

دورة شاملة في التدقيق على التقنيات الحديثة

UK Traininig

PARTNER



دورة شاملة في التدقيق على التقنيات الحديثة

مقدمة

مع تسارع التحول الرقمي في مختلف القطاعات، أصبحت المؤسسات تعتمد بشكل متزايد على الحوسبة السحابية، والذكاء الاصطناعي، والأتمتة، والمنصات الرقمية، والتقنيات المترابطة لإدارة عملياتها وتحقيق أهدافها الاستراتيجية. وفي المقابل، ظهرت مخاطر جديدة ومعقدة تتعلق بالأمن السيبراني، وحوكمة البيانات، والامتثال التنظيمي، واستمرارية الأعمال، وإدارة التقنيات الناشئة.

لم يعد دور المدقق التقني مقتصرًا على مراجعة الضوابط والإجراءات التقليدية، بل أصبح شريكًا استراتيجيًا يساهم في تقييم المخاطر الرقمية، وتعزيز الحوكمة، ودعم المرونة المؤسسية، وتقديم الضمانات اللازمة للإدارة العليا وأصحاب المصلحة. ويتطلب ذلك امتلاك فهم متقدم للتقنيات الحديثة وأطر الحوكمة وإدارة المخاطر وأساليب التدقيق المعاصرة.

ضمنت هذه الدورة للمدققين ذوي الخبرة، ومتخصصي المخاطر والامتثال، ومديري التقنية والأمن السيبراني الذين يسعون إلى تطوير قدراتهم في تدقيق البيئات الرقمية الحديثة. ومن خلال التطبيقات العملية، والمحاكاة الواقعية، ودراسات الحالة، سيكتسب المشاركون المعرفة اللازمة لتقييم التقنيات الناشئة، وتحليل المخاطر، وقياس فعالية الضوابط، وتعزيز الثقة في الأنظمة الرقمية المعقدة.

كما تعتمد الدورة على أفضل الممارسات والمعايير العالمية في الحوكمة والأمن السيبراني وإدارة المخاطر، بما يمكن المشاركين من تنفيذ عمليات تدقيق فعالة تدعم أهداف المؤسسة وتحافظ على أمنها واستدامتها الرقمية.

أهداف الدورة

بنهاية هذه الدورة سيكون المشاركون قادرين على:

UK Training

PARTNER



- تنفيذ عمليات تدقيق قائمة على المخاطر في البيئات الرقمية المعقدة.
- تطوير خطط تدقيق استراتيجية للتقنيات الحديثة.
- تقييم فعالية ضوابط الأمن السيرياني والحوكمة التقنية.
- تدقيق أنظمة الذكاء الاصطناعي وتقييم مخاطرها التشغيلية والتنظيمية.
- تقييم البيئات السحابية والبنى التحتية الهجينة.
- مراجعة ضوابط الهوية وإدارة الصلاحيات.
- تقييم برامج التحول الرقمي والأتمتة المؤسسية.
- تحليل المخاطر المرتبطة بالتقنيات الناشئة والأجهزة المترابطة.
- استخدام التحليلات المتقدمة في دعم أعمال التدقيق.
- دمج معلومات التهديدات السيريانية ضمن خطط التدقيق.
- إجراء مراجعات جنائية رقمية وتحليل الحوادث الأمنية.
- تقييم قدرات الاستجابة للحوادث واستمرارية الأعمال.
- تدقيق تقنيات سلاسل الكتل والعقود الذكية.
- تقييم الامتثال للمتطلبات التنظيمية والتشريعية الدولية.
- إعداد تقارير تدقيق احترافية للإدارة العليا واللجان الرقابية.
- تطوير استراتيجيات تدقيق مستقبلية للتقنيات الحديثة.

محاور الدورة

اليوم الأول: التخطيط الاستراتيجي للتدقيق وإدارة المخاطر الرقمية

- تطور التدقيق التقني في عصر التحول الرقمي.
- تحديد نطاق التدقيق في البيئات الرقمية المعقدة.
- منهجيات التدقيق القائمة على المخاطر.
- تقييم المخاطر التقنية والمؤسسية.
- دمج معلومات التهديدات في عمليات التدقيق.
- تدقيق البيئات الرقمية الحديثة.
- موازنة الضوابط مع الأطر العالمية.
- دراسة حالة حول إعداد خطة تدقيق متكاملة.

UK Traininig

PARTNER



اليوم الثاني: حوكمة التقنية وإدارة المخاطر المؤسسية

- أطر حوكمة تقنية المعلومات.
- إدارة المخاطر التقنية على مستوى المؤسسة.
- حوكمة مشاريع التحول الرقمي.
- إدارة مخاطر الأطراف الخارجية والموردين.
- تقييم مقدمي الخدمات التقنية.
- الامتثال التنظيمي للتقنيات الرقمية.
- مراجعة السياسات والإجراءات التقنية.
- ورشة عمل لتقييم نضج الحوكمة الرقمية.

