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



18 - 22 اكتوبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #CYB3092_397385

مقدمة الدورة التدريبية / لمحة عامة:

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

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- 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:

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

- فهم شامل لمبادئ إدارة المخاطر الأمنية والامتثال (GRC).
- القدرة على تطوير وتنفيذ برنامج GRC متكامل.
- تحديد وتقييم المخاطر الأمنية التي تواجه المؤسسة.
- تصميم وتطبيق الضوابط الأمنية اللازمة لتخفيف المخاطر.
- ضمان الامتثال للوائح والمعايير المحلية والدولية (مثل GDPR, ISO 27001).
- إعداد تقارير المخاطر والامتثال للإدارة العليا.
- تعزيز ثقافة الوعي بالمخاطر والامتثال داخل المؤسسة.

منهجية الدورة التدريبية:

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

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).
- تقييم المخاطر الأمنية (Risk Assessment) باستخدام أطر عمل (مثل FAIR).
- 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

- اللوائح الرئيسية (GDPR, HIPAA, SOX, PCI DSS) وتأثيرها.
- معايير الأمن الدولية (ISO 27001, 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.

الوحدة الرابعة: حوكمة أمن المعلومات والرقابة الداخلية

- 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.

الوحدة الخامسة: دمج GRC ومستقبل إدارة المخاطر الأمنية

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

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العميق والعملي على إدارة المخاطر الأمنية والامتثال (GRC)، مما يوفر للمشاركين فهمًا شاملاً لكيفية دمج هذه المفاهيم في إطار عمل متكامل. بدلاً من مجرد سرد اللوائح، نغوص في التطبيق العملي لأطر عمل GRC مثل NIST وISO 27001، وكيفية استخدامها لتقييم المخاطر وبناء الضوابط الأمنية الفعالة. تقدم الدورة دراسات حالة واقعية لتحديات GRC في المؤسسات الكبرى، مما يمنح المشاركين رؤى عملية حول كيفية التعامل معها. نركز على الربط بين GRC وأهداف العمل الاستراتيجية، وكيفية تقديم تقارير فعالة للإدارة العليا. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء قادة GRC قادرين على حماية المؤسسات الكبرى وتعزيز حوكمتها.