



تدقيق تقنية المعلومات وتوكيد نظم المعلومات: الضوابط العامة وضوابط التطبيقات وتقارير التدقيق



تدقيق تقنية المعلومات وتوكيد نظم المعلومات: الضوابط العامة وضوابط التطبيقات وتقارير التدقيق

مقدمة:

حين يقتصر تدقيق تقنية المعلومات على مراجعة السياسات والاستبيانات، تبقى صلاحيات المستخدمين الضعيفة والتغيرات غير المختبرة في البرامج وإخفاقات النسخ الاحتياطي مخفية حتى يكشفها توقف نظام أو خطأ في البيانات أو اختراق. وتتلقى لجان المراجعة عندئذ تأكيدات لا يمكن ربطها بأدلة مستخرجة من الأنظمة نفسها. تمكن هذه الدورة من كور كونسبت المدققين من تخطيط أعمال تدقيق تقنية المعلومات وتنفيذها على الضوابط العامة لتقنية المعلومات وضوابط التطبيقات والواجهات، ثم رفع تقارير بالملاحظات المصنفة ومتابعتها. ويغادر المشاركون ببرنامج تدقيق للضوابط العامة لتقنية المعلومات وتقرير ملاحظات مبني على أنظمتهم.

أهداف الدورة:

- تخطيط تدقيق تقنية المعلومات المبني على المخاطر بربط الأنظمة وطبقات البنية التحتية وتدفقات البيانات بمخاطر التقنية وأهداف الرقابة
- استخدام COBIT 2019 وأدلة GTAG الصادرة عن IIA معايير تدقيق لحوكمة تقنية المعلومات والضوابط العامة
- اختبار ضوابط الوصول المنطقي وتغيير البرامج وعمليات التقنية والنسخ الاحتياطي بجولات التتبع وطلبات الأدلة والعينات
- تقييم ضوابط المدخلات والمعالجة والمخرجات في التطبيقات والواجهات وإعدادات قواعد البيانات وأنظمة ERP وتقارير مقدمي الخدمات
- تطبيق تحليل البيانات على المجتمع الكامل لسجلات الوصول والتغيير والمهام لاكتشاف استثناءات الرقابة
- رفع ملاحظات تدقيق تقنية المعلومات مع تصنيف المخاطر وخطط الإدارة المتفق عليها وأدلة المتابعة بصورة جاهزة للجنة المراجعة

الفئة المستهدفة:

- المدققون الداخليون الذين يوسعون مهام التأكد لتشمل ضوابط الأنظمة والتقنية
- مدققو تقنية المعلومات الذين يخططون لاختبار الضوابط العامة وضوابط التطبيقات وينفذونه
- موظفو المخاطر والرقابة الذين يقيمون مخاطر التقنية ويتابعون المعالجة
- مراجعو الامتثال وخط الدفاع الثاني الذين يعتمدون على أدلة ضوابط التقنية في أعمالهم
- أعضاء فرق التدقيق الذين يراجعون تقارير مقدمي الخدمات وتأكيدات التقنية من الأطراف الخارجية

محاور الدورة:

اليوم 1: عملية تدقيق تقنية المعلومات وخريطة مخاطر التقنية

- أنواع تدقيق تقنية المعلومات: مراجعة الضوابط العامة مقابل مراجعة ضوابط التطبيقات
- تصنيف ضوابط التقنية إلى وقائية وكاشفة وتصحيحية
- أهداف السرية والسلامة والإتاحة في تحديد نطاق تدقيق التقنية
- مجال تدقيق تقنية المعلومات من التطبيقات وطبقات البنية التحتية وتدفقات البيانات
- خطة تدقيق تقنية المعلومات المبنية على المخاطر ومذكرة تحديد نطاق المهمة

اليوم 2: أطر حوكمة تقنية المعلومات والرقابة للمدققين

- أهداف الحوكمة والإدارة في COBIT 2019 إطار حوكمة التقنية بوصفها معايير تدقيق
- هيكل ضوابط تقنية المعلومات في دليل 1 GTAG الصادر عن IIA
- منهج دليل 17 GTAG في تدقيق حوكمة تقنية المعلومات
- خريطة مجالات الضوابط العامة: الوصول المنطقي والتغيير والتشغيل والنسخ الاحتياطي والأمن المادي
- نموذج مصفوفة المخاطر والضوابط للأنظمة ضمن النطاق

