الحوكمة الاستراتيجية لمخاطر تقنية المعلومات والأمن السيبراني لقادة المجالس

26 - 30 Oct 2026

براغ

AGILE LEADERS
Training Center

الحوكمة الاستراتيجية لمخاطر تقنية المعلومات والأمن السيبراني لقادة المجالس

المرجع: 103600459_81147 التاريخ: 26 - 30 Oct 2026 الموقع: براغ الرسوم: 6000 Euro

نظرة عامة على الدورة

يمكّن هذا البرنامج التنفيذي المتقدم مديري الأمن السيبراني وكبار قادة تقنية المعلومات من قيادة وحوكمة وتقييم مبادرات الأمن السيبراني ومخاطر تقنية المعلومات على مستوى المؤسسة بشكل استراتيجي. ويؤكد على مواءمة الأمن السيبراني مع الأهداف التنظيمية، وأطر المرونة، والالتزامات التنظيمية. سيتعلم المشاركون كيفية تقييم الوضع العام للمخاطر في المؤسسة، وإنشاء آليات الحوكمة، وتوصيل قيمة الأمن السيبراني إلى مجالس الإدارة وأصحاب المصلحة.

من خلال المحاكاة القائمة على السيناريوهات، ودراسات الحالة، وحوارات القيادة، سيصقل المديرون قدرتهم على الإشراف على استراتيجية الأمن السيبراني، ودمج الأطر مثل NIST وISO 27001 وCOBIT 2019، وتوجيه برامج إدارة المخاطر متعددة الوظائف التي تعزز المرونة والامتثال والثقة الرقمية.

الجمهور المستهدف

- كبار مسؤولي أمن المعلومات CISOs
- مديرو الأمن السيبراني وكبار المديرين
- قادة مخاطر وحوكمة تقنية المعلومات
- المدراء التنفيذيون لإدارة مخاطر المؤسسة
- أعضاء مجلس الإدارة المشرفون على تقنية المعلومات والأمن الرقمي

الاقسام المستهدفة

- الأمن السيبراني وحوكمة المخاطر
- استراتيجية تقنية المعلومات وهندسة المؤسسة
- استمرارية الأعمال والتعافي من الكوارث
- الحوكمة والمخاطر والامتثال GRC
- إدارة أمن المعلومات

القطاعات المستهدفة

- الحكومة والبنية التحتية الحيوية
- البنوك والتمويل والتأمين
- الرعاية الصحية والمستحضرات الصيدلانية
- الطاقة والمرافق
- التكنولوجيا والاتصالات

AGILE LEADERS
Training Center

أهداف الدورة:

بنهاية هذا البرنامج، سيتمكن المشاركون من:

- قيادة حوكمة الأمن السيبراني والإشراف على المخاطر عبر مجالات المؤسسة.
- مواءمة استراتيجية الأمن السيبراني مع استمرارية الأعمال والامتثال ورغبة المخاطرة.
- تقييم وتحديد أولويات استثمارات الأمن السيبراني للمؤسسة.
- تصميم لوحة معلومات لمخاطر الأمن السيبراني جاهزة للمجلس باستخدام مؤشرات أداء رئيسية قابلة للقياس.
- تطوير وحوكمة أطر مرونة متعددة الطبقات للأنظمة البيئية الرقمية الحديثة.
- الإشراف على الاستجابة والتعافي من الحوادث السيبرانية الاستراتيجية بأقل قدر من التعطيل.

منهجية التدريب

- محاكاة استراتيجية وسيناريوهات قيادية واقعية
- تمارين الطاولة لأزمات الأمن السيبراني وعروض تقديمية للمجلس
- تحليل قائم على الأطر ISO 31000, CSF NIST, COBIT 2019
- دراسات حالة من حوادث الأمن السيبراني العالمية الكبرى
- مناقشات الأقران حول نماذج نضج الحوكمة

أدوات الدورة

- قائمة تدقيق حوكمة الأمن السيبراني للمؤسسة
- قوالب خريطة المخاطر ونموذج النضج لتقنية المعلومات
- دليل الاتصال والإبلاغ عن أزمات الأمن السيبراني
- مجموعة أدوات إحاطة المجلس وقالب مقاييس لوحة المعلومات
- إطار عمل تطوير استراتيجية المرونة

محتوى الدورة:

اليوم الأول: قيادة الأمن السيبراني وأسس الحوكمة

- الموضوع 1: المشهد المتطور للتهديدات السيبرانية: منظور المدير
- الموضوع 2: نماذج الحوكمة: تكامل CSF NIST، COBIT 2019، ISO 27001
- الموضوع 3: تحديد رؤية الأمن السيبراني ورسالته ورغبة المخاطرة
- الموضوع 4: إنشاء إشراف المجلس ولجان حوكمة الأمن السيبراني
- الموضوع 5: أدوار ومسؤوليات ومساءلة مديري الأمن السيبراني
- الموضوع 6: دراسة حالة: إخفاقات حوكمة المجلس والدروس المستفادة
- تأمل ومراجعة: رؤى قيادية حول حوكمة الأمن السيبراني الاستراتيجية

