

دورة كبير مديري أمن السحابة المعتمد 27017 ISO/IEC و 27018

3 – 7 أكتوبر 2027

كيب تاون

AGILE LEADERS
Training Center

دورة كبير مديري أمن السحابة المعتمد ISO/IEC 27017 و 27018

المرجع: 98940_103600297 **التاريخ:** 3 – 7 أكتوبر 2027 **المكان:** كيب تاون **الرسوم:** Euro 6000

نظرة عامة على الدورة

صُممت دورة كبير مديري أمن السحابة المعتمد - ISO/IEC 27017 و 27018 لتزويد المهنيين بالأدوات والمنهجيات والأطر الأساسية اللازمة لإدارة وتعزيز برامج أمن السحابة بما يتماشى مع المعايير الدولية المعترف بها. يغطي هذا التدريب الشامل دورة حياة تنفيذ برنامج أمن السحابة بالكامل، بدءًا من تقييم المخاطر واختيار الضوابط، وصولاً إلى إدارة الحوادث والتدريب على التوعية وأفضل ممارسات التوثيق.

تطرح البيئات السحابية تحديات فريدة، بما في ذلك مخاطر خصوصية البيانات، ومتطلبات الامتثال المتطورة، وتعقيد النماذج الهجينة ومتعددة السحابات. سيكتسب المشاركون رؤية عميقة حول إدارة مخاطر أمن السحابة، وتطوير سياسات وإجراءات أمن السحابة، وتطبيق ضوابط السحابة المحددة وفقًا لمعيار ISO 27017 لتأمين البنية التحتية والخدمات السحابية.

بالإضافة إلى ذلك، تسلط الدورة الضوء على أهمية حماية بيانات السحابة وفقًا لمعيار ISO 27018 لحماية المعلومات الشخصية المحددة للهوية PII، مما يضمن دمج الخصوصية في الحوسبة السحابية في كل مرحلة من مراحل اعتماد السحابة. من خلال الجلسات التفاعلية ودراسات الحالة والتمارين العملية والعمل الجماعي التعاوني، سيخرج المشاركون باستراتيجيات عملية لدمج أفضل ممارسات أمن السحابة في النظام البيئي السحابي لمؤسساتهم.

الجمهور المستهدف

- مديرو أمن السحابة
- مسؤولو أمن المعلومات
- مديرو البنية التحتية لتكنولوجيا المعلومات والعمليات
- مهندسو ومعماريو السحابة
- المحترفون في إدارة المخاطر
- مسؤولو الامتثال والفرق القانونية
- مسؤولو حماية البيانات والخصوصية
- مستشارو وخبراء أمن السحابة

AGILE LEADERS
Training Center

الإدارات التنظيمية المستهدفة

- إدارات تكنولوجيا المعلومات والأمن السيبراني
- فرق المخاطر والامتثال
- وحدات حوكمة واستراتيجية السحابة
- الوظائف القانونية وخصوصية البيانات
- فرق المراجعة الداخلية
- فرق البنية التحتية السحابية وDevOps
- مقدمو الخدمات المُدارة MSPs

القطاعات المستهدفة

- الخدمات المالية البنوك، التأمين، التكنولوجيا المالية
- الرعاية الصحية والصناعات الدوائية
- الاتصالات
- التجزئة والتجارة الإلكترونية
- الجهات الحكومية والقطاع العام
- شركات التكنولوجيا وتطوير البرمجيات والبرمجيات كخدمة SaaS
- التصنيع والخدمات اللوجستية ذات العمليات القائمة على السحابة
- الطاقة والمرافق التي تستفيد من الحلول السحابية

أهداف الدورة

بنهاية هذا التدريب، سيتمكن المشاركون من:

