BLACKBIRD FOR TRAINING

# دورة إدارة مخاطر الأمن السيبراني والالتزام المؤسسي



**دورة إدارة مخاطر الأمن السيبراني والالتزام المؤسسي**

## مقدمة

تقدم هذه الدورة إطاراً عملياً ومنهجياً لإدارة مخاطر الأمن السيبراني وضمان الالتزام بالضوابط والسياسات المؤسسية.

تركز على تمكين المشاركين من فهم المخاطر الرقمية وتأثيرها المباشر على استمرارية الأعمال واتخاذ القرار الإداري.

تعالج الدورة كيفية الانتقال من رد الفعل بعد وقوع الحوادث إلى إدارة استباقية قائمة على التحليل والتقييم المنتظم.

تستهدف الدورة القيادات التنفيذية، ومديري الإدارات، ومسؤولي الأمن السيبراني، وإدارات التدقيق والحوكمة، ومديري المشاريع، والمتخصصين في الامتثال وإدارة المخاطر.

كما تخدم العاملين في القطاعات التي تعتمد على حماية البيانات والأنظمة الحيوية واستقرار العمليات.

توفر الدورة أدوات عملية لتحديد الأصول الحساسة، وتحليل مصادر التهديد، وقياس حجم التأثير، وبناء خطط معالجة فعالة.

يساعد محتواها على رفع مستوى النضج المؤسسي في إدارة المخاطر، وتحسين جودة التقارير المرفوعة للإدارة العليا، وتعزيز ثقافة الالتزام داخل المؤسسة.

## أهداف الدورة

تهدف الدورة إلى بناء قدرات تحليلية وتطبيقية تمكن المشاركين من إدارة المخاطر السيبرانية بشكل منهجي ومنظم.

- التعرف على المفاهيم الأساسية لإدارة مخاطر الأمن السيبراني.
- تحليل مصادر التهديد ونقاط الضعف داخل المؤسسة.
- تقييم أثر المخاطر على العمليات والأصول الحيوية.
- تطبيق أساليب قياس المخاطر بصورة كمية ونوعية.
- إعداد سجل مخاطر محدث وواضح.
- ترتيب أولويات المعالجة وفق مستوى التأثير والاحتمالية.
- ربط إدارة المخاطر بسياسات الحوكمة والرقابة الداخلية.
- إعداد تقارير مخاطر موجهة للإدارة العليا بلغة واضحة.
- متابعة مؤشرات المخاطر وتحليل نتائجها بشكل دوري.
- تعزيز ثقافة الالتزام والمسؤولية داخل بيئة العمل.



## محاور الدورة

### اليوم الأول: المفاهيم الأساسية وإطار إدارة المخاطر.

- تعريف مفهوم المخاطر في سياق الأمن السيبراني.
- تحديد الأصول الحرجة داخل المؤسسة.
- تصنيف المعلومات وفق مستويات الحساسية.
- التعرف على أنواع التهديدات الداخلية والخارجية.
- فهم العلاقة بين المخاطر والأهداف الاستراتيجية.
- دراسة حالات تطبيقية توضح آثار ضعف إدارة المخاطر.
- تنفيذ تمرين عملي لتحديد الأصول والتهديدات.

### اليوم الثاني: تقييم المخاطر وتحليلها.

- شرح أساليب القياس الكمي والنوعي للمخاطر.
- إعداد مصفوفة لتصنيف المخاطر.
- حساب احتمالية الحدوث وتأثيره على العمليات.
- ترتيب المخاطر وفق مستوى الأولوية.
- تحليل الفجوات بين الوضع الحالي والمستهدف.
- إعداد تقرير تقييم شامل.
- تطبيق عملي على تحليل حادث افتراضي.

### اليوم الثالث: الالتزام والرقابة المؤسسية.

- توضيح مفهوم الالتزام بالأنظمة والسياسات.
- ربط إدارة المخاطر بالحوكمة المؤسسية.
- تحديد المتطلبات الرقابية الأساسية.
- تقييم مستوى الالتزام الحالي داخل المؤسسة.
- إعداد خطة لمعالجة فجوات الالتزام.
- دراسة أثر عدم الالتزام على السمعة والثقة.
- تمرين إعداد سياسة مختصرة لإدارة المخاطر.



## اليوم الرابع: بناء برنامج متكامل لإدارة المخاطر.

- تصميم إطار شامل لإدارة المخاطر.
- تحديد الأدوار والمسؤوليات بوضوح.
- وضع آلية متابعة دورية للمخاطر.
- إعداد مؤشرات أداء لقياس مستوى التعرض للمخاطر.
- تطوير آلية رفع التقارير للإدارة العليا.
- إعداد لوحة متابعة للمؤشرات.
- تطبيق عملي لبناء برنامج مؤسسي متكامل.

## اليوم الخامس: التطبيق العملي والتقييم.

- مراجعة شاملة للمفاهيم والمحاور الرئيسية.
- مناقشة التحديات عند التطبيق العملي.
- عرض مشاريع تطبيقية من المشاركين.
- تقييم مستوى التحليل وإعداد خطط المعالجة.
- إعداد خطة عمل فردية للتنفيذ داخل المؤسسة.
- مناقشة آليات التحسين المستمر.
- تقديم تغذية راجعة منهجية لكل مشارك.

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

- تعزيز القدرة على اتخاذ قرارات مبنية على تحليل دقيق للمخاطر.
- رفع مستوى الالتزام التنظيمي داخل المؤسسة.
- تقليل احتمالية الخسائر الناتجة عن الحوادث السيبرانية.
- تحسين جودة التقارير الموجهة للإدارة العليا.
- دعم استمرارية الأعمال وتقليل الانقطاعات التشغيلية.
- رفع مستوى الجاهزية والاستجابة للمخاطر.
- تعزيز ثقة الجهات الرقابية وأصحاب المصلحة.
- بناء ثقافة مؤسسية قائمة على الوعي بالمخاطر.



## الخاتمة

تمثل هذه الدورة برنامجاً منهجياً متكاملاً لإدارة مخاطر الأمن السيبراني والالتزام المؤسسي داخل المؤسسات الحديثة.تجمع بين التحليل المنظم، والتطبيق العملي، والربط المباشر بين المخاطر والاستراتيجية المؤسسية. تساعد المشاركين على بناء رؤية واضحة للمخاطر، وتقييم أثرها، ووضع خطط معالجة قابلة للتنفيذ.يساهم تطبيق ما يتم تعلمه في تحسين جودة القرارات الإدارية، ورفع مستوى الحوكمة، وتعزيز استقرار العمليات. كما يدعم بناء ثقافة تنظيمية واعية بالمخاطر وقادرة على التعامل مع التحديات الرقمية المتسارعة.

**إن إدارة المخاطر لم تعد خياراً ثانوياً، بل أصبحت جزءاً أساسياً من منظومة النجاح المؤسسي واستدامة الأعمال.توفر هذه الدورة الأساس العملي لبناء برنامج فعال ومستدام يحقق التوازن بين التطوير والحماية.**

