الدورة التدريبية: الأمن السيبراني وحوكمة البيانات في رحلة التحول الرقمي



19 - 23 اكتوبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #DT4227_325201

مقدمة الدورة التدريبية / لمحة عامة:

في عصر التحول الرقمي المتسارع، أصبحت البيانات هي المحرك الأساسي للاقتصاد الحديث، بينما يمثل الأمن السيبراني الحصن المنيع الذي يحمي هذه البيانات والأصول الرقمية للمؤسسات. لم يعد كافيًا مجرد تبني التقنيات الحديثة، بل أصبح من الضروري وضع استراتيجيات قوية لـ حوكمة البيانات وضمان الأمن السيبراني للحفاظ على الثقة والامتثال وحماية الأصول الحيوية. تقدم هذه الدورة التدريبية الشاملة من BIG BEN Training Center، رؤى معمقة حول العلاقة المتكاملة بين الأمن السيبراني وحوكمة البيانات في سياق التحول الرقمي، بدءًا من فهم التهديدات المعاصرة وصولًا إلى بناء أطر عمل متينة. سيتمكن المشاركون من استكشاف كيفية تصميم وتنفيذ سياسات حوكمة البيانات الفعالة، وتقييم المخاطر السيبرانية، وتطبيق أفضل الممارسات في حماية الأنظمة والشبكات. تتناول الدورة مفاهيم حيوية مثل خصوصية البيانات، الامتثال للوائح (مثل GDPR)، إدارة الهوية والوصول، والاستجابة للحوادث السيبرانية. تعتمد الدورة على منهجية متكاملة تجمع بين المعرفة النظرية والتطبيق العملي، مستلهمة من أعمال خبراء مرموقين في هذا المجال مثل بروس شناير (Bruce Schneier)، الذي ساهم بشكل كبير في فهم تعقيدات الأمن السيبراني. إن فهم هذه المفاهيم وتطبيقها بشكل استراتيجي يضمن المرونة والقدرة على الاستمرارية في البيئة الرقمية المتغيرة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء تقنية المعلومات والأمن السيبراني.
- مسؤولو حوكمة البيانات والامتثال.
- مدراء التحول الرقمي.
- المتخصصون في أمن المعلومات.
- مدراء المخاطر.
- المستشارون في مجال البيانات والأمن.
- المدراء التنفيذيون وأعضاء مجالس الإدارة.
- مدراء المشاريع التقنية.
- مدققو الأنظمة.
- المحللون الأمنيون.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الاتصالات.
- القطاع الحكومي.
- قطاع الرعاية الصحية.
- قطاع التكنولوجيا والبرمجيات.
- قطاع التجارة الإلكترونية.
- قطاع الطاقة.
- قطاع الخدمات اللوجستية.
- القطاع التعليمي.
- قطاع التأمين.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة الأمن السيبراني.
- إدارة المخاطر والامتثال.
- إدارة البيانات.
- الإدارة القانونية.
- إدارة التحول الرقمي.
- إدارة العمليات.
- إدارة المراجعة الداخلية.
- إدارة تطوير المنتجات.
- إدارة الشؤون التنظيمية.

أهداف الدورة التدريبية:

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

- فهم العلاقة الجوهرية بين الأمن السيبراني وحوكمة البيانات.
- تحديد التحديات الأمنية الرئيسية في عصر التحول الرقمي.

- صياغة وتطبيق سياسات حوكمة البيانات الفعالة.
- تقييم المخاطر السيبرانية وتطوير استراتيجيات التخفيف.
- تصميم وتنفيذ برامج شاملة لـ الأمن السيبراني.
- الامتثال للوائح العالمية والمحلية المتعلقة بخصوصية البيانات.
- إدارة الهوية والوصول بشكل آمن وفعال.
- وضع خطط للاستجابة للحوادث السيبرانية والتعافي منها.
- تطبيق مبادئ أمن البيانات في جميع مراحل دورة حياة البيانات.
- بناء ثقافة مؤسسية واعية بـ الأمن السيبراني وحوكمة البيانات.
- الاستفادة من التقنيات المتقدمة في حماية الأصول الرقمية.
- فهم أهمية إدارة الثغرات ونقاط الضعف.

