# دورة NIST لإتقان إدارة المخاطر والضوابط الأمنية

12 – 16 يوليو 2027

أديس أبابا

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# دورة NIST لإتقان إدارة المخاطر والضوابط الأمنية

**المرجع:** 225136_103600310 **التاريخ:** 12 – 16 يوليو 2027 **المكان:** أديس أبابا **الرسوم:** Euro 6000

## نظرة عامة على الدورة

صُممت دورة NIST لإتقان إدارة المخاطر والضوابط الأمنية لتزويد المهنيين بالمعرفة والمهارات اللازمة لتطبيق وإدارة الضوابط الأمنية بناءً على معايير NIST. تقدم هذه الدورة منهجًا منظمًا لإدارة مخاطر الأمن السيبراني، وتوفر تدريبًا عمليًا على أطر الأمن السيبراني وإرشادات الامتثال وأفضل الممارسات.

سيكتسب المشاركون خبرة في التدريب على أطر NIST للأمن السيبراني، وشهادات الأمن السيبراني، والتدريب على امتثال أمن تكنولوجيا المعلومات. سيتعلمون كيفية تطبيق تقنيات اختيار الضوابط الأمنية من NIST، وتنفيذ متطلبات شهادة SP 800-171 NIST، وتطوير استراتيجيات إدارة المخاطر بما يتماشى مع أفضل الممارسات الفيدرالية للأمن السيبراني.

تغطي الدورة مجالات رئيسية مثل تقييم مخاطر الأمن السيبراني، والاستجابة للحوادث باستخدام إرشادات NIST، وتطوير برنامج للأمن السيبراني يتماشى مع تطبيق ضوابط NIST الأمنية.

## الجمهور المستهدف

- محترفو الأمن السيبراني وأخصائيو أمن تكنولوجيا المعلومات
- مديرو المخاطر ومسؤولو الامتثال
- مديرو النظم ومهندسو الشبكات
- المتعاقدون الحكوميون الذين يتعاملون مع المعلومات الحساسة
- المديرون التنفيذيون وصناع القرار المسؤولون عن برامج الأمن السيبراني
- مستشارو ومدققو الأمن السيبراني

## الأقسام التنظيمية المستهدفة

- فرق أمن تكنولوجيا المعلومات والبنية التحتية
- أقسام الامتثال وإدارة المخاطر
- الوكالات الحكومية والفيدرالية التي تتعامل مع لوائح الأمن السيبراني
- شركات استشارات الأمن السيبراني
- وحدات الأدلة الجنائية الرقمية والتحقيق في الجرائم السيبرانية

AGILE LEADERS
Training Center

## القطاعات المستهدفة

- الوكالات الحكومية والمنظمات الفيدرالية
- المؤسسات المالية والقطاعات المصرفية
- مؤسسات الرعاية الصحية التي تتعامل مع البيانات الحساسة
- صناعات الدفاع والفضاء
- شركات التكنولوجيا والبرمجيات
- قطاعات سلسلة التوريد والبنية التحتية الحيوية

## مخرجات الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق امتثال الأمن السيبراني مع NIST عبر مختلف القطاعات
- تقييم وتخفيف التهديدات السيبرانية باستخدام تطبيق ضوابط NIST الأمنية
- تطوير برامج للأمن السيبراني تتماشى مع أطر NIST الأمنية
- إجراء تقييمات لمخاطر الأمن السيبراني وتطبيق تقنيات المراقبة
- تطبيق تطوير سياسات الأمن السيبراني وفقًا لإرشادات NIST

## منهجية التدريب

تستخدم هذه الدورة نهج التعلم المدمج، الذي يجمع بين التعليم النظري والتطبيقات العملية. وتساعد الجلسات التفاعلية ودراسات الحالة الواقعية والأنشطة المشاركين على فهم تهديدات الأمن السيبراني واستراتيجيات تخفيف المخاطر. كما تسمح سيناريوهات لعب الأدوار ومحاكاة الاستجابة للحوادث للمتعلمين بممارسة تقنيات مراقبة مخاطر الأمن السيبراني.

