

دورة معتمدة في إدارة حوادث أمن المعلومات

ISO/IEC 27035

8 – 12 أغسطس 2027

شيكاغو

AGILE LEADERS
Training Center

دورة معتمدة في إدارة حوادث أمن المعلومات ISO/IEC 27035

المرجع: 98839_103600295 **التاريخ:** 8 – 12 أغسطس 2027 **المكان:** شيكاغو **الرسوم:** 16000 Euro

نظرة عامة على الدورة التدريبية

تزود دورة التدريب والاعتماد في إدارة حوادث أمن المعلومات ISO/IEC 27035 المشاركين بالمعرفة الشاملة والمهارات العملية اللازمة لتصميم عمليات فعالة للاستجابة للحوادث وتنفيذها وإدارتها بما يتماشى مع معيار ISO/IEC 27035. تركز هذه الدورة التدريبية على دورة حياة إدارة الحوادث، بدءًا من اكتشاف الحوادث والإبلاغ عنها، وصولاً إلى الاحتواء والإزالة والتعافي والدروس المستفادة.

سيكتسب المشاركون خبرة في التدريب على إدارة حوادث أمن المعلومات من خلال التمارين العملية ودراسات الحالة والسيناريوهات الواقعية. تسلط الدورة الضوء على تكامل معيار ISO/IEC 27035 مع معياري ISO/IEC 27001 و ISO/IEC 27005، مع التركيز على إدارة المخاطر ومواءمة الامتثال. من خلال التدريب على الاستجابة للحوادث، سيطور المشاركون تقنيات لتحديد التهديدات وتقييم تأثير الحوادث وتفعيل فرق الاستجابة للحوادث.

يغطي التدريب على إدارة الحوادث وفقًا لمعيار ISO/IEC 27035 أيضًا التواصل بشأن الحوادث والإبلاغ عنها والتحسين المستمر، مما يضمن قدرة المشاركين على قيادة وتعزيز قدرات الاستجابة للحوادث في المنظمة. يُعد إتمام هذه الدورة التدريبية المعتمدة المشاركين للحصