التدريبية: إدارة المخاطر الأمنية والامتثال
للمؤسسات الكبرى (GRC) الدورة

يونيو ٢٠٢٦ ٠٥ - ٠١

روما

(للشخص الواحد) € ٥٧٠٠

Ref: #CYB3092_268784

مقدمة الدورة التدريبية / لمحة عامة:

التنظيمية، وضمان استمرارية الزاوية لأي مؤسسة كبرى تسعى لحماية أصولها، تُعد إدارة المخاطر الأمنية والامتثال (GRC) حجر
لمبادئ السيبرانية وتعقيدات اللوائح التنظيمية، أصبح الفهم الأعمال. في بيئة عمل تتزايد فيها المخاطر الوفاء بالمتطلبات
في الأمن السيبراني الدورة التدريبية المتخصصة للمديرين التنفيذيين، ضرورة لا غنى عنها. تقدم هذه GRC العميق
في وضمان فعالة، تحديد المخاطر الأمنية، GRC والامتثال، الأدوات والمعرفة اللازمة لبناء برامج مديري المخاطر، والمتخصصين
الأمنية، وإعداد تقارير هذه الدورة إطار عمل GRC المتكامل، تقييم المخاطر الامتثال للتشريعات المحلية والدولية. سنتناول
تهدف استراتيجيات الأمن السيبراني بأهداف العمل، الامتثال. سيكتسب المشاركون القدرة على ربط الأمنية، إدارة الضوابط
الفعال. يستند المحتوى الدورة إلى تمكين المؤسسات الكبرى من تحقيق الحوكمة وتقليل التعرض للمخاطر القانونية والمالية.
من إسهامات خبراء أكاديميين بارزين مثل إلى أحدث المعايير وأفضل الممارسات الصناعية، مع الرشيدة والأمن السيبراني
Training عمل FAIR لتحليل مخاطر المعلومات. يقدم BIG BEN البروفيسور جاك جونز (Jack Jones)، مبتكر إطار الاستفادة
الكبرى. التنظيمية والامتثال الاستراتيجي في المؤسسات هذه الدورة لتعزيز المرونة Center

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو المخاطر الأمنية والتشغيلية.
- مسؤولو الامتثال والحوكمة.
- مديرو الأمن السيبراني ومديرو أمن المعلومات.
- مدققو الأنظمة الداخلية والخارجية.
- المستشارون في مجال GRC.
- مديرو الإدارات القانونية.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات التأمين.
- شركات الاتصالات.
- القطاع الحكومي والهيئات التنظيمية وما في حكمها.
- شركات النفط والغاز والطاقة.
- المؤسسات المتعددة الجنسيات.

الأقسام المؤسسية المستهدفة:

- إدارة المخاطر.
- إدارة الامتثال.
- إدارة الأمن السيبراني.
- الإدارة القانونية.
- التدقيق الداخلي.

أهداف الدورة التدريبية:

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

- (GRC). فهم شامل لمبادئ إدارة المخاطر الأمنية والامتثال
- القدرة على تطوير وتنفيذ برنامج GRC متكامل.
- تحديد وتقييم المخاطر الأمنية التي تواجه المؤسسة.
- المخاطر. تصميم وتطبيق الضوابط الأمنية اللازمة لتخفيف
- (مثل. (GDPR, ISO ٢٧٠٠١ ضمان الامتثال للوائح والمعايير المحلية والدولية
- إعداد تقارير المخاطر والامتثال للإدارة العليا.
- المؤسسة. تعزيز ثقافة الوعي بالمخاطر والامتثال داخل

منهجية الدورة التدريبية:

بيئات GRC نحو الحلول، مصممة لتمكين المشاركين من تطبيق مبادئ تعتمد هذه الدورة التدريبية منهجية تفاعلية وموجهة الصناعات المختلفة، وورش GRC المتدربون من خلال دراسات الحالة الشاملة لتحديات المؤسسات الكبرى المعقدة. سيتمكن في تتضمن المنهجية مناقشات متعمقة حول أطر من فهم كيفية ربط الأمن السيبراني بأهداف الحوكمة العمل العملية، في والتعامل مع متكامل يناسب الاحتياجات التنظيمية. سيتم التركيز عمل GRC مثل COSO وNIST، وكيفية بناء إطار والامتثال. قادة المؤسسات من Center متطلبات الامتثال المعقدة. يقدم BIG BEN Training على تحليل المخاطر الكمي والنوعي، المخاطر الأمنية بفعالية وضمان الامتثال التنظيمي. إدارة هذه الدورة لتمكين

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الحوكمة والمخاطر والامتثال (GRC)

- مقدمة إلى مفاهيم GRC.
- أهمية GRC للمؤسسات الكبرى.
- العلاقة بين الحوكمة والمخاطر والامتثال.
- أهداف ومكونات برنامج GRC فعال.
- فوائد تطبيق GRC الشامل.
- التحديات الشائعة في تطبيق GRC.
- دور الإدارة العليا في GRC.