اليوم الثاني: تقييم المخاطر الاستراتيجية ومرونة المؤسسة

- الموضوع 1: أطر تحديد أولويات ومخاطر الأمن السيبراني
- الموضوع 2: التقييم الكمي المتقدم للمخاطر لاتخاذ القرارات التنفيذية
- الموضوع 3: دمج مخاطر تقنية المعلومات مع إدارة مخاطر المؤسسة ERM
- الموضوع 4: مقاييس المرونة السيبرانية وهياكل إعداد التقارير للمجلس
- الموضوع 5: مواءمة اللوائح والامتثال GDPR, ECC NCA, ISO, NIST
- الموضوع 6: ورشة عمل: بناء لوحة معلومات حوكمة مخاطر الأمن السيبراني
- تأمل ومراجعة: محاكاة تنفيذية وتخطيط مؤشرات الأداء الرئيسية

اليوم الثالث: تخفيف مخاطر الأمن السيبراني، والحوكمة، وأطر التحكم

- الموضوع 1: تصميم بنية دفاع سيبراني على مستوى المؤسسة
- الموضوع 2: حوكمة مراكز العمليات الأمنية SOCs ومعلومات التهديدات
- الموضوع 3: الإشراف على مخاطر الأمن السيبراني للجهات الخارجية وسلسلة التوريد
- الموضوع 4: مواءمة ضوابط المخاطر مع استراتيجية وأهداف الشركة
- الموضوع 5: بروتوكولات تصعيد الأزمات وسلسلة القيادة للمديرين
- الموضوع 6: دراسة حالة: إدارة اختراق سيبراني متعدد القطاعات
- تأمل ومراجعة: تقييم استجابة القيادة

اليوم الرابع: استثمار الأمن السيبراني، والسياسات، والاتصال

- الموضوع 1: ميزانية الأمن السيبراني، وعائد الاستثمار، وتبرير التكلفة والفائدة
- الموضوع 2: قيادة السياسات ومعايير الأمن السيبراني للمؤسسة
- الموضوع 3: المواءمة الاستراتيجية بين تقنية المعلومات، والأعمال، ووحدات المخاطر
- الموضوع 4: إبلاغ مخاطر الأمن السيبراني إلى المجالس والمديرين التنفيذيين غير التقنيين
- الموضوع 5: الاعتبارات القانونية والتنظيمية والأخلاقية لقادة الأمن السيبراني
- الموضوع 6: ورشة عمل: صياغة خطة استثمار في الأمن السيبراني
- تأمل ومراجعة: تقييم الأقران للعروض التقديمية للحوكمة

اليوم الخامس: التقنيات الناشئة وقيادة الأمن السيبراني المستقبلية

- الموضوع 1: تحديات الحوكمة في الحوسبة السحابية والذكاء الاصطناعي والحوسبة الكمومية
- الموضوع 2: إدارة المخاطر الناشئة في إنترنت الأشياء والبنية التحتية الحيوية
- الموضوع 3: تقييم نضج الأمن السيبراني وتحديد المعايير
- الموضوع 4: تطوير خارطة طريق للأمن السيبراني على مستوى المدير
- الموضوع 5: المشروع الختامي: تقديم خطة استراتيجية للأمن السيبراني على مستوى المجلس
- الموضوع 6: حلقة نقاش: الدور المستقبلي لمديري الأمن السيبراني
- تأمل ومراجعة: عروض مشاريع التخرج والملاحظات

الأسئلة الشائعة

ما هي المؤهلات أو المتطلبات المسبقة المحددة المطلوبة للمشاركين قبل التسجيل في الدورة؟

لا توجد متطلبات مسبقة صارمة. ومع ذلك، يجب أن يكون لدى المشاركين خبرة سابقة في أمن المعلومات، أو حوكمة تقنية المعلومات، أو إدارة مخاطر المؤسسة.

كم مدة جلسة كل يوم، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تم تصميم جلسة كل يوم لتستمر حوالي 4-5 ساعات، بما في ذلك فترات الراحة والمناقشات الجماعية ومحاكاة الاستراتيجية. يمتد إجمالي مدة البرنامج على مدار خمسة أيام، بإجمالي حوالي 20-25 ساعة.

كيف تختلف حوكمة مخاطر تقنية المعلومات عن إدارة الأمن السيبراني التشغيلية؟

تركز إدارة الأمن السيبراني التشغيلية على آليات الدفاع التقنية، مثل تقوية الأنظمة، وفحص الثغرات الأمنية، ومراقبة الشبكة. أما حوكمة مخاطر تقنية المعلومات، فهي استراتيجية - تضمن مواءمة أولويات الأمن السيبراني مع أهداف الشركة، ومتطلبات الامتثال، ورغبة المجلس في المخاطرة. تسد هذه الدورة الفجوة بين البعدين، حيث تعلم المديرين كيفية ترجمة المخاطر التقنية المعقدة إلى قرارات تنفيذية تدفع مرونة المؤسسة ومساءلتها.

