BLACKBIRD FOR TRAINING

# حوكمة الأمن السيبراني وإدارة المخاطر والامتثال

22 – 26 نوفمبر 2026

أون لاين

UK Traininig

PARTNER

www.blackbird-training.com

# حوكمة الأمن السيبراني وإدارة المخاطر والامتثال

**المرجع:** 322001_3254809 **التاريخ:** 22 – 26 نوفمبر 2026 **المكان:** أون لاين **الرسوم:** GBP 2700

## مقدمة

في ظل التحول الرقمي السريع، أصبحت حوكمة الأمن السيبراني أولوية قصوى للمؤسسات التي تسعى لحماية أصولها الرقمية، وضمان الامتثال التنظيمي، وإدارة المخاطر الإلكترونية بفعالية. تم تصميم هذه الدورة التدريبية الشاملة لتزويد المهنيين بالمهارات اللازمة لإدارة حوكمة الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، وإطار الامتثال GRC وفقًا للمعايير العالمية مثل NIST، GDPR، ISO 27001، وCOBIT.

سيتعلم المشاركون كيفية تصميم وتنفيذ برامج GRC متكاملة، إجراء تحليل للمخاطر، وضمان الامتثال التنظيمي من خلال دراسات حالة واقعية، محاكاة عملية، وتمارين تطبيقية. هذا البرنامج يُمكّن المشاركين من تحديد وتقييم المخاطر السيبرانية بفعالية، مما يضمن حلول حوكمة الأمن السيبراني التي تدعم استمرارية الأعمال وثقة الجهات الرقابية.

## أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- فهم المبادئ الأساسية لحوكمة الأمن السيبراني وكيفية مواءمتها مع الاستراتيجية التنظيمية.
- تطبيق المتطلبات القانونية والتنظيمية الوطنية والدولية في أمن المعلومات والامتثال للأمن السيبراني.
- تصميم وتنفيذ إطار عمل متكامل لإدارة الحوكمة والمخاطر والامتثال GRC وفقًا لمعايير الامتثال السيبراني العالمي.
- إجراء تحليل المخاطر السيبرانية لتحديد نقاط الضعف ووضع استراتيجيات فعالة للتخفيف منها.
- تعزيز نضج الأمن السيبراني من خلال المراقبة المستمرة، وإعداد التقارير، والاستعداد للتدقيق الأمني.
- التواصل بفعالية مع القيادات وأصحاب المصلحة حول استراتيجيات حوكمة الأمن السيبراني.

## محاور الدورة

### اليوم الأول: أساسيات حوكمة الأمن السيبراني

- مقدمة عن حوكمة الأمن السيبراني وأهميتها الاستراتيجية.
- نظرة عامة على الأطر العالمية مثل: NIST، ISO 27001، COBIT.
- تحديد الأدوار والمسؤوليات والمساءلة ضمن هياكل GRC.
- تطوير استراتيجيات وسياسات الأمن السيبراني التنظيمية.
- دمج الحوكمة مع إدارة تقنية المعلومات IT Governance لتعزيز الامتثال السيبراني.

### اليوم الثاني: مبادئ إدارة المخاطر السيبرانية

- فهم دورة حياة إدارة مخاطر الأمن السيبراني.
- تقنيات تحديد وتقييم المخاطر السيبرانية في مختلف البيئات.
- اختيار استراتيجيات معالجة المخاطر وتخفيفها بفعالية.
- مقارنة بين التقييم الكمي والنوعي للمخاطر.
- استخدام سجلات المخاطر ولوحات التحكم البصرية لمتابعة مستمرة واتخاذ قرارات مدروسة.

### اليوم الثالث: الامتثال والجوانب القانونية

- نظرة عامة على المعايير التنظيمية العالمية: SOX، HIPAA، GDPR.
- معالجة المسائل القانونية والأخلاقية في الامتثال السيبراني.
- الاستعداد لإدارة عمليات التدقيق الأمني Audit بفعالية.
- فهم لوائح الخصوصية ومتطلبات التعامل مع البيانات.
- مواءمة الامتثال مع الاستراتيجية المؤسسية والعمليات التشغيلية.

### اليوم الرابع: تفعيل الحوكمة وإدارة المخاطر والامتثال GRC

- بناء وصيانة برنامج GRC للأمن السيبراني يتماشى مع المعايير العالمية.
- أتمتة عمليات الامتثال وإدارة المخاطر باستخدام أدوات GRC.
- التخطيط للاستجابة للحوادث الأمنية وإدارة الأزمات السيبرانية بفاعلية.
- دمج GRC مع استمرارية الأعمال BCP واستراتيجيات التعافي من الكوارث DRP.
- التواصل الفعّال حول وضع GRC والمخاطر مع المديرين التنفيذيين ومجالس الإدارة.

## اليوم الخامس: دراسات حالة، التقييم، وخطة الطريق

- مراجعة تطبيقات واقعية لإدارة GRC في الأمن السيبراني.
- إجراء تقييم مخاطر سيبرانية محاكي وتحديد الضوابط المناسبة.
- ورشة عمل جماعية: تصميم إطار عمل مخصص لـ GRC.
- اختبار معرفي وخيار امتحان الشهادة.
- إعداد خطة طريق شخصية أو تنظيمية لـ GRC لتعزيز التخطيط الاستراتيجي.

## لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- إتقان حوكمة الأمن السيبراني: اكتساب فهم عميق لكيفية تطبيق حوكمة الأمن السيبراني بما يتماشى مع الأهداف الاستراتيجية للمؤسسة.
- تطوير استراتيجيات فعّالة لإدارة مخاطر الأمن السيبراني: تعلم كيفية تحديد، تقييم، وتخفيف المخاطر السيبرانية بشكل استباقي.
- تعزيز الامتثال العالمي للأمن السيبراني: تطبيق المعايير الدولية مثل NIST ،ISO 27001، وGDPR بثقة.
- ضمان الثقة التنظيمية: الاستعداد لعمليات التدقيق الأمني والحفاظ على الامتثال التنظيمي بشكل دائم.
- تعزيز استمرارية الأعمال: ضمان استمرارية العمل من خلال إدارة الحوكمة بفعالية، والتخطيط لمواجهة الكوارث السيبرانية.
- التواصل الأمني الفعّال: تطوير القدرة على إعداد التقارير الأمنية وشرح مستويات المخاطر لأصحاب القرار.

## الخاتمة

تعد هذه الدورة استثمارًا هامًا للمهنيين العاملين في الأمن السيبراني، إدارة المخاطر التقنية، التدقيق، والامتثال.
تزود المشاركين بالمعرفة والأدوات اللازمة لتصميم وتنفيذ برامج GRC فعّالة تتماشى مع المعايير العالمية لحوكمة الأمن السيبراني.

بنهاية البرنامج، سيكون المشاركون قادرين على قيادة بيئات رقمية آمنة ومتوافقة مع المعايير، مما يدعم استمرارية الأعمال، الثقة التنظيمية، والمرونة على المدى الطويل.

**انضم الآن لتصبح قائدًا في حوكمة الأمن السيبراني، وتمتلك المهارات اللازمة لحماية أصول مؤسستك الرقمية، وضمان الامتثال، وتخفيف المخاطر بفعالية.**