CONCEPT

حوكمة تقنية المعلومات والإشراف على مخاطر الأمن السيبراني للأطراف الثالثة وفق COBIT 2019 ISO/IEC 38500g

حوكمة تقنية المعلومات والإشراف على مخاطر الأمن السيبراني للأطراف الثالثة وفق COBIT 2019 وISO/IEC 38500g

العمق التقني: مفاهيمي · **أسلوب التطبيق:** دراسة حالة

مقدمة

تعتمد معظم المؤسسات اليوم على منصات سحابية ومزودي خدمات مدارة وموردي برمجيات في خدمات كانت تشغلها بنفسها، فقد يوقف اختراق مورد واحد أو انقطاع خدمته العمليات في أرجاء المؤسسة. وتبقى مجالس الإدارة والقيادات التنفيذية مسؤولة عن هذا التعرض، في حين تعمل قرارات التقنية وضمان الموردين في مسارات منفصلة بلا رؤية موحدة للمخاطر. تمكن هذه الدورة من كور كونسبت القيادات التنفيذية من توجيه حوكمة تقنية المعلومات والإشراف على المخاطر السيبرانية للأطراف الثالثة باستخدام ISO/IEC 38500 وCOBIT 2019 وNIST CSF 2.0. ويخرج المشاركون بإطار حوكمة المخاطر السيبرانية للأطراف الثالثة لمؤسساتهم.

أهداف الدورة

- تحديد صلاحيات القرار التقني لمجلس الإدارة والقيادات التنفيذية وفق ISO/IEC 38500:2024 وأهداف الحوكمة في COBIT 2019
- وضع مستوى تقبل مخاطر التقنية والأمن السيبراني بما يوجه قرارات الاستثمار والإسناد واختيار الموردين
- الإشراف على تصنيف أهمية الموردين والعناية الواجبة والحماية التعاقدية وفق مخرجات سلاسل الإمداد في NIST CSF 2.0
- مساءلة أدلة الضمان مثل تقارير SOC 2 وشهادات ISO/IEC 27001 واستبيانات الأمن
- تقييم مخاطر التركز والأطراف الرابعة والخروج في الخدمات السحابية والمسندة وتوجيه معالجتها
- إعداد إطار حوكمة المخاطر السيبرانية للأطراف الثالثة بصيغة جاهزة لاعتماد مجلس الإدارة أو اللجنة التنفيذية

الفئة المستهدفة

- القيادات التنفيذية المسؤولة عن استراتيجية التقنية والاستثمار الرقمي وعمليات تقنية المعلومات
- القيادات التنفيذية المشرفة على أمن المعلومات والمخاطر السيبرانية المؤسسية
- رؤساء المشتريات وإدارة الموردين المسؤولون عن موردي التقنية الحرجين
- رؤساء المخاطر والامتثال والمراجعة الداخلية الذين يقدمون الضمان بشأن مخاطر التقنية
- أعضاء مجالس الإدارة واللجان المشرفون على مخاطر التقنية والأمن السيبراني والإسناد الخارجي
- رؤساء وحدات الأعمال التي تعتمد عملياتها على خدمات رقمية مسندة أو سحابية

محاور الدورة

اليوم الأول: بيئة حوكمة تقنية المعلومات والاعتماد الرقمي

- الفرق بين حوكمة تقنية المعلومات وإدارتها وفق ISO/IEC 38500:2024
- مساءلة جهة الحوكمة وفق مبادئ ISO 37000:2021
- خريطة الاعتماد على سلاسل الإمداد الرقمية ومخاطر التركز
- دروس من حوادث سلاسل الإمداد الكبرى: SolarWinds وMOVEitg وانقطاع CrowdStrike عام 2024
- مراجعة الوضع الراهن لحوكمة تقنية المعلومات بمستويات القدرة في COBIT 2019