كيف تختلف هذه الدورة عن دورات قيادة مخاطر تقنية المعلومات والأمن السيبراني الاستراتيجية الأخرى

تتميز دورة "الحوكمة الاستراتيجية لمخاطر تقنية المعلومات وقيادة الأمن السيبراني للمديرين" بتركيزها على المستوى التنفيذي ونهجها الموجه نحو المجلس. على عكس برامج إدارة مخاطر تقنية المعلومات التقليدية التي تركز على الضوابط التشغيلية والعمليات التقنية، تزود هذه الدورة كبار قادة الأمن السيبراني بالقدرة على الحوكمة من الأعلى - دمج أطر مثل CSF NIST وCOBIT 2019 وISO 31000 في نموذج استراتيجي متماسك.

يتعلم المشاركون كيفية تقييم مخاطر الأمن السيبراني كمياً والتواصل بشأنها بلغة الأعمال، وتصميم لوحات معلومات الحوكمة، وتبرير استثمارات الأمن السيبراني باستخدام المقاييس التنفيذية ومؤشرات الأداء الرئيسية. يدمج كل وحدة دراسات حالة من حوادث عالمية كبرى، وسيناريوهات الامتثال التنظيمي، ومحاكاة القيادة لتعزيز اتخاذ القرار تحت الضغط.

يتناول البرنامج أيضاً تحديات الحوكمة الناشئة التي تفرضها الذكاء الاصطناعي، وإنترنت الأشياء، وبرامج الفدية، وتحولات الحوسبة السحابية - مما يعد مديري الأمن السيبراني للقيادة بثقة في العصر الرقمي المتطور. بنهاية الدورة، لن يفهم المشاركون كيفية إدارة مخاطر تقنية المعلومات فحسب، بل سيتعلمون أيضاً كيفية حوكمة الأمن السيبراني كممكن أعمال استراتيجي، ومواءمة الحماية والأداء والنمو التنظيمي.

AGILE LEADERS
Training Center

فئات الدورات التدريبية

- الدورات التدريبية في مجال البيئة والاستدامة
- دورات إدارة الجودة وتطوير العمليات
- دورات إدارة و تحليل البيانات ودورات علم البيانات
- دورات إدارة و تطوير الموارد البشرية
- دورات الأمن السيبراني ودورات تقنية المعلومات
- دورات الاتصال الجماهيري و السياسات والعلاقات العامة
- دورات التدريب القانوني والمشتريات والتعاقدات
- دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
- دورات الحوكمة وإدارة المخاطر والامتثال
- دورات السكرتارية و إدارة المكاتب
- دورات الصحة والسلامة والأمن المهني
- دورات الصيانة ودورات المجالات الهندسية المتنوعة
- دورات المحاسبة و التمويل و دورات الإدارة المالية
- دورات المهارات الشخصية وتطوير الذات
- دورات في مجالات القيادة والإدارة
- دورات معتمدة من قبل هيئات دولية
- دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقة

AGILE LEADERS
Training Center

مدن التدريب

أبوظبي الإمارات العربية المتحدة	أثينا اليونان	أكرا غانا
أمستردام هولندا	اسطنبول تركيا	الجبيل المملكة العربية السعودية
الدار البيضاء المغرب	الدوحة قطر	الرياض المملكة العربية السعودية
القاهرة مصر	الكويت الكويت	المنامة مملكة البحرين
باريس فرنسا	باكو أذربيجان	بالي جمهورية إندونيسيا
بانكوك تايلند	براغ جمهورية التشيك	برشلونة إسبانيا
برلين ألمانيا	بورتو البرتغال	بوكيت تايلاند
تبليسي جورجيا	تورنتو كندا	جاكرتا جمهورية إندونيسيا
جنيف سويسرا	جوهانسبرغ جنوب إفريقيا	دبي الإمارات العربية المتحدة
روما إيطاليا	زنجبار تنزانيا	سان دييغو الولايات المتحدة الأمريكية
سنغافورة سنغافورة	سيول كوريا الجنوبية	شرم الشيخ مصر
شيكاغو الولايات المتحدة الأمريكية	طرابزون تركيا	طشقند أوزبكستان
طوكيو اليابان	عمان المملكة الأردنية الهاشمية	عن بعد منصة زووم

AGILE LEADERS
Training Center

مدن التدريب

فرانكفورت ألمانيا	فيينا النمسا	كوالالمبور ماليزيا
كيب تاون جنوب إفريقيا	لانكاوي ماليزيا	لشبونة البرتغال
لندن المملكة المتحدة	ماربيا اسبانيا	مدريد إسبانيا
مسقط سلطنة عمان	مونترو سويسرا	ميلان إيطاليا
ميونخ ألمانيا	نيروبي كينيا	نيس فرنسا
نيويورك الولايات المتحدة الأمريكية		