الدورة التدريبية: أمن المعلومات والحوكمة والامتثال وإدارة المخاطر (GRC)

19 - 23 اكتوبر 2026

ميونخ

5100 € (للشخص الواحد)

Ref: #SM5464_339550

مقدمة الدورة التدريبية / لمحة عامة:

تُعد أمن المعلومات والحوكمة والامتثال وإدارة المخاطر (GRC) ركائز أساسية لأي مؤسسة تسعى لضمان استمرارية أعمالها وحماية أصولها الرقمية في بيئة تتطور فيها التهديدات باستمرار. هذه الدورة التدريبية الشاملة مصممة لتزويد المشاركين بفهم عميق للمفاهيم والممارسات اللازمة لتطبيق إطار عمل GRC فعال، مما يضمن توافق الأمن مع الأهداف الاستراتيجية للمؤسسة. سنستعرض من خلالها كيفية بناء سياسات أمن معلومات قوية، وإدارة الامتثال للوائح الدولية والمحلية، وتقييم المخاطر السيبرانية والتخفيف منها بفعالية. تستند الدورة إلى أحدث المعايير وأفضل الممارسات العالمية، وتستلهم من أعمال رواد الفكر في هذا المجال مثل الدكتور Christopher Hodson Christopher Hodson، الذي يُعتبر مرجعًا في حوكمة أمن المعلومات. يقدم BIG BEN Training Center هذه الدورة لمساعدة المتخصصين والقادة على تطوير قدراتهم في إدارة أمن المعلومات بشكل استباقي، وتعزيز مرونة مؤسساتهم في مواجهة التحديات الأمنية المعقدة، مع التركيز على الجوانب التشغيلية والاستراتيجية لضمان أقصى حماية للأصول الحساسة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو أمن المعلومات.
- مسؤولو الامتثال.
- مديرو المخاطر.
- مدققو أمن المعلومات.
- مستشارو GRC.
- مديرو تقنية المعلومات.
- متخصصو الأمن السيبراني.
- القادة وصناع القرار.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- الرعاية الصحية.
- قطاع الاتصالات.
- القطاع الحكومي وما في حكمها.
- الصناعات الدفاعية.
- الاستشارات الأمنية.
- التكنولوجيا والبرمجيات.
- الطاقة والمرافق.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- إدارة المخاطر.
- القسم القانوني والامتثال.
- إدارة التدقيق الداخلي.
- إدارة تقنية المعلومات.
- الإدارة العليا.
- إدارة الحوكمة.

أهداف الدورة التدريبية:

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

- فهم العلاقة بين أمن المعلومات، والحوكمة، والامتثال، والمخاطر.
- تطوير وتنفيذ إطار عمل GRC شامل.
- تقييم وإدارة المخاطر الأمنية بشكل فعال.
- ضمان الامتثال للوائح والمعايير الدولية والمحلية.
- بناء سياسات وإجراءات أمن معلومات قوية.
- إدارة برامج التدقيق والتقييم لأمن المعلومات.
- تعزيز ثقافة الوعي الأمني داخل المؤسسة.
- تطبيق أفضل الممارسات في حوكمة أمن المعلومات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية متكاملة وتفاعلية، تهدف إلى بناء فهم عميق ومهارات عملية في مجال أمن المعلومات والحوكمة والامتثال وإدارة المخاطر (GRC). تتضمن المنهجية مزيجًا من المحاضرات التفاعلية التي يقدمها خبراء متخصصون في مجال GRC، تليها جلسات نقاش جماعية تتيح للمشاركين تبادل الخبرات والتحديات التي يواجهونها في بيئات عملهم. يتم التركيز بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المتدربون بتحليل سيناريوهات معقدة تتعلق بحوادث أمن المعلومات، تحديات الامتثال، وتقييم المخاطر، ثم يطورون حلولاً عملية. تشمل الدورة ورش عمل تطبيقية تسمح للمشاركين بتصميم أطر GRC، وصياغة سياسات أمنية، وإجراء تقييمات للمخاطر. يشجع BIG BEN Training Center المشاركة النشطة والتعاون بين المتدربين لتعزيز التفكير النقدي وتطوير حلول مبتكرة. يتم تقديم تغذية راجعة مستمرة وفردية لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من تطبيق أفضل الممارسات في مؤسساتهم وتعزيز قدرتها على إدارة المخاطر الأمنية بفعالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى حوكمة أمن المعلومات والامتثال والمخاطر