اليوم الثالث: التدقيق المتقدم للأمن السيبراني

- منهجيات تدقيق الأمن السيبراني.
- مراجعة البنية الأمنية للمؤسسات.
- تقييم ضوابط أمن الشبكات.
- تدقيق إدارة الثغرات الأمنية.
- تقييم قدرات المراقبة والكشف المبكر.
- مراجعة مراكز العمليات الأمنية.
- تقييم أنظمة جمع وتحليل الأحداث الأمنية.
- دراسة حالة حول تدقيق الأمن السيبراني.

اليوم الرابع: تدقيق الذكاء الاصطناعي والأتمتة الذكية

- حوكمة الذكاء الاصطناعي وإدارة مخاطره.
- تدقيق نماذج التعلم الآلي.
- تقييم الشفافية وقابلية التفسير.
- مراجعة العدالة وتقليل التحيز في النماذج.
- الاعتبارات الأخلاقية للذكاء الاصطناعي.
- تدقيق الأتمتة الروبوتية للعمليات.
- حوكمة مشاريع الأتمتة الذكية.
- تطبيق عملي لتقييم أنظمة الذكاء الاصطناعي.

UK Traininig

PARTNER



اليوم الخامس: تدقيق الحوسبة السحابية والبنى التحتية الهجينة

- تدقيق البيئات السحابية.
- حوكمة الخدمات السحابية.
- إدارة المخاطر في البيئات متعددة السحب.
- مراجعة ضوابط أمن البيانات السحابية.
- إدارة الهوية والصلاحيات في البيئات السحابية.
- تقييم الامتثال والخصوصية.
- تدقيق الخدمات السحابية المؤسسية.
- دراسة حالة حول تدقيق بيئة سحابية هجينة.

اليوم السادس: تدقيق حوكمة البيانات والخصوصية

- أطر حوكمة البيانات المؤسسية.
- تصنيف البيانات وإدارة دورة حياتها.
- الامتثال لمتطلبات الخصوصية.
- مراجعة ضوابط حماية البيانات.
- تقييم جودة البيانات وسلامتها.
- بناء الثقة الرقمية داخل المؤسسة.
- متطلبات نقل البيانات عبر الحدود.
- ورشة عمل حول تقييم أثر الخصوصية.

اليوم السابع: التدقيق الجنائي الرقمي والاستجابة للحوادث

- مبادئ التدقيق الجنائي الرقمي.
- حوكمة إدارة الحوادث الأمنية.
- منهجيات التحقيق في الاختراقات.
- جمع الأدلة الرقمية وحفظها.
- تقييم إدارة الحوادث الأمنية.
- مراجعة خطط التعافي بعد الحوادث.
- استخلاص الدروس المستفادة.
- محاكاة عملية للتحقيق في حادثة أمنية.

UK Traininig

PARTNER



اليوم الثامن: تدقيق التقنيات الناشئة والأنظمة المترابطة

- تدقيق الأجهزة المتصلة وإنترنت الأشياء.
- تقييم مخاطر الحوسبة الطرفية.
- تدقيق تقنيات سلاسل الكتل.
- مراجعة العقود الذكية.
- حوكمة الأصول الرقمية.
- تدقيق الأنظمة الصناعية والتشغيلية.
- تقييم مخاطر التقنيات الحديثة.
- دراسة حالة حول تدقيق بيانات سلاسل الكتل.

اليوم التاسع: التدقيق المستمر وتحليلات البيانات

- مفهوم التدقيق المستمر.
- مراقبة الضوابط بشكل مستمر.
- استخدام تحليلات البيانات في التدقيق.
- التدقيق المدعوم بالمؤشرات التنبؤية.
- تطوير لوحات المتابعة والتقارير.
- أتمتة إجراءات التدقيق.
- قياس فعالية الضوابط بشكل لحظي.
- ورشة عمل لبناء برنامج تدقيق ذكي.

اليوم العاشر: التقارير التنفيذية ومستقبل التدقيق التقني

- إعداد تقارير تدقيق عالية التأثير.
- عرض النتائج على الإدارة العليا.
- التواصل مع لجان التدقيق والحوكمة.
- ترتيب المخاطر والتوصيات الاستراتيجية.
- الجوانب الأخلاقية لتدقيق التقنيات الحديثة.
- تأثير الحوسبة الكمية على مستقبل التدقيق.
- نماذج الثقة الصفريّة وآليات التدقيق المستقبلية.
- مشروع تطبيقي شامل وعرض النتائج النهائية.