اليوم 3: اختبار الضوابط العامة لتقنية المعلومات

- اختبار الوصول المنطقي: منح الصلاحيات والموظفون المغادرون والحسابات ذات الامتيازات باستخدام 9 GTAG
- اختبار تغيير البرامج والتحديثات الأمنية ودورة تطوير الأنظمة باستخدام 2 GTAG
- اختبار عمليات التقنية: جدولة المهام وسجلات الحوادث والأمن المادي لمركز البيانات
- اختبار النسخ الاحتياطي والاستعادة: أدلة الاستعادة وفحص مدد الاحتفاظ
- معايير أدلة تدقيق التقنية وعينات الصفات حسب تكرار الضابط

اليوم 4: ضوابط التطبيقات وبيئات ERP والسحابة وتأكيد الأمن السيبراني

- ضوابط المدخلات والمعالجة والمخرجات في التطبيقات واختبار مطابقة الواجهات
- نظرة عامة على مراجعة قواعد البيانات وبيئات ERP: الأدوار والإعدادات ومسارات التدقيق
- نظرة عامة على تأكيد مقدمي الخدمات: تقارير 1 SOC و 2 SOC من النوع الأول والنوع الثاني
- أساسيات تدقيق الأمن السيبراني: فحص الثغرات وسجلات الأمن وحالة التحديثات
- تحليل البيانات في تدقيق التقنية: اختبار المجتمع الكامل لسجلات الوصول والتغيير والمهام

اليوم 5: حالات تدقيق تقنية المعلومات والتقارير والمتابعة

- دراسة حالة عن الوصول والتغيير في نظام ERP: الاستثناءات والضوابط التعويضية
- دراسة حالة عن مقدم خدمات سحابية: استثناءات تقرير SOC 2 من النوع الثاني وضوابط الجهة المستخدمة المكمل
- صياغة تقرير تدقيق التقنية: الملاحظات المصنفة وخطط عمل الإدارة
- سجل متابعة المعالجة ومراجعة أدلة الإغلاق
- عرض برنامج تدقيق الضوابط العامة لتقنية المعلومات وتقرير الملاحظات ومناقشته مع الزملاء

المهارات التي ستكتسبها:

- تخطيط تدقيق تقنية المعلومات
- ربط مخاطر التقنية بالضوابط
- اختبار ضوابط الوصول
- مراجعة إدارة التغيير
- تقييم ضوابط التطبيقات
- مراجعة تقارير مقدمي الخدمات
- تحليل بيانات التدقيق
- إعداد تقارير تدقيق التقنية

لماذا تحضر هذه الدورة:

- العودة ببرنامج تدقيق للضوابط العامة لتقنية المعلومات وتقرير ملاحظات معد لأحد أنظمتك
- طلب أدلة الأنظمة المناسبة من فرق التقنية والحكم على ما إذا كانت تثبت تشغيل الضابط فعلاً
- قراءة تقرير SOC أو قائمة صلاحيات في نظام ERP وتحديد الاستثناءات المؤثرة في رأي التدقيق
- مقارنة ممارسات تدقيق التقنية مع مدققين من قطاعات المصارف والطاقة والخدمات العامة والتصنيع

الخاتمة:

يعتمد التأكيد الموثوق على التقنية على اختبار الضوابط داخل الأنظمة لا على قراءة السياسات المكتوبة عنها فقط. تنتقل الدورة من أنواع تدقيق التقنية وأهداف الرقابة والتخطيط المبني على المخاطر، إلى COBIT 2019 وأدلة GTAG، ثم إلى اختبار ضوابط الوصول والتغيير والتشغيل والنسخ الاحتياطي، ومنها إلى ضوابط التطبيقات وبيئات ERP وقواعد البيانات وتقارير SOC وأساسيات الأمن السيبراني وتحليلات التدقيق. ويطبق اليوم الأخير هذه الأساليب على حالات عملية، وينتج برنامج تدقيق للضوابط العامة لتقنية المعلومات وتقرير ملاحظات جاهزاً للمراجعة.