- تطوير وتنفيذ برنامج لأمن السحابة مصمم خصيصًا لتلبية احتياجات المؤسسة
- تطبيق أفضل ممارسات أمن السحابة المتوافقة مع مبادئ التدريب على ISO/IEC 27017 وشهادة ISO/IEC 27018
- تقييم وتحديد وتخفيف المخاطر الخاصة بالسحابة من خلال مناهج منظمة لإدارة مخاطر أمن السحابة
- تطوير سياسات وإجراءات شاملة لأمن السحابة تغطي الجوانب التشغيلية والتقنية والحوكمية
- تصميم وتنفيذ ضوابط السحابة المحددة وفقًا لمعيار ISO 27017 عبر بيئات البنية التحتية كخدمة IaaS والمنصة كخدمة PaaS والبرمجيات كخدمة SaaS
- إنشاء وتعزيز ممارسات توثيق أمن السحابة لدعم عمليات المراجعة وإعداد التقارير والحوكمة الداخلية
- إنشاء وتقديم تدريب فعال للتوعية بأمن السحابة لجميع المستويات التنظيمية
- الاستجابة لحوادث أمن السحابة وإدارتها من خلال تدريب منظم على الاستجابة لحوادث أمن السحابة
- دعم عمليات التدريب على الترحيل السحابي الآمن لضمان دمج الأمن في مشاريع اعتماد السحابة
- ضمان الامتثال المستمر للامتثال السحابي واللوائح التنظيمية المعمول بها في قطاعهم

منهجية التدريب

يتميز هذا التدريب بطابعه العملي المكثف، حيث يمزج بين التوجيهات المتخصصة ودراسات الحالة الواقعية والعمل الجماعي التفاعلي وحل المشكلات التعاوني والتمارين الموجهة والمصممة خصيصًا لتناسب قطاعات المشاركين وبيئاتهم السحابية.

تتضمن كل جلسة مناقشات حية، وتمارين لتقييم المخاطر، وتطويرًا عمليًا لسياسات وإجراءات أمن السحابة، ومحاكاة جماعية لإدارة حوادث أمن السحابة. يتم التركيز بشكل خاص على الخصوصية في الحوسبة السحابية وحماية بيانات السحابة وفقًا لمعيار ISO 27018 لضمان فهم المشاركين لكيفية دمج ضوابط الخصوصية في العمليات والتوثيق السحابي.

ستتحدى سيناريوهات لعب الأدوار المشاركين لتطبيق ضوابط السحابة المحددة وفقًا لمعيار ISO 27017 على البيئات السحابية الهجينة والعامة المتطورة، مما يعزز المهارات العملية اللازمة لمواجهة التهديدات الناشئة والتوقعات التنظيمية. تتيح جلسات المراجعة في نهاية كل يوم للمشاركين ترسيخ ما تعلموه وتبادل الرؤى مع أقرانهم.

أدوات الدورة

- دليل عمل رقمي شامل للدورة مع إرشادات ونماذج وقوائم تحقق
- أمثلة على سياسات وإجراءات أمن السحابة المتوافقة مع معياري ISO/IEC 27017 و ISO/IEC 27018
- نماذج عملية للتدريب على تقييم المخاطر السحابية
- نماذج لممارسات توثيق أمن السحابة وقوائم تحقق للمراجعة
- شرائح عرض ومواد تواصل للتدريب على التوعية بأمن السحابة
- سيناريوهات تدريبية للاستجابة لحوادث أمن السحابة وقوائم تحقق للاستجابة
- دراسات حالة توضح أفضل ممارسات أمن السحابة في العالم الحقيقي
- لا يتم توفير الأدوات بشكل مباشر، ولكن يتم تغطية الرؤى العملية والأطر والأمثلة الواقعية للأدوات بشكل مكثف

جدول أعمال الدورة

اليوم الأول: أسس أمن السحابة والحوكمة

- الموضوع 1: مقدمة إلى أفضل ممارسات أمن السحابة ودورها في تنفيذ برنامج أمن السحابة، مع التركيز على التوافق مع التدريب على ISO/IEC 27017 وشهادة ISO/IEC 27018.
- الموضوع 2: تحديد سياسات وإجراءات أمن السحابة التي تعالج المخاطر الخاصة بالسحابة، وحماية البيانات، والامتثال السحابي واللوائح التنظيمية عبر نماذج الخدمات المختلفة.
- الموضوع 3: تحديد أدوار ومسؤوليات أمن السحابة داخل فرق تكنولوجيا المعلومات والأمن السيبراني والحوكمة لضمان فعالية التدريب على التوعية بأمن السحابة.
- الموضوع 4: تطوير ممارسات توثيق أمن السحابة التي تدعم الإدارة المستمرة للمخاطر، والاستجابة للحوادث، وعمليات المراجعة.
- الموضوع 5: نظرة عامة على مناهج التدريب على أمن السحابة الهجينة للمؤسسات التي تستخدم بيئات متعددة السحابات وهجينة.
- تأمل ومراجعة: مناقشة جماعية حول كيفية إدارة مؤسسات المشاركين لبرامج أمن السحابة حاليًا والخطوات الأولية لتعزيزها باستخدام ضوابط السحابة المحددة وفقًا لمعيار ISO 27017.