الوحدة الثانية: إدارة المخاطر الأمنية للمؤسسات

- تحديد المخاطر الأمنية (Cybersecurity Risk Identification).
- باستخدام أطر عمل (مثل FAIR). تقييم المخاطر الأمنية (Risk Assessment)
- تحليل المخاطر الكمي والنوعي.
- تصنيف المخاطر وتحديد أولوياتها.
- استراتيجيات معالجة المخاطر (Risk Treatment).
- مراقبة المخاطر وإعادة تقييمها.
- إعداد سجل المخاطر (Risk Register).

الوحدة الثالثة: الامتثال للوائح والمعايير

- وتأثيرها. اللوائح الرئيسية (GDPR, HIPAA, SOX, PCI DSS)
- معايير الأمن الدولية (ISO ٢٧٠٠١, NIST Cybersecurity Framework).
- تصميم وتنفيذ الضوابط الأمنية لضمان الامتثال.
- عمليات التدقيق والتقييم للامتثال.
- إدارة الثغرات الأمنية من منظور الامتثال.
- التعامل مع المتطلبات القانونية والتشريعية.
- أتمتة عمليات الامتثال.

الداخلية الوحدة الرابعة: حوكمة أمن المعلومات والرقابة

- بناء إطار حوكمة أمن المعلومات.
- الأدوار والمسؤوليات في أمن المعلومات.
- وضع السياسات والإجراءات الأمنية.
- الرقابة الداخلية لأمن المعلومات.
- إدارة أداء الأمن السيبراني.
- مؤشرات الأداء الرئيسية (KPIs) لـ GRC
- التقارير الدورية للإدارة العليا ومجالس الإدارة.

الأمنية الوحدة الخامسة: دمج GRC ومستقبل إدارة المخاطر

- استراتيجيات دمج GRC في العمليات التشغيلية.
- استخدام التكنولوجيا لدعم GRC (GRC Platforms)
- إدارة المخاطر في سلسلة التوريد.
- الحوسبة الكمية). التعامل مع المخاطر الناشئة (الذكاء الاصطناعي،
- بناء ثقافة واعية بالمخاطر والامتثال.
- التعاون مع الجهات التنظيمية.
- الاتجاهات المستقبلية لـ GRC

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 ٢٠-٢٥ 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:

) أن تتحول من التنظيمية بوتيرة متسارعة، كيف يمكن لبرامج إدارة في عالم تتطور فيه التهديدات السيبرانية واللوائح في بناء مرونة تنظيمية شاملة وقيمة مجرد استجابة للمتطلبات إلى محرك استراتيجي يساهم المخاطر الأمنية والامتثال (GRC) مضافة للمؤسسات الكبرى؟ بشكل فعال

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

دمج هذه المفاهيم إدارة المخاطر الأمنية والامتثال (GRC)، مما يوفر تتميز هذه الدورة بتركيزها العميق والعملي على التطبيق العملي لأطر عمل GRC مثل NIST في إطار عمل متكامل. بدلاً من مجرد سرد اللوائح، للمشاركين فهمًا شاملاً لكيفية الكبرى، وبناء الضوابط الأمنية الفعالة. تقدم الدورة دراسات ، وكيفية استخدامها لتقييم المخاطر ٢٧٠٠١ ISO و نغوص في بين GRC وأهداف العمل مما يمنح المشاركين رؤى عملية حول كيفية التعامل حالة واقعية لتحديات GRC في المؤسسات على العليا. إنها ليست مجرد دورة نظرية، بل هي برنامج الاستراتيجية، وكيفية تقديم تقارير فعالة للإدارة معها. نركز على الربط حماية المؤسسات الكبرى وتعزيز حوكمتها. تدريبي مكثف يهدف إلى بناء قادة GRC قادرين