المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

IT Governance and Risk Management Training

فكرة الدورة

أصبحت حوكمة تقنية المعلومات عنصرًا محوريًا في قدرة المؤسسات على تحقيق القيمة، وضبط المخاطر، وضمان الامتثال في بيئات رقمية سريعة التغير. ومع تزايد الاعتماد على الأنظمة والمنصات والبيانات، تحتاج الإدارات التقنية إلى إطار واضح يربط القرارات التقنية بالأهداف المؤسسية ومتطلبات الرقابة والمساءلة. لا تقتصر الحوكمة على السياسات، بل تشمل توزيع المسؤوليات، إدارة المخاطر، قياس الأداء، وتحسين الضوابط بصورة مستمرة.

يركز هذا البرنامج التدريبي من AINFCT على بناء قدرات متقدمة في حوكمة تقنية المعلومات وإدارة المخاطر، من خلال تناول مفاهيم القيمة والمواءمة والرقابة والامتثال وفق ممارسات مهنية معروفة مثل COBIT وISO/IEC 38500 وISO 31000. ويمنح البرنامج المشاركين قدرة عملية على تحليل المخاطر التقنية، تصميم نماذج رقابية، تقييم النضج، وتطوير تقارير حوكمة تدعم قرارات الإدارة العليا. يوفر البرنامج قيمة تطبيقية من خلال تحويل أطر الحوكمة إلى ممارسات قابلة للتنفيذ داخل المؤسسات.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- فهم مبادئ حوكمة تقنية المعلومات المتقدمة.
- تحليل مخاطر تقنية المعلومات المؤسسية.
- تطبيق أطر COBIT وISO ذات الصلة.
- تصميم ضوابط رقابية فعالة للخدمات التقنية.
- تقييم نضج الحوكمة والمخاطر التقنية.
- إعداد تقارير حوكمة للإدارة العليا.

منهجية الدورة

- شرح تفاعلي للأطر والمفاهيم المهنية.
- تمارين تطبيقية على تقييم المخاطر والضوابط.
- تحليل حالات مرتبطة بحوكمة تقنية المعلومات.
- نماذج عمل لتقارير الحوكمة والمؤشرات.
- مناقشات جماعية حول تحديات التطبيق المؤسسي.

أثر الدورة على المنظمة

يمكن تعزيز حوكمة تقنية المعلومات المؤسسية من خلال:

- رفع مواءمة التقنية مع أهداف الأعمال.
- تحسين إدارة المخاطر التقنية الحرجة.
- تعزيز الامتثال والرقابة على الخدمات.
- دعم قرارات الاستثمار التقني بثقة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- تقييم ممارسات الحوكمة التقنية بفعالية.
- تحليل المخاطر التقنية بمنهجية واضحة.
- تصميم ضوابط رقابية قابلة للتطبيق.
- عرض نتائج الحوكمة للإدارة العليا.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المهنيين المشاركين في حوكمة وإدارة ومراجعة تقنية المعلومات. كما يفيد القيادات التقنية التي تتعامل مع المخاطر والامتثال وقرارات الاستثمار التقني.

- مدراء تقنية المعلومات والتحول الرقمي.
- مسؤولو حوكمة ومخاطر تقنية المعلومات.
- مدراء أمن المعلومات والامتثال التقني.
- مراجعو نظم المعلومات والرقابة الداخلية.
- قادة الخدمات والمشاريع التقنية.

موضوعات الدورة

اليوم الأول: مدخل متقدم إلى حوكمة تقنية المعلومات

- مفهوم حوكمة تقنية المعلومات ودورها المؤسسي.
- الفرق بين الإدارة التقنية والحوكمة التقنية.
- مبادئ القيمة والمساءلة والرقابة.
- العلاقة بين الحوكمة والاستراتيجية الرقمية.
- تحديات الحوكمة في البيئات التقنية الحديثة.

اليوم الثاني: مواءمة تقنية المعلومات مع أهداف الأعمال

- تحليل العلاقة بين التقنية والأهداف المؤسسية.
- تحديد أصحاب المصلحة في الحوكمة التقنية.
- ترجمة المتطلبات المؤسسية إلى أولويات تقنية.
- إدارة التوقعات بين التقنية والأعمال.
- قياس قيمة الخدمات والاستثمارات التقنية.

اليوم الثالث: أطر الحوكمة التقنية COBIT وISO/IEC 38500

- مبادئ COBIT في حوكمة وإدارة التقنية.
- مجالات ISO/IEC 38500 للحوكمة المؤسسية.
- مقارنة استخدامات الأطر حسب السياق.
- ربط الأهداف التقنية بممارسات الحوكمة.
- اختيار الإطار المناسب للاحتياج المؤسسي.

اليوم الرابع: نموذج التشغيل والمسؤوليات التقنية

- تصميم أدوار الحوكمة داخل المؤسسة.
- تحديد صلاحيات القرار التقني.
- بناء لجان ومجالس حوكمة تقنية المعلومات.

- توزيع المسؤوليات باستخدام RACI.
- ضبط التصعيد والمساءلة في القرارات التقنية.

اليوم الخامس: إدارة مخاطر تقنية المعلومات

- مفهوم مخاطر تقنية المعلومات ومصادرها.
- تصنيف المخاطر التشغيلية والأمنية والاستراتيجية.
- تحليل احتمالية المخاطر وأثرها.
- بناء سجل مخاطر تقنية المعلومات.
- تحديد شهية المخاطر وحدود القبول.