من خلال التدريب على الأمن السيبراني المخصص للوكالات الفيدرالية والمتعاقدين الحكوميين، سيشارك المتدربون في تمارين عملية تركز على أهداف دورة استشارات الامتثال لـ NIST. وسيتلقون أيضًا توجيهًا منظمًا حول كيفية استخدام NIST لتقييم مخاطر الأمن السيبراني واختيار الضوابط الأمنية في مؤسساتهم.

## أدوات الدورة

- كتيبات عمل رقمية تتضمن إرشادات امتثال الأمن السيبراني
- قوائم تحقق ونماذج للتدريب على امتثال أمن تكنولوجيا المعلومات
- دراسات حالة حول استراتيجيات إدارة مخاطر الأمن السيبراني

AGILE LEADERS
Training Center

# جدول أعمال الدورة

## اليوم الأول: مقدمة في الأمن السيبراني والحوكمة حسب NIST

- **الموضوع 1:** نظرة عامة على NIST ودوره في الأمن السيبراني
- **الموضوع 2:** فهم إطار NIST للأمن السيبراني وأهميته
- **الموضوع 3:** منشورات NIST الرئيسية: NIST SP 800-171، NIST SP 800-53، NIST SP 800-12
- **الموضوع 4:** تطوير سياسات الأمن السيبراني ونماذج الحوكمة
- **الموضوع 5:** الأدوار والمسؤوليات في برنامج الأمن السيبراني
- **الموضوع 6:** السياق التنظيمي واعتبارات مخاطر الأمن السيبراني
- **تأمل ومراجعة:** النقاط الرئيسية حول مبادئ الأمن السيبراني والحوكمة حسب NIST

## اليوم الثاني: إدارة المخاطر واختيار الضوابط الأمنية

- **الموضوع 1:** مقدمة في إطار إدارة المخاطر من NIST NIST RMF
- **الموضوع 2:** تحديد وتقييم مخاطر الأمن السيبراني في المؤسسة
- **الموضوع 3:** اختيار وتطبيق الضوابط الأمنية من NIST
- **الموضوع 4:** إدارة مخاطر سلسلة التوريد ومخاطر الأمن السيبراني لدى الأطراف الثالثة
- **الموضوع 5:** إدارة الأصول والتحسين الأمني المستمر
- **الموضوع 6:** أفضل الممارسات الفيدرالية للأمن السيبراني من أجل الامتثال
- **تأمل ومراجعة:** تقييم فعالية إدارة المخاطر باستخدام أطر NIST

AGILE LEADERS
Training Center

## اليوم الثالث: التوعية بالأمن السيبراني والتدريب والمراقبة المستمرة

- **الموضوع 1:** برامج التوعية والتدريب الأمني بناءً على إرشادات NIST
- **الموضوع 2:** تطبيق التدابير الأمنية لحماية نظم المعلومات
- **الموضوع 3:** المراقبة الأمنية المستمرة وتكامل استخبارات التهديدات
- **الموضوع 4:** امتثال الأمن السيبراني للوائح ومعايير NIST
- **الموضوع 5:** قياس أداء ومقاييس الأمن السيبراني ورفع التقارير بشأنها
- **الموضوع 6:** استمرارية الأعمال والجاهزية للأمن السيبراني
- **تأمل ومراجعة:** مراجعة أفضل الممارسات للتوعية والمراقبة الأمنية

