BOOST
THE LEADING TRAINING PROVIDER

التحول الرقمي

برامج تدريبية فى الحوكمة

# استراتيجيات حوكمة أمن المعلومات

## Course Introduction

يهدف هذا البرنامج التدريبي إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتطوير وتنفيذ سياسات حوكمة أمن المعلومات التي تتماشى مع أفضل الممارسات الدولية وتساعد على تحقيق استدامة الأمان المعلوماتي داخل المؤسسات.

## Target Audience

- مدراء أمن المعلومات
- مختصو تكنولوجيا المعلومات
- مدراء المخاطر
- مختصو الأمن السيبراني
- مهندسو الشبكات

## Learning Objectives

- التعرف على مفهوم الحوكمة في مجال أمن المعلومات.
- فهم العلاقة بين الحوكمة وأمن المعلومات في ضمان حماية البيانات.
- التعرف على الأطر التنظيمية والمعايير الدولية مثل ISO 27001 وNIST.
- وضع السياسات والإجراءات الخاصة بحوكمة أمن المعلومات.
- تعلم كيفية تحليل وتقييم مخاطر أمن المعلومات.
- تطوير استراتيجيات لمواجهة التهديدات الأمنية.
- التعمق في قوانين حماية البيانات مثل GDPR.
- تطبيق الممارسات القانونية المطلوبة في حماية المعلومات.
- تقييم فعالية تدابير أمن المعلومات داخل المؤسسة.

# Course Outline

- **Day 01**

**مقدمة في حوكمة أمن المعلومات**

- تعريف حوكمة أمن المعلومات وأهميتها.
- العلاقة بين حوكمة أمن المعلومات وحوكمة تكنولوجيا المعلومات.
- مبادئ الحوكمة في مجال أمن المعلومات.
- مقدمة للأطر والمعايير الدولية لحوكمة أمن المعلومات مثل ISO 27001وCOBIT.

**الأطر والمعايير الدولية في حوكمة أمن المعلومات**

- التعرف على المعايير الدولية لحوكمة أمن المعلومات (ISO 27001، NIST، COBIT).
- المبادئ الرئيسية التي تستند إليها المعايير الدولية.
- كيفية تطبيق هذه المعايير في المؤسسات الخاصة والعامة.
- التحديات المرتبطة بتنفيذ هذه الأطر والمعايير.
- دراسة حالات.
- تطبيق عملي.

- **Day 02**

**تحليل وتقييم مخاطر أمن المعلومات:**

- فهم طبيعة التهديدات والمخاطر الأمنية في مجال المعلومات.
- كيفية إجراء تحليل للمخاطر الأمنية (Risk Assessment).
- تصنيف المخاطر وتحديد أولويات التعامل معها.
- استراتيجيات التعامل مع التهديدات مثل الهجمات الإلكترونية والبرمجيات الخبيثة.
- تطبيق عملي.

**تطوير السياسات والإجراءات الخاصة بحوكمة أمن المعلومات**

- كيفية تطوير سياسات أمن المعلومات التي تتماشى مع الأطر العالمية.
- تصميم السياسات التي تتضمن الحماية من الهجمات الأمنية، الوصول إلى المعلومات، وحمايتها.

- كيفية تحديد الإجراءات المتبعة عند وقوع خرق أمني.
- استخدام أداة إدارة المخاطر لإنشاء السياسات.
- تطبيق عملي: تطوير سياسة أمن معلومات لمؤسسة مع تحديد الإجراءات الواجب اتباعها.

• **Day 03**

**الاستجابة للحوادث والتعامل مع الاختراقات الأمنية:**

- كيفية وضع خطة استجابة للحوادث الأمنية.
- استراتيجيات التعامل مع الهجمات السيبرانية والاختراقات.
- خطوات التحقيق والتعافي بعد الحادث.
- أهمية التنسيق مع الوكالات الحكومية أو الأطراف الخارجية في حالة الحوادث الأمنية الكبرى.
- تطبيق عملي.

**إدارة الامتثال للقوانين واللوائح في مجال أمن المعلومات**

- قوانين حماية البيانات العالمية.
- تأثير الامتثال على الأعمال التجارية.
- كيفية تطبيق الامتثال لهذه القوانين في حوكمة أمن المعلومات.
- مسؤوليات الموظفين والمديرين في ضمان الامتثال.
- دراسة حالات.

• **Day 04**

**تحقيق التوازن بين أمان المعلومات ومتطلبات الأعمال**

- كيفية تحقيق التوازن بين حماية المعلومات واحتياجات المؤسسة لتحقيق أهدافها.
- إدارة الوصول إلى البيانات وحمايتها مع ضمان الإنتاجية.
- استخدام تقنيات التشفير وإدارة الحقوق الرقمية للحفاظ على أمان البيانات.
- تطوير ثقافة مؤسسية فعالة للحفاظ على أمن المعلومات.
- أهمية الوعي الثقافي في تطبيق الحوكمة للأمن المعلوماتي.
- استراتيجيات تدريب الموظفين على أمن المعلومات.
- تطبيق عملي.

• **Day 05**

**تقييم الأداء في حوكمة أمن المعلومات**

- كيفية تقييم فعالية السياسات الأمنية والممارسات في المؤسسة.

- لقياس نجاح حوكمة أمن المعلومات استخدام مؤشرات الأداء الرئيسية (KPIs).
- أدوات المراجعة والتدقيق لضمان الامتثال لسياسات أمن المعلومات.
- تطوير خطة لتقييم أداء أمن المعلومات داخل مؤسسة معينة.
- تطبيق عملي.

## Confirmed Sessions

| FROM | TO | DURATION | FEES | LOCATION |
|---|---|---|---|---|
| June 29, 2025 | July 3, 2025 | 5 days | 4250.00 $ | KSA - Riyadh |
| Aug. 18, 2025 | Aug. 22, 2025 | 5 days | 4250.00 $ | UAE - Dubai |
| Dec. 29, 2025 | Jan. 2, 2026 | 5 days | 5950.00 $ | USA - Los Angeles |