اليوم الثاني: أطر الحوكمة وأمن الموردين

- نظام الحوكمة وعوامل التصميم ومجالات التركيز في COBIT 2019
- أهداف EDM في COBIT 2019: التقييم والتوجيه والمتابعة
- وظيفة الحوكمة ومخرجات سلاسل الإمداد GV.SC في NIST CSF 2.0
- سلسلة ISO/IEC 27036 لأمن العلاقة مع الموردين
- ضوابط الموردين من 5.19 إلى 5.23 في الملحق A من ISO/IEC 27001:2022

اليوم الثالث: توجيه قرارات التقنية والإشراف على الموردين

- بيان تقبل مخاطر التقنية وحدود التحمل
- سجل الأطراف الثالثة ونموذج تصنيف أهميتها
- مراجعة أدلة الضمان: تقارير SOC 2 Type II وشهادات ISO/IEC 27001 واستبيان SIG
- البنود السيبرانية في العقود: حق التدقيق والإبلاغ عن الاختراقات وشروط الخروج
- الإشراف على محفظة استثمارات تقنية المعلومات باستخدام APO05 في COBIT

اليوم الرابع: المخاطر المتقدمة للأطراف الثالثة والصمود

- رسم خريطة مخاطر الأطراف الرابعة وما بعدها
- المسؤولية المشتركة في الحوسبة السحابية ومصفوفة ضوابط السحابة CCM v4 من CSA
- ضمان سلسلة إمداد البرمجيات بقائمة مكونات البرمجيات SBOM وNIST SP 800-161 الإصدار الأول
- المراقبة المستمرة للموردين بالتصنيفات الأمنية ومؤشرات المخاطر الرئيسية
- التخطيط للخروج من المورد وإمكانية الاستبدال بما يتوافق مع ISO 22301:2019

اليوم الخامس: دراسات الحالة وإطار الحوكمة

- دراسة حالة انقطاع مزود سحابي حرج: فجوات إشراف مجلس الإدارة
- دراسة حالة اختراق مزود خدمات مدارة: إخفاقات العقد والضمان
- تصميم لوحة معلومات مخاطر التقنية والأطراف الثالثة لمجلس الإدارة
- إعداد مسودة إطار حوكمة المخاطر السيبرانية للأطراف الثالثة
- مراجعة اللجنة التنفيذية والدفاع عن الإطار

المهارات المكتسبة

- تصميم صلاحيات القرار التقني
- تحديد تقبل المخاطر السيبرانية
- تقييم أهمية الموردين
- تقييم أدلة الضمان
- الإشراف على مخاطر التركز
- حوكمة عقود التقنية
- إعداد تقارير المخاطر لمجلس الإدارة

لماذا تحضر هذه الدورة

- تعود إلى عملك بإطار حوكمة المخاطر السيبرانية للأطراف الثالثة لمؤسستك، وقد ناقشه تنفيذيون من الزملاء
- تطرح على الموردين والفرق الداخلية الأسئلة التي تكشف هل الضمان حقيقي أم شكلي
- تتعرف على الاعتماد الخطر على مزود سحابي أو خدمي واحد قبل أن يكشفه انقطاع
- تقارن ممارسات الحوكمة بقيادات تنفيذية من قطاعات ودول مختلفة تعتمد على الموردين العالميين أنفسهم

الخاتمة

إسناد خدمة تقنية إلى طرف خارجي لا ينقل المسؤولية عن مخاطرها. تنتقل هذه الدورة من مبادئ حوكمة تقنية المعلومات وحجم الاعتماد الرقمي، مرورا بإطار COBIT 2019 والمواصفة ISO/IEC 38500 وNIST CSF 2.0، وصولا إلى تصنيف الموردين وأدلة الضمان والحماية التعاقدية ومخاطر التركز. ويحول اليوم الأخير هذه المادة إلى إطار حوكمة المخاطر السيبرانية للأطراف الثالثة يعود به المشارك إلى مجلس الإدارة أو اللجنة التنفيذية، فيمتلك أساسا واضحا وقابلا للدفاع عنه للإشراف على الموردين الذين تعتمد عليهم مؤسسته.