AGILE LEADERS
Training Center

اليوم الثاني: إدارة مخاطر أمن السحابة وتصميم الضوابط

- الموضوع 1: مقدمة إلى إدارة مخاطر أمن السحابة وتقنيات التدريب على تقييم المخاطر السحابية، مع التركيز على تحديد نقاط الضعف الخاصة بالسحابة.
- الموضوع 2: تطبيق أفضل ممارسات أمن السحابة لتطوير سياسات وإجراءات أمن السحابة التي تخفف من المخاطر المحددة وتدعم التدريب على الترحيل السحابي الآمن.
- الموضوع 3: اختيار وتنفيذ ضوابط السحابة المحددة وفقًا لمعيار ISO 27017 عبر بيئات شهادات أمن السحابة العامة والخاصة والمجتمعية.
- الموضوع 4: ربط ممارسات توثيق أمن السحابة بعمليات إدارة المخاطر لتحسين التتبع والمساءلة.
- الموضوع 5: الخصوصية في الحوسبة السحابية ودور حماية بيانات السحابة وفقًا لمعيار ISO 27018 في حماية المعلومات الشخصية المحددة للهوية PII.
- تأمل ومراجعة: يشارك المشاركون أمثلة لسيناريوهات المخاطر السحابية من مؤسساتهم ويتعاونون على تحديد ضوابط السحابة المناسبة المحددة وفقًا لمعيار ISO 27017.

اليوم الثالث: التوعية الأمنية وحماية البيانات وإدارة الحوادث

- الموضوع 1: تصميم وتقديم برامج تدريب فعالة للتوعية بأمن السحابة للفرق التقنية والإدارة والموظفين غير التقنيين.
- الموضوع 2: دمج مبادئ الخصوصية في الحوسبة السحابية في تنفيذ برنامج أمن السحابة، مع التركيز على حماية بيانات السحابة وفقًا لمعيار ISO 27018.
- الموضوع 3: تطوير وتوثيق برامج التدريب على الاستجابة لحوادث أمن السحابة لتحسين جاهزية المؤسسة لحوادث أمن السحابة.
- الموضوع 4: محاكاة عملية لعمليات إدارة حوادث أمن السحابة، تغطي الكشف والاحتواء والتحقيق والتعافي.
- الموضوع 5: ممارسات توثيق أمن السحابة لتسجيل سجلات الحوادث والدروس المستفادة وتقارير الحوادث المتوافقة مع الامتثال السحابي واللوائح التنظيمية.
- تأمل ومراجعة: يراجع المشاركون سيناريوهات الاستجابة للحوادث التي تمت خلال اليوم، ويقارنون بين المناهج المختلفة عبر مختلف القطاعات والبنى السحابية.

اليوم الرابع: العمليات السحابية الآمنة والتحسين المستمر

- الموضوع 1: عمليات اختبار ومراقبة أمن السحابة لتحديد نقاط الضعف وتقييم الامتثال وضمان التوافق المستمر مع أفضل ممارسات أمن السحابة.
- الموضوع 2: تطوير عمليات التدريب على الترحيل السحابي الآمن التي تدمج متطلبات الأمن في مشاريع الترحيل السحابي ومبادرات التدريب على أمن السحابة الهجينة.
- الموضوع 3: تعزيز ممارسات توثيق أمن السحابة لتتوافق مع متطلبات القطاع والحوكمة الداخلية والتقارير التنظيمية.
- الموضوع 4: استكشاف مناهج خدمات استشارات أمن السحابة لتقديم المشورة لوحدات الأعمال ومقدمي الخدمات من الأطراف الثالثة بشأن تنفيذ برنامج أمن السحابة.
- الموضوع 5: إنشاء عمليات تحسين مستمر للحفاظ على أفضل ممارسات أمن السحابة وتطويرها لمواجهة التهديدات الناشئة والتغييرات التنظيمية.
- تأمل ومراجعة: جلسة عصف ذهني جماعية حول الاتجاهات المستقبلية في إدارة مخاطر أمن السحابة، والامتثال السحابي واللوائح التنظيمية، وضوابط السحابة المحددة وفقًا لمعيار ISO 27017.

