

# دورة إدارة مخاطر تكنولوجيا المعلومات والأمن السيبراني على مستوى المؤسسة

21 – 25 يونيو 2027

برشلونة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# دورة إدارة مخاطر تكنولوجيا المعلومات والأمن السيبراني على مستوى المؤسسة

**المرجع:** 80022_36392 **التاريخ:** 21 – 25 يونيو 2027 **المكان:** برشلونة **الرسوم:** Euro 5700

## نظرة عامة

تعنى إدارة مخاطر تكنولوجيا المعلومات على مستوى المؤسسة بتحديد حجم المخاطر التقنية والسيبرانية التي تقبل المؤسسة تحملها، ومن يملكها، وكيف يطلع عليها مجلس الإدارة. تتناول هذه الدورة مخاطر تكنولوجيا المعلومات والأمن السيبراني بوصفها محفظة واحدة تشمل المؤسسة كلها، لا تطبيقا منفردا في كل مرة. يربط المشاركون مبادئ ISO 31000 وأهداف الحوكمة في COBIT وإطار NIST Cybersecurity Framework 2.0 في نموذج تشغيلي واحد: تحديد الرغبة في المخاطر وحدود التحمل، وإدارة سجل مؤسسي لمخاطر تكنولوجيا المعلومات، ومواءمة الضوابط مع أهداف الأعمال، والتخطيط لاستمرارية الأعمال والتعافي، ورفع تقارير التعرض السيبراني بلغة تساعد الإدارة العليا على اتخاذ القرار. وتستشرف الأيام الأخيرة مخاطر الحوسبة السحابية وإنترنت الأشياء والذكاء الاصطناعي وبرامج الفدية. تقدم هذه الدورة من أجايل للتدريب.

## الفئة المستهدفة

- مديرو تكنولوجيا المعلومات ورؤساء البنية التحتية
- مسؤولو أمن المعلومات ومديرو برامج الأمن السيبراني
- مختصو إدارة المخاطر المؤسسية والحوكمة والامتثال المعنيون بالمخاطر التقنية
- منسقو استمرارية الأعمال والمرونة المؤسسية
- المدققون الداخليون ومديرو الامتثال المراجعون لحوكمة تكنولوجيا المعلومات

## الإدارات والقطاعات المستهدفة

تناسب كل جهة يلزمها حوكمة المخاطر التقنية والسيبرانية ورفع التقارير عنها على مستوى المؤسسة كلها.

- مكاتب الحوكمة والمخاطر والامتثال
- الأمن السيبراني وعمليات تكنولوجيا المعلومات
- وحدات استمرارية الأعمال وإدارة الأزمات
- البنوك والتأمين والخدمات المالية
- الطاقة والقطاع الحكومي والرعاية الصحية والتجزئة والتجارة الإلكترونية

AGILE LEADERS
Training Center

## أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تطبيق ISO 31000 وCOBIT وإطار NIST Cybersecurity Framework معا في عملية مؤسسية واحدة لإدارة مخاطر تكنولوجيا المعلومات.
- تحديد الرغبة في المخاطر التقنية والسيبرانية وحدود التحمل وملكية المخاطر عبر وحدات الأعمال.
- تقييم محفظة المخاطر التقنية للمؤسسة باستخدام الخرائط الحرارية والسيناريوهات ومؤشرات المخاطر الرئيسية.
- تطوير استراتيجيات معالجة تجمع الضوابط الوقائية والكشفية والتصحيحية مع خطط استمرارية الأعمال.
- إعداد تقارير ولوحات متابعة لمخاطر تكنولوجيا المعلومات موجهة لمجلس الإدارة تدعم قرارات الاستثمار.
- تقييم المخاطر الناشئة من الخدمات السحابية وإنترنت الأشياء والذكاء الاصطناعي وبرامج الفدية.

