Global Horizon
TRAINING CENTER

دورة:

استراتيجيات التحول الرقمي وأمن المعلومات للمدراء التنفيذيين

19 أكتوبر - 6 نوفمبر 2025

القاهرة (مصر)

Holiday Inn & Suites Cairo Maa

استراتيجيات التحول الرقمي وأمن المعلومات للمدراء التنفيذيين

رمز الدورة: IT13036 تاريخ الإنعقاد: 19 أكتوبر - 6 نوفمبر 2025 دولة الإنعقاد: القاهرة (مصر) - Maa Cairo Suites & Inn Holiday رسوم الإشتراك: 9700 Euro

المقدمة

يعد**التحول الرقمي** عاملاً أساسيًا في تحقيق التميز التنافسي وتعزيز الكفاءة التشغيلية في المؤسسات الحديثة. ومع زيادة اعتماد الشركات على الحلول الرقمية، أصبح**أمن المعلومات**عنصرًا استراتيجيًا لحماية الأصول الرقمية وضمان استمرارية الأعمال.
يهدف هذا البرنامج التدريبي إلى تمكين**المدراء التنفيذيين** من **تطوير وتنفيذ استراتيجيات التحول الرقمي** مع التركيز على**إدارة المخاطر السيبرانية وحماية البيانات**، مما يضمن تحوّلا رقميًا آمنًا ومستدامًا للمؤسسات.
يقدم البرنامج**على مدار 15 يومًا** محتوى مكثفًا يغطي أحدث الاتجاهات والتحديات في التحول الرقمي وأمن المعلومات، مع التركيز على**التطبيقات العملية، الحوكمة الرقمية، إدارة البيانات، وحماية الأنظمة من التهديدات السيبرانية**.

أهداف البرنامج

- **فهم دور التحول الرقمي في تعزيز القدرة التنافسية للمؤسسات**.
- **تصميم وتنفيذ استراتيجيات رقمية فعالة**لتعزيز العمليات المؤسسية.
- **تعزيز وعي المدراء التنفيذيين بمخاطر الأمن السيبراني**وكيفية الحد منها.
- **تحليل البيانات الضخمة واتخاذ قرارات استراتيجية قائمة على البيانات**.
- **التعرف على أحدث التقنيات الرقمية**مثل الذكاء الاصطناعي والحوسبة السحابية والبلوك تشين.
- **تطوير استراتيجيات الحوكمة الرقمية**وإدارة الامتثال الأمني.
- **استخدام أفضل الممارسات لحماية البيانات والخصوصية** وفقًا للمعايير الدولية مثل **ISO 27001 و GDPR** .

الفئات المستهدفة

- **المدراء التنفيذيون Level-C** مثل **الرؤساء التنفيذيين CEO، مدراء التكنولوجيا CTO، مدراء العمليات CIO المعلومات ومدراء ،COO**.
- **مدراء التحول الرقمي وأمن المعلومات**في المؤسسات الكبرى.
- **صناع القرار وأصحاب الرؤية الاستراتيجية**في الشركات والمنظمات الحكومية.
- **مديرو تقنية المعلومات Directors IT**المسؤولون عن تطوير استراتيجيات الأمن الرقمي.
- **الاستشاريون والخبراء في التحول الرقمي والأمن السيبراني**.

المحاور

الأسبوع الأول:

التحول الرقمي - المفاهيم والاستراتيجيات التنفيذية

اليوم 1: مقدمة إلى التحول الرقمي للمدراء التنفيذيين

- مفهوم التحول الرقمي وأهميته في بيئة الأعمال الحديثة.
- الفرق بين الرقمنة والتحول الرقمي.
- كيف يؤثر التحول الرقمي على نموذج العمل التقليدي؟

اليوم 2: بناء استراتيجية التحول الرقمي

- تصميم خارطة طريق للتحول الرقمي وفقًا لأهداف المؤسسة.
- التحديات والفرص في تطبيق التحول الرقمي.
- مؤشرات النجاح الرئيسية للتحول الرقمي KPIs.

اليوم 3: التقنيات الداعمة للتحول الرقمي

- الذكاء الاصطناعي AI والتعلم الآلي في دعم القرارات الاستراتيجية.
- تحليل البيانات الضخمة **Big Data Analytics** ودورها في اتخاذ القرار.
- استخدام الحوسبة السحابية **Cloud Computing** لتسهيل التحول الرقمي.