UK Training

PARTNER



لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- تطوير خبرات متقدمة في تدقيق التقنيات الحديثة.
- تعزيز القدرة على تقييم مخاطر الأمن السيبراني.
- اكتساب مهارات تدقيق الذكاء الاصطناعي والأتمتة.
- تحسين القدرة على تدقيق البيئات السحابية.
- تطوير مهارات التحقيق والتدقيق الجنائي الرقمي.
- تعزيز فهم حوكمة البيانات والخصوصية.
- اكتساب خبرة عملية في تدقيق التقنيات الناشئة.
- تحسين جودة التقارير والتوصيات التنفيذية.
- دعم اتخاذ القرارات الاستراتيجية المبنية على المخاطر.
- تعزيز الدور الاستراتيجي لوظيفة التدقيق داخل المؤسسة.

الخاتمة

أصبحت وظيفة التدقيق التقني اليوم عنصراً أساسياً في دعم الحوكمة المؤسسية وإدارة المخاطر وتعزيز الأمن السيبراني وضمان نجاح مبادرات التحول الرقمي. ومع التوسع المستمر في استخدام الذكاء الاصطناعي والحوسبة السحابية والأتمتة والتقنيات الناشئة، باتت الحاجة ملحة إلى مدققين يمتلكون القدرة على تقييم هذه البيئات المعقدة وتقديم ضمانات فعالة للإدارة وأصحاب المصلحة.

توفر هذه الدورة إطاراً متكاملًا لتدقيق التقنيات الحديثة من خلال الجمع بين الحوكمة وإدارة المخاطر والأمن السيبراني والتدقيق الجنائي وتحليلات البيانات والتقنيات الناشئة. كما تمنح المشاركين فرصة لاكتساب خبرات عملية تساعد على التعامل مع التحديات التقنية والتنظيمية المتزايدة بكفاءة واحترافية.

ومن خلال تطبيق أفضل الممارسات العالمية والمنهجيات الحديثة في التدقيق، سيتمكن المشاركون من تطوير قدراتهم المهنية وتعزيز مساهمتهم في حماية مؤسساتهم ودعم استدامة أعمالها وتحقيق أهدافها الاستراتيجية في البيئة الرقمية المتسارعة.

UK Training

PARTNER



الأسئلة الشائعة

ما هي مراجعة تقنية المعلومات ولماذا تعد مهمة؟

تعد مراجعة تقنية المعلومات عملية مستقلة ومنهجية لتقييم ضوابط التقنية، وأمن المعلومات، والحوكمة، وإدارة المخاطر داخل المؤسسات. وللمن يتساءل ما هي مراجعة تقنية المعلومات، فإنها تساعد على التأكد من كفاءة الأنظمة الرقمية، وحماية البيانات، والامتثال للمتطلبات التنظيمية، ودعم استمرارية الأعمال في بيئات العمل الحديثة.

ما هي خطوات عملية مراجعة تقنية المعلومات؟

تعتمد عملية مراجعة تقنية المعلومات على منهجية تبدأ بتحديد نطاق المراجعة، وتقييم المخاطر، ومراجعة الضوابط الأمنية والتشغيلية، واختبار فعالية الأنظمة، ثم إعداد التقارير والتوصيات. وتستند هذه العملية إلى أفضل الممارسات والأدلة المهنية مثل الدليل العالمي لمراجعة التقنية لضمان تقديم نتائج دقيقة وقابلة للتنفيذ.

ما الفرق بين مراجعة تقنية المعلومات ومراجعة أمن المعلومات؟

تركز مراجعة تقنية المعلومات على تقييم البنية التقنية، والحوكمة، والضوابط التشغيلية، وإدارة المخاطر، بينما تهتم مراجعة أمن تقنية المعلومات بتقييم الضوابط الأمنية، وحماية الشبكات، وإدارة الهوية والصلاحيات، والاستجابة للتهديدات السيبرانية. ويؤدي التكامل بين المجالين إلى تعزيز أمن المؤسسة ورفع مستوى الامتثال والجاهزية الرقمية.

من المستفيد من دورة مراجعة تقنية المعلومات؟

تستهدف دورة مراجعة تقنية المعلومات المراجعين الداخليين، ومتخصصي المخاطر والامتثال، وأمن المعلومات، ومديري التقنية، وكل من يرغب في تطوير مهاراته في مراجعة البيانات الرقمية الحديثة. كما تساعد المشاركين على فهم أفضل ممارسات المراجعة، وتقييم المخاطر التقنية، واستخدام أحدث حلول وتقنيات المراجعة في تنفيذ مهام المراجعة بكفاءة.

ما المهارات التي سيكتسبها المشاركون من دورة مراجعة تقنية المعلومات؟

سيكتسب المشاركون مهارات إعداد وتنفيذ خطط مراجعة تقنية المعلومات المبنية على المخاطر، وتقييم ضوابط الأمن السيبراني، ومراجعة الحوسبة السحابية، والذكاء الاصطناعي، وحوكمة البيانات، وتحليل المخاطر التقنية، وإعداد التقارير التنفيذية. كما ستساعدهم الدورة على تطبيق أفضل الأطر والمعايير العالمية لتعزيز الحوكمة، وتحسين الضوابط، ودعم التحول الرقمي بثقة وكفاءة.

UK Training

PARTNER

