتعزيز الثقة والشفافية في ومتخصصي الامتثال من بناء بيئات رقمية آمنة،

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مدراء أمن المعلومات.
- مسؤولو المخاطر والامتثال.
- مدققو نظم المعلومات.
- المستشارون في الأمن السيبراني.
- مدراء تقنية المعلومات.
- مدراء الحوكمة المؤسسية.
- المحامون والمتخصصون القانونيون في المجال الرقمي.
- المتخصصون في إدارة استمرارية الأعمال.
- قادة الأعمال والمدراء التنفيذيون.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الاتصالات وتقنية المعلومات.
- القطاع الحكومي والجهات التنظيمية.
- قطاع الرعاية الصحية.
- شركات التأمين.
- شركات الطاقة والمرافق.
- الشركات الكبرى والمتعددة الجنسيات.
- شركات الاستشارات الأمنية والقانونية.
- الشركات الناشئة التقنية.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات.
- أقسام إدارة المخاطر.
- أقسام الامتثال (Compliance).
- أقسام التدقيق الداخلي والخارجي.
- الأقسام القانونية.
- أقسام تقنية المعلومات.
- أقسام الحوكمة المؤسسية.
- أقسام التخطيط الاستراتيجي.

أهداف الدورة التدريبية:

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

- تحديد وتقييم وإدارة المخاطر السيبرانية للمؤسسة.
- المخاطر. فهم وتطبيق الأطر والمعايير الدولية لإدارة
- بناء وتطبيق برامج الامتثال التنظيمي الفعالة.
- المعلومات والخصوصية. التعامل مع التشريعات واللوائح المتعلقة بأمن
- إعداد وتنفيذ خطط الاستجابة للحوادث الأمنية.
- تحليل الثغرات الأمنية ونقاط الضعف في الأنظمة.
- تطوير سياسات وإجراءات أمنية متوافقة مع المتطلبات.
- قياس فعالية برامج إدارة المخاطر والامتثال.
- تعزيز ثقافة الوعي بالمخاطر الأمنية داخل المؤسسة.

منهجية الدورة التدريبية:

والامتثال التدريبية على منهجية متقدمة تجمع بين الفهم النظري يعتمد BIG BEN Training Center في هذه الدورة يقدمها خبراء في الأمن السيبراني التنظيمي والتطبيق العملي المكثف. تتضمن المنهجية العميق لإدارة المخاطر السيبرانية أحدث التهديدات وأفضل الممارسات. سيشارك المتدربون وإدارة المخاطر والقانون الرقمي، مع التركيز على محاضرات تفاعلية وفاشلة المخاطر، وتحليل الثغرات، وتطوير خطط المعالجة. كما في ورش عمل عملية تستعرض سيناريوهات واقعية لتقييم وكيفية التغلب عليها. يتم في إدارة المخاطر والامتثال، مما يمنح المشاركين سيتم التطرق إلى دراسات حالة لأمثلة ناجحة حلول مبتكرة. الهدف هو تزويد المشاركين تشجيع العمل الجماعي والمناقشات لتبادل الخبرات رؤى عملية حول التحديات مما يعزز المرونة استراتيجيات فعالة للتخفيف منها، وضمان الامتثال بالقدرة على تحديد وتقييم المخاطر، ووضع وتطوير الأمنية للمؤسسات الصارم للمتطلبات التنظيمية،

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

العام الوحدة الأولى: أساسيات المخاطر السيبرانية وإطارها

- مقدمة في المخاطر السيبرانية وأنواعها.
- مفاهيم التهديد، ونقاط الضعف، والأثر.
- منهجيات تقييم المخاطر (Qualitative and Quantitative).
- تحديد الأصول الحيوية للمؤسسة.
- مراحل دورة حياة إدارة المخاطر.
- تحليل سيناريوهات المخاطر السيبرانية.
- أهمية سجل المخاطر.

الوحدة الثانية: أطر إدارة المخاطر السيبرانية والمعايير الدولية.

- إطار NIST للتحكم في الأمن السيبراني.
- معيار ISO ٢٧٠٠٥ لإدارة مخاطر أمن المعلومات.
- إطار COBIT لإدارة وحوكمة تكنولوجيا المعلومات.
- إدارة مخاطر الطرف الثالث (Third-Party Risk Management).
- أدوات وتقنيات تقييم المخاطر.
- التحكم في المخاطر: التخفيف، القبول، التحويل، التجنب.
- قياس مؤشرات الأداء الرئيسية (KPIs) للمخاطر.

الوحدة الثالثة: الامتثال التنظيمي وقوانين حماية البيانات.

- مقدمة في الامتثال التنظيمي وأهميته.
- اللائحة العامة لحماية البيانات (GDPR) ومتطلباتها.
- قوانين حماية البيانات والخصوصية المحلية والدولية.
- الامتثال لمعايير الصناعة (PCI DSS، HIPAA).
- دور الهيئات التنظيمية والتدقيق.
- إعداد برامج الامتثال الداخلية.
- سياسات وإجراءات الامتثال.

والامتثال. الوحدة الرابعة: تنفيذ برامج إدارة المخاطر

- بناء فريق إدارة المخاطر والامتثال.
- دمج إدارة المخاطر في دورة حياة التطوير.
- إعداد خطط الاستجابة للحوادث السيبرانية.
- التدقيق الأمني واختبار الاختراق.
- التوعية والتدريب على الأمن السيبراني.
- إدارة التغيير في بيئة المخاطر والامتثال.
- التقارير والإبلاغ عن المخاطر.

المستقبلية. الوحدة الخامسة: التحديات المتقدمة والاتجاهات

- المخاطر السيبرانية في الحوسبة السحابية.
- الذكاء الاصطناعي في إدارة المخاطر والامتثال.
- مخاطر إنترنت الأشياء (IoT).
- سلاسل الكتل (Blockchain) وأثرها على الأمن.
- التحديات القانونية والتنظيمية الجديدة.
- تطور الهجمات السيبرانية (APTs، Ransomware).
- المرونة السيبرانية (Cyber Resilience).

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:

على "وضع والمتطلبات التنظيمية المتزايدة، كيف يمكن للمؤسسات في ظل مشهد التهديدات السيبرانية المتطور باستمرار المخاطر السيبرانية تركز على القيمة وتدعم العلامات في المربعات" وتتبنى استراتيجية شاملة أن تبتعد عن نهج الامتثال القائم الابتكار؟ لإدارة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

مما يميزها عن الدورات يجمع بين إدارة المخاطر السيبرانية والامتثال تتميز هذه الدورة التدريبية بتقديمها منهجاً فريداً حول التهديدات أو اللوائح، بل نركز على التي تركز على أحد الجانبين فقط. نحن لا نقدم مجرد التنظيمي في سياق متكامل، مما مؤسساتهم وضمان التزامها. ترتكز الدورة على دراسات تمكين المشاركين من بناء استراتيجيات شاملة لحماية معلومات الحقيقي. كما نغطي أحدث يمنح المشاركين فهماً عميقاً للتحديات والحلول حالة واقعية وأمثلة عملية من مختلف القطاعات، تكييفها مع البيئات المؤسسية المختلفة. إن هذا المعايير والأطر العالمية، مع التركيز على كيفية المطبقة في العالم في الأمن، يضمن للمشاركين والتدريب العملي المكثف، بالإضافة إلى التركيز على المزيج الفريد من المعرفة النظرية المتقدمة المخاطر والامتثال بفعالية وثقة. اكتساب المهارات اللازمة لقيادة جهود إدارة التفكير الاستراتيجي