- مفاهيم GRC وأهميتها في البيئة الرقمية.
- العلاقة بين أمن المعلومات، الحوكمة، الامتثال، والمخاطر.
- أطر عمل GRC العالمية (مثل ISO 27000 series، COBIT).
- بناء استراتيجية GRC متكاملة.
- تحديات تطبيق GRC في المؤسسات الحديثة.
- الوعي بأهمية GRC على مستوى الإدارة العليا.
- القياس وتقييم فعالية برامج GRC.

الوحدة الثانية: إدارة مخاطر أمن المعلومات

- تحديد أنواع المخاطر الأمنية وتقييمها.
- منهجيات تقييم المخاطر (NIST SP 800-30).
- تحليل الثغرات الأمنية ونقاط الضعف.
- تطوير استراتيجيات تخفيف المخاطر.
- مراقبة المخاطر وإعداد تقارير المخاطر.
- إدارة مخاطر الطرف الثالث (Third-Party Risk Management).
- تحديد أولويات المخاطر واتخاذ القرارات المستنيرة.

الوحدة الثالثة: حوكمة أمن المعلومات والسياسات

- بناء هيكل حوكمة فعال لأمن المعلومات.
- تطوير سياسات وإجراءات أمن المعلومات.
- أهمية الأدوار والمسؤوليات في حوكمة الأمن.
- إدارة دورة حياة السياسات والإجراءات.
- التوعية الأمنية والتدريب للموظفين.
- ضمان الامتثال للسياسات الداخلية.
- المراجعة الدورية لفعالية الحوكمة.

الوحدة الرابعة: الامتثال للوائح والمعايير

- فهم اللوائح والقوانين المتعلقة بأمن المعلومات (GDPR, HIPAA, PCI DSS).
- تأثير الامتثال على استراتيجيات الأعمال.
- تطوير برامج الامتثال الفعالة.
- إدارة عمليات التدقيق الداخلي والخارجي.
- التعامل مع حالات عدم الامتثال والعقوبات.
- تتبع التغييرات في اللوائح والمعايير.
- أدوات وتقنيات الامتثال.

الوحدة الخامسة: عمليات GRC المتقدمة والتقنيات

- أتمتة GRC وتقنيات الذكاء الاصطناعي.
- تكامل GRC مع الأمن السيبراني.
- إدارة الاستجابة للحوادث الأمنية في إطار GRC.
- قياس أداء GRC وإعداد التقارير.
- التواصل الفعال حول GRC مع الأطراف المعنية.
- التوجهات المستقبلية في GRC.
- دراسات حالة متقدمة وتطبيق عملي لإطار 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:

كيف يمكن للمؤسسات أن توازن بفعالية بين تحقيق الأهداف التجارية الطموحة ومتطلبات الامتثال التنظيمية الصارمة والمتغيرة باستمرار في مجال أمن المعلومات؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتقديم منظور شامل ومتكامل لـ أمن المعلومات والحوكمة والامتثال وإدارة المخاطر (GRC)، مما يتجاوز مجرد التركيز على جانب واحد. نحن نقدم نهجًا شموليًا يربط بين هذه العناصر الحيوية، مما يمكّن المشاركين من فهم الصورة الكاملة وكيفية تأثير كل مكون على الآخر. تتميز الدورة بمحتواها الأكاديمي المتقدم المستند إلى أحدث المعايير العالمية، مع التركيز على التطبيقات العملية ودراسات الحالة الواقعية التي تعكس التحديات الحقيقية التي تواجه المؤسسات اليوم. بدلاً من مجرد سرد النظريات، نقدم أدوات وتقنيات عملية يمكن للمشاركين تطبيقها فورًا في بيئات عملهم. يقدم BIG BEN Training Center هذه الدورة بخبرة عميقة، مما يضمن أن يكتسب المتدربون فهمًا نظريًا وعمليًا يميزهم في سوق العمل، ويؤهلهم لقيادة مبادرات GRC بنجاح داخل مؤسساتهم، وتعزيز مرونة أعمالهم وحمايتها من التهديدات المتزايدة.