منهجية الدورة التدريبية:

يقدم BIG BEN Training Center هذه الدورة بمنهجية متكاملة تجمع بين الشرح النظري المتعمق والتطبيقات العملية، لضمان استيعاب شامل لمفاهيم الأمن السيبراني وحوكمة البيانات. تعتمد المنهجية على محاضرات تفاعلية تستعرض أحدث التهديدات الأمنية، التقنيات الدفاعية، وأفضل الممارسات في حوكمة البيانات. يتم إثراء المحتوى بتحليل دراسات حالة واقعية لحوادث سيبرانية شهيرة وكيفية التعامل معها، بالإضافة إلى أمثلة تطبيقية لأطر عمل حوكمة البيانات الفعالة. تتضمن الدورة ورش عمل تفاعلية تتيح للمشاركين فرصة تصميم سياسات أمنية، تحليل مخاطر، ووضع خطط استجابة للحوادث. كما يتم تشجيع النقاش وتبادل الخبرات بين المشاركين لتعزيز فهمهم للتحديات التي تواجه المؤسسات في هذا المجال. تهدف هذه المنهجية إلى تمكين المشاركين من تطوير القدرات اللازمة لحماية البيانات الحساسة، وضمان الامتثال التنظيمي، وبناء بنية تحتية رقمية آمنة وموثوقة تدعم رحلة التحول الرقمي لمؤسساتهم.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني وحوكمة البيانات.

- مقدمة إلى الأمن السيبراني وتطوره.
- مفهوم حوكمة البيانات وأهميتها الاستراتيجية.
- العلاقة المتكاملة بين الأمن السيبراني وحوكمة البيانات.
- أنواع التهديدات السيبرانية الشائعة.
- مبادئ حماية البيانات (السرية، السلامة، التوافر).
- تحديات إدارة البيانات الضخمة وأمنها.
- الوعي بأهمية الأمن في عصر التحول الرقمي.

الوحدة الثانية: أطر عمل الأمن السيبراني وإدارة المخاطر.

- أطر عمل الأمن السيبراني العالمية (مثل NIST, ISO 27001).
- تقييم المخاطر السيبرانية وتحليل الثغرات.
- إدارة نقاط الضعف والتهديدات.
- تطوير سياسات وإجراءات الأمن السيبراني.
- بناء خطة استجابة للحوادث السيبرانية.
- التعافي من الكوارث واستمرارية الأعمال.
- مؤشرات الأداء الرئيسية لـ الأمن السيبراني.

الوحدة الثالثة: حوكمة البيانات والامتثال التنظيمي.

- مبادئ حوكمة البيانات الفعالة.
- دور حوكمة البيانات في اتخاذ القرارات.
- لوائح حماية البيانات (GDPR, CCPA).
- أهمية خصوصية البيانات وحمايتها.
- تصنيف البيانات وإدارتها.
- مراجعة الامتثال والتدقيق.
- بناء إطار قانوني وتنظيمي لـ البيانات.

الوحدة الرابعة: حماية البنية التحتية والأنظمة الرقمية.

- أمن الشبكات والاتصالات.
- أمن تطبيقات الويب والخدمات السحابية.
- إدارة الهوية والوصول (IAM).
- التشفير وأنواع خوارزميات التشفير.
- أمن نقطة النهاية والأجهزة المحمولة.
- نظم كشف ومنع الاختراقات (IDS/IPS).
- أمن الحوسبة السحابية وحماية البيانات.

الوحدة الخامسة: ثقافة الأمن السيبراني ومستقبل حوكمة البيانات.

- بناء ثقافة واعية بـ الأمن السيبراني في المؤسسات.
- برامج التوعية والتدريب على الأمن.
- دور القيادة في تعزيز الأمن وحوكمة البيانات.
- الاتجاهات المستقبلية في الأمن السيبراني.
- الذكاء الاصطناعي في تعزيز الأمن السيبراني.
- أخلاقيات البيانات واستخدامها المسؤول.
- صياغة خطة عمل شخصية لتعزيز الأمن وحوكمة البيانات.

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 ظل التطور المتسارع لتهديدات الأمن السيبراني وظهور تقنيات جديدة، كيف يمكن للمؤسسات أن تضمن أن أطر حوكمة البيانات لديها تظل مرنة بما يكفي للتكيف مع هذه التحديات مع الحفاظ على الامتثال الصارم للوائح المتغيرة باستمرار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية من BIG BEN Training Center بتقديمها منظورًا فريدًا يربط بين الأمن السيبراني وحوكمة البيانات، وهما مجالان حيويان لنجاح أي تحول رقمي. بخلاف الدورات التي تركز على أحد الجانبين فقط، توفر هذه الدورة فهمًا متكاملًا لكيفية بناء استراتيجيات دفاعية قوية وفي نفس الوقت ضمان الاستخدام المسؤول والأخلاقي لـ البيانات. نركز على الأمثلة العملية ودراسات الحالة التي توضح التحديات والحلول في سيناريوهات واقعية، مما يمنح المشاركين رؤى قابلة للتطبيق مباشرة. تهدف الدورة إلى تمكين القادة والمتخصصين من حماية أصولهم الرقمية، والامتثال للمتطلبات التنظيمية، وبناء ثقة العملاء من خلال إدارة البيانات بشكل آمن وفعال. نقدم منهجية شاملة تتيح للمشاركين تطوير خطط عمل عملية لتعزيز الأمن السيبراني وحوكمة البيانات في مؤسساتهم.