اليوم 4: الحوكمة الرقمية والإدارة الاستراتيجية للتحول الرقمي

- مبادئ الحوكمة الرقمية وتأثيرها على استدامة التحول الرقمي.
- إدارة المخاطر في مشاريع التحول الرقمي.
- كيفية تحقيق التكامل بين التحول الرقمي واستراتيجية المؤسسة.

اليوم 5: إدارة التغيير وقيادة فرق العمل الرقمية

- كيفية تمكين فرق العمل للتكيف مع التحول الرقمي.
- استراتيجيات إدارة التغيير لتجنب مقاومة الموظفين.
- دور القيادة في تعزيز الثقافة الرقمية داخل المؤسسة.

الأسبوع الثاني:

أمن المعلومات وحماية الأصول الرقمية

اليوم 6: مقدمة في الأمن السيبراني وإدارة مخاطر البيانات

- أهمية الأمن السيبراني في عصر التحول الرقمي.

- تحليل المخاطر السيبرانية وتأثيرها على المؤسسات.
- استراتيجيات التعامل مع التهديدات الرقمية.

اليوم 7:حماية البيانات والخصوصية في المؤسسات الرقمية

- مبادئ حماية البيانات وفقًا لمعايير**GDPR, ISO 27001**.
- إدارة الامتثال الرقمي وتطبيق سياسات الأمن والخصوصية.
- استراتيجيات تقليل المخاطر المرتبطة بسرقة البيانات واختراق الأنظمة.

اليوم 8:تأمين البنية التحتية الرقمية

- طرق تأمين الشبكات والبنية التحتية السحابية.
- استراتيجيات الحماية من هجمات الاختراق والفيروسات.
- دور الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية ومنعها.

اليوم 9:تطوير سياسات الأمن السيبراني وإدارة الامتثال

- كيفية إعداد سياسات الأمن السيبراني وفقًا للمعايير الدولية.
- إدارة الامتثال القانوني والمتطلبات التنظيمية.
- حماية المعلومات الحساسة والتعامل مع البيانات المشفرة.

اليوم 10:الاستجابة للطوارئ والتعافي من الكوارث الرقمية

- كيفية تطوير خطط الطوارئ السيبرانية.
- استراتيجيات استعادة البيانات بعد الهجمات الإلكترونية.
- إدارة الأزمات الرقمية وتعزيز استمرارية الأعمال.

الأسبوع الثالث:

الابتكار الرقمي والاستعداد للمستقبل

اليوم 11:الذكاء الاصطناعي والتحليلات المتقدمة في أمن المعلومات

- كيف يساعد الذكاء الاصطناعي في حماية البيانات؟
- تطبيقات التحليل التنبئي في كشف التهديدات الأمنية.
- مستقبل الذكاء الاصطناعي في الأمن السيبراني.

اليوم 12: دور تقنية البلوك تشين في تعزيز أمن المعلومات

- كيف تعمل **Blockchain** على تعزيز أمن البيانات؟
- تطبيقات البلوك تشين في حماية العمليات المالية والشفافية الرقمية.
- تحديات استخدام البلوك تشين في المؤسسات.

اليوم 13: الأمن السيبراني في قطاع الحوسبة السحابية وإنترنت الأشياء

- المخاطر الأمنية المتعلقة بالخدمات السحابية **Cloud Security**.
- تأمين أجهزة إنترنت الأشياء **IoT Security** ضد الهجمات الإلكترونية.
- استراتيجيات الحفاظ على بيئة رقمية آمنة في المؤسسات.

اليوم 14: بناء ثقافة الأمن السيبراني داخل المؤسسة

- دور القادة التنفيذيين في تعزيز الوعي الأمني.
- استراتيجيات التدريب والتثقيف الأمني لموظفي المؤسسات.
- كيفية تطوير سياسات تحكم الوصول والمصادقة الأمنية.

اليوم 15: ورشة عمل تطبيقية: إعداد استراتيجية التحول الرقمي الآمن للمؤسسة

- تحليل نقاط القوة والضعف في البنية الرقمية الحالية.
- تطوير خارطة طريق متكاملة للتحول الرقمي الآمن.
- تنفيذ محاكاة لهجوم سيبراني وإعداد استجابة فورية.