اليوم السادس: تقييم المخاطر والضوابط التقنية

- منهجيات تقييم المخاطر التقنية.
- ربط المخاطر بالضوابط الوقائية والكشفية.
- تحليل فجوات الضوابط الحالية.
- تقدير المخاطر المتبقية بعد المعالجة.
- توثيق نتائج التقييم بصورة مهنية.

اليوم السابع: الامتثال والرقابة الداخلية التقنية

- متطلبات الامتثال في بيئات تقنية المعلومات.
- عناصر الرقابة الداخلية على الخدمات التقنية.
- إدارة السياسات والإجراءات التقنية.
- تتبع الالتزام بالضوابط المعتمدة.
- التعامل مع نتائج التدقيق والمراجعة.

اليوم الثامن: أمن المعلومات ضمن الحوكمة والمخاطر

- العلاقة بين الحوكمة وأمن المعلومات.
- دور ISO/IEC 27001 في الضوابط الأمنية.
- إدارة مخاطر السرية والسلامة والتوافر.

- دمج الأمن في قرارات التقنية.
- تقييم نضج الضوابط الأمنية المؤسسية.

اليوم التاسع: استمرارية الأعمال والمرونة التقنية

- مفهوم المرونة التقنية واستمرارية الخدمات.
- تحليل أثر الأعطال على الأعمال.
- تحديد الخدمات والأنظمة الحرجة.
- حوكمة خطط التعافي من الكوارث.
- متابعة اختبارات الاستمرارية والتعافي.

اليوم العاشر: قياس أداء حوكمة تقنية المعلومات

- تحديد مؤشرات أداء الحوكمة التقنية.
- قياس جودة الخدمات التقنية والمخاطر.
- ربط المؤشرات بالأهداف والضوابط.
- استخدام Dashboards للمتابعة التنفيذية.
- تحليل اتجاهات الأداء والتحسين.

اليوم الحادي عشر: إدارة الموردين والمخاطر الخارجية

- حوكمة العلاقات مع موردي التقنية.
- تقييم مخاطر الطرف الثالث التقنية.
- متابعة مستويات الخدمة والالتزام التعاقدي.
- ضبط الوصول والبيانات لدى الموردين.
- إدارة المخاطر المرتبطة بالخدمات السحابية.

اليوم الثاني عشر: تقييم النضج والتحسين المستمر

- مفهوم النضج في حوكمة تقنية المعلومات.
- استخدام نماذج تقييم القدرات التقنية.
- تحديد فجوات الممارسات والضوابط.

- ترتيب أولويات التحسين وفق المخاطر.
- بناء خارطة طريق لتحسين الحوكمة.

اليوم الثالث عشر: تقارير الحوكمة والمخاطر للإدارة العليا

- تصميم تقارير تنفيذية للمخاطر التقنية.
- عرض مؤشرات الحوكمة بلغة إدارية.
- صياغة رسائل واضحة لأصحاب القرار.
- تصعيد المخاطر الحرجة بفعالية.
- ربط التقارير بخطط المعالجة والمتابعة.

اليوم الرابع عشر: تكامل الحوكمة مع التحول الرقمي

- حوكمة المبادرات والمشاريع الرقمية.
- إدارة مخاطر الابتكار والتحول التقني.
- ضبط قرارات الاستثمار في الحلول الرقمية.
- حوكمة البيانات والمنصات والتكاملات.
- دعم الاستدامة في التحول الرقمي.

اليوم الخامس عشر: تطبيق عملي متكامل

- تحليل حالة حوكمة تقنية معلومات.
- بناء سجل مخاطر وضوابط مختصر.
- تقييم فجوات الحوكمة والمخاطر.
- إعداد لوحة مؤشرات تنفيذية.
- عرض خطة تحسين قابلة للتطبيق.

course_daily_schedule

يمتد البرنامج لمدة 15 يومًا تدريبيًا، بواقع 4 ساعات يوميًا. يجمع كل يوم بين الشرح المفاهيمي، التحليل التطبيقي، التمارين العملية، ودراسة الحالات. يتم تخصيص الأيام الأخيرة لتطبيق متكامل يشمل تقييم الحوكمة، تحليل المخاطر، تصميم الضوابط، وإعداد عرض تنفيذي قابل للاستخدام في بيئة العمل.

course_assessment

يتم تقييم المشاركين من خلال التفاعل أثناء الجلسات، التمارين التطبيقية، تحليل الحالات، ومخرجات التطبيق العملي النهائي. وفي نهاية البرنامج، يحصل المشاركون على شهادة حضور أو إتمام صادرة عن AINFCT وفق متطلبات المشاركة المعتمدة.

course_key_competencies

- حوكمة تقنية المعلومات.
- إدارة المخاطر التقنية.
- الرقابة والامتثال التقني.
- تقييم نضج الحوكمة.
- تقارير المخاطر التنفيذية.
- مواءمة التقنية والأعمال.

مكتب القاهرة الرئيسي

القاهرة، جمهورية مصر العربية

7 شارع وهران، الطيران، مدينة نصر

+201152466358

info@ainfct.com

ainfct.com

رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي

مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد

training@ainfct.com
ainfct.com