اليوم الخامس: التطبيق العملي والمواضيع المتقدمة

- الموضوع 1: ورشة عمل لدراسة حالة: تطبيق سياسات وإجراءات أمن السحابة، وتقنيات التدريب على تقييم المخاطر السحابية، وضوابط السحابة المحددة وفقًا لمعيار ISO 27017 على بيئة سحابية هجينة معقدة.
- الموضوع 2: تطوير برامج مخصصة للتدريب على التوعية بأمن السحابة والتدريب على الاستجابة للحوادث لمختلف المستويات التنظيمية والأطراف الثالثة.
- الموضوع 3: تنفيذ أطر خدمات استشارات أمن السحابة لتقييم وتصميم وتعزيز تنفيذ برنامج أمن السحابة عبر مختلف القطاعات.
- الموضوع 4: تطبيق أفضل ممارسات أمن السحابة على سيناريوهات شهادات أمن السحابة المجتمعية، وشهادات أمن السحابة العامة، والتدريب على أمن السحابة الهجينة.
- الموضوع 5: ممارسات توثيق متقدمة لأمن السحابة لإنشاء تقارير جاهزة للمراجعة، وملخصات تنفيذية، وحزم الامتثال التنظيمي.
- تأمل ومراجعة: يطور المشاركون خطط عمل فردية لتعزيز برنامج أمن السحابة في مؤسساتهم، باستخدام الرؤى المكتسبة من التدريب بأكمله.

AGILE LEADERS
Training Center

الأسئلة الشائعة

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

لا توجد متطلبات مسبقة إلزامية، ولكن وجود فهم أساسي للحوسبة السحابية وإدارة أمن المعلومات ومبادئ إدارة المخاطر سيعزز تجربة التعلم للمشاركين. تعتبر الدورة مثالية للأفراد المشاركين في مسارات شهادات مديري أمن السحابة، أو خدمات استشارات أمن السحابة، أو المسؤولين عن حوكمة السحابة والمخاطر والامتثال.

كم مدة جلسة كل يوم، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تستمر جلسة كل يوم عادةً من 4 إلى 5 ساعات، وتتضمن أجزاء تعليمية ودراسات حالة وعملاً جماعيًا ومناقشات تفاعلية. على مدار أسبوع، سيكمل المشاركون ما يقرب من 20 إلى 25 ساعة من التعلم المنظم.

كيف ينطبق معيارا ISO/IEC 27017 و ISO/IEC 27018 على أمن السحابة الهجينة وحماية الخصوصية؟

يقدم معيار ISO/IEC 27017 إرشادات لتطبيق ضوابط السحابة المحددة وفقًا لمعيار ISO 27017 لتأمين البيئات السحابية الهجينة، مما يضمن فهم كل من مزودي الخدمات والعملاء لمسؤولياتهم. يعزز معيار ISO/IEC 27018 ذلك من خلال إدخال ضوابط خاصة بالخصوصية تركز على حماية المعلومات الشخصية المحددة للهوية PII، وهو أمر بالغ الأهمية بشكل خاص عند التعامل مع البيانات الحساسة في السحابات العامة والهجينة.

بماذا تختلف هذه الدورة عن دورات كبير مديري أمن السحابة المعتمد الأخرى

تتميز هذه الدورة بتركيزها العملي والتطبيقي المكثف. فبدلاً من الاكتفاء بالتعليمات النظرية، يشارك المتدربون بفعالية في تطوير سياسات وإجراءات أمن السحابة، وتقييم المخاطر الخاصة بالسحابة، وبناء ممارسات توثيق أمن السحابة، وإدارة حوادث أمن السحابة المحاكاة. من خلال دمج التدريب على تقييم المخاطر السحابية، والتدريب على الترحيل السحابي الآمن، ودراسات الحالة الواقعية، تضمن الدورة أن يخرج المشاركون بأدوات عملية يمكنهم تطبيقها على الفور.