## جدول الدورة

### اليوم 1: أسس مخاطر تكنولوجيا المعلومات المؤسسية

- أنواع المخاطر التقنية والسيبرانية ومصادرها وأثرها على الأعمال
- الرغبة في المخاطر وحدود التحمل والمخاطر المتبقية على مستوى المؤسسة
- مبادئ ISO 31000 وإطاره وعمليته
- موقع مخاطر تكنولوجيا المعلومات ضمن إدارة المخاطر المؤسسية
- المتطلبات التنظيمية ومتطلبات الامتثال للمخاطر التقنية

### اليوم 2: الأطر وهياكل الحوكمة

- أهداف الحوكمة والإدارة في COBIT المتعلقة بالمخاطر
- الوظائف الست في NIST Cybersecurity Framework 2.0
- ربط الأطر بمجموعة ضوابط موحدة
- نموذج خطوط الدفاع الثلاثة واللجان وملكية المخاطر
- السياسات والمعايير التي تحول الرغبة في المخاطر إلى قواعد

## اليوم 3: تحليل المخاطر المؤسسية ومعالجتها

- بناء سجل مؤسسي لمخاطر تكنولوجيا المعلومات وتحديثه
- تحليل السيناريوهات والخرائط الحرارية عبر وحدات الأعمال
- خيارات المعالجة ومواءمتها مع أهداف الأعمال
- محافظ الضوابط الوقائية والكشفية والتصحيحية
- المخاطر التقنية للأطراف الثالثة وسلاسل الإمداد

## اليوم 4: المرونة والمتابعة والتقارير لمجلس الإدارة

- تخطيط استمرارية الأعمال والتعافي من كوارث تكنولوجيا المعلومات
- الجاهزية للاستجابة للحوادث والتواصل في الأزمات
- مؤشرات المخاطر الرئيسية والمتابعة المستمرة للمخاطر
- تصميم لوحات متابعة للإدارة التنفيذية ومجلس الإدارة
- ربط تقارير المخاطر بالميزانيات وقرارات الاستثمار

## اليوم 5: المخاطر التقنية الناشئة

- البيئات السحابية والهجينة: المسؤولية المشتركة ومخاطر التركز
- التعرض في إنترنت الأشياء والتقنيات التشغيلية
- مخاطر الذكاء الاصطناعي وتعلم الآلة
- الاستعداد لبرامج الفدية والتعافي منها والتأمين السيبراني
- بناء خارطة طريق لرفع نضج برنامج مخاطر تكنولوجيا المعلومات

## التمارين التطبيقية

يعمل المشاركون في فرق على شركة افتراضية متوسطة الحجم لتنفيذ الأنشطة المقترحة التالية.

- نشاط مقترح: صياغة بيان للرغبة في المخاطر التقنية والسيبرانية مع حدود تحمل لثلاث وحدات أعمال.
- نشاط مقترح: ربط الضوابط الحالية للشركة بأهداف COBIT ووظائف NIST Cybersecurity Framework.
- نشاط مقترح: تنفيذ ورشة سيناريو لهجوم فدية واختبار خطة الاستمرارية والتعافي في مواجهته.
- نشاط مقترح: إعداد تقرير مخاطر من صفحة واحدة لمجلس الإدارة يتضمن مؤشرات المخاطر الرئيسية وخارطة المعالجة.

AGILE LEADERS
Training Center

## الأسئلة الشائعة

### ما الفرق بين هذه الدورة وتقييم مخاطر نظام تقني واحد؟

تعمل هذه الدورة على مستوى المؤسسة: الرغبة في المخاطر والحوكمة والمحفظة والاستمرارية والتقارير لمجلس الإدارة، ولا تتناول التقييم الفني لنظام منفرد خطوة بخطوة.

### هل أحتاج إلى خلفية فنية في أمن المعلومات؟

لا. تفيد المعرفة بعمليات تكنولوجيا المعلومات أو مفاهيم المخاطر، لكن المحتوى موجه للمديرين وأدوار الحوكمة.

### ما الأطر التي تغطيها الدورة؟

ISO 31000 وCOBIT وإطار NIST Cybersecurity Framework، وتستخدم معا لا كل منها على حدة.

### الخلاصة

يغادر المشاركون بنموذج عملي لإدارة مخاطر تكنولوجيا المعلومات على مستوى المؤسسة: رغبة واضحة في المخاطر، وأطر مشتركة، وسجل مخاطر حي، وخطط استمرارية مختبرة، وتقارير يستطيع مجلس الإدارة البناء عليها، بما يعزز حوكمة الأمن السيبراني في مؤسساتهم.