



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

26 - 30 Apr 2027

أهستردام - فندق حي النعمال زوداس



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

المرجع: 1264_7637 التاريخ: 26 - 30 Apr 2027 الموقع: أمستردام - فندق حي النعمال زوداس الرسوم: SAR 23500

العوق 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. تهكّن هذه الدورة من كور كونسبث القيادات التنفيذية من توجيه حوكمة تقنية المعلومات والإشراف على المخاطر السيبرانية للأطراف الثالثة باستخدام ISO/IEC 38500 و COBIT 2019 و CSF NIST 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 الاستئثار والإسناد واختيار الموردين
- الإشراف على تصنيف أهمية الموردين والعناية الواجبة والتعاقدية وفق مخرجات سلاسل الإمداد في CSF NIST 2.0
- مساءلة أدلة الضمان مثل تقارير SOC 2 وشهادات ISO/IEC 27001 واستبيانات الأمن
- تقييم مخاطر التركيز والأطراف الرابعة والخروج في الخدمات السحابية والسندقة وتوجيه معالجتها
- إعداد إطار حوكمة المخاطر السيبرانية للأطراف الثالثة بصيغة جاهزة للاعتماد مجلس الإدارة أو اللجنة التنفيذية

الفئة المستهدفة

- القيادات التنفيذية المسؤولة عن استراتيجية التقنية والاستئثار الرقمي وعمليات تقنية المعلومات
- القيادات التنفيذية المشرفة على أمن المعلومات والمخاطر السيبرانية المؤسسية
- رؤساء المشتريات وإدارة الموردين المسؤولين 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 التركيز
- دروس من حوادث سلاسل الإمداد الكبرى: SolarWinds و MOVEit 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 SC.GV في NIST CSF 2.0
- سلسلة IEC/ISO 27036 لأمن العلاقة مع الموردين
- ضوابط الموردين من 5.19 إلى 5.23 في الملحق A من IEC/ISO 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 II Type 2 SOC وشهادات IEC/ISO 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 ووثائق 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 حرجية: 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 التركيز
- حوكمة عقود التقنية
- إعداد تقارير المخاطر لمجلس الإدارة

لهذا تحضر هذه الدورة

- تعود إلى عملك بإطار حوكمة المخاطر السيبرانية للطرف الثالث لمؤسستك، وقد ناقشه تنفيذيون من الزملاء
- تطرح على الموردين والفرق الداخلية الأسئلة التي تكشف هل الضمان حقيقي أم شكلي
- تتعرف على الاعتراف بالخطر 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 الاعتراف الرقمي، مروراً بإطار اليوم ويحول. التركيز ومخاطر التعاقدية والحماية الضمان وأدلة الموردين تصنيف إلى وصولاً NIST CSF 2.0 و ISO/IEC 38500 والمواصفة COBIT 2019 الأخير هذه الهادة إلى إطار حوكمة المخاطر السيبرانية للطرف الثالث يعود به المشاركون إلى مجلس الإدارة أو اللجنة التنفيذية، فيمتلك أساساً واضحاً وقابلًا للدفاع عنه للإشراف على الموردين الذين تعتمد عليهم مؤسستهم.