## اليوم الرابع: إدارة حوادث الأمن السيبراني واستراتيجيات الاستجابة

- **الموضوع 1:** إطار الاستجابة لحوادث الأمن السيبراني بناءً على إرشادات NIST
- **الموضوع 2:** جاهزية تكنولوجيا المعلومات والاتصالات وإجراءات التعامل مع الحوادث
- **الموضوع 3:** اختبار مرونة الأمن السيبراني واستراتيجيات تخفيف التهديدات
- **الموضوع 4:** تطوير خطة فعالة للاستجابة لحوادث الأمن السيبراني
- **الموضوع 5:** أفضل ممارسات التحقيق في الحوادث والأدلة الجنائية الرقمية
- **الموضوع 6:** التحسين المستمر في إدارة حوادث الأمن السيبراني
- **تأمل ومراجعة:** الدروس المستفادة من دراسات حالة الاستجابة للحوادث

AGILE LEADERS
Training Center

### اليوم الخامس: استراتيجيات الأمن السيبراني المتقدمة والتحضير لشهادة الاعتماد

- **الموضوع 1:** مفاهيم وتطبيقات متقدمة لشهادة الأمن السيبراني من NIST
- **الموضوع 2:** استراتيجيات تطوير وتنفيذ برامج الأمن السيبراني
- **الموضوع 3:** مواءمة أطر الأمن السيبراني مع أهداف العمل والامتثال
- **الموضوع 4:** التحضير لامتحان شهادة الأمن السيبراني من NIST
- **الموضوع 5:** دراسة حالة عملية حول إدارة مخاطر الأمن السيبراني والضوابط
- **الموضوع 6:** جلسة أسئلة وأجوبة نهائية ومناقشة حول التقدم الوظيفي في مجال الأمن السيبراني
- **تأمل ومراجعة:** مراجعة شاملة ورؤى رئيسية من الدورة بأكملها

## الأسئلة الشائعة

### ما هي المؤهلات أو المتطلبات المسبقة المحددة اللازمة للمشاركين قبل التسجيل في الدورة؟

هذه الدورة متاحة لمحترفي الأمن السيبراني وأخصائيي تكنولوجيا المعلومات ومسؤولي الامتثال الذين لديهم معرفة أساسية بمبادئ الأمن السيبراني. لا يُشترط الحصول على شهادة NIST مسبقة، ولكن يوصى بالإلمام بمفاهيم إدارة المخاطر.

### كم تبلغ مدة الجلسة اليومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تستمر كل جلسة يومية حوالي 4-5 ساعات، بما في ذلك فترات الراحة والأنشطة التفاعلية. وتمتد الدورة الكاملة على مدى أسبوع، وتغطي 20-25 ساعة من التدريب المتعمق في مجال الأمن السيبراني.

### ما الذي يجعل إطار NIST للأمن السيبراني ضروريًا لإدارة المخاطر؟

يوفر إطار NIST للأمن السيبراني نهجًا منظمًا لإدارة المخاطر الأمنية عبر مختلف القطاعات. ويساعد المؤسسات على تطوير برامج الأمن السيبراني، وتطبيق أفضل الممارسات، والامتثال للوائح الحكومية.

## بماذا تختلف هذه الدورة عن دورات NIST الأخرى في مجال الأمن السيبراني

تتميز هذه الدورة بتقديمها نهجًا عمليًا لتقييم مخاطر الأمن السيبراني والتدريب على امتثال أمن تكنولوجيا المعلومات. وعلى عكس دورات الأمن السيبراني التقليدية، يقدم هذا البرنامج تطبيقات عملية لتنفيذ ضوابط NIST الأمنية، وهو مصمم خصيصًا للتدريب على إطار الأمن السيبراني الحكومي وامتثال القطاع الخاص.

سيكتسب المشاركون خبرة واقعية في تطوير سياسات الأمن السيبراني باستخدام NIST وتقنيات الكشف عن التهديدات السيبرانية. ومن خلال الجلسات التفاعلية حول تقنيات مراقبة مخاطر الأمن السيبراني واستراتيجيات دورة استشارات الامتثال لـ NIST، يضمن هذا التدريب فهمًا عميقًا لأفضل الممارسات الفيدرالية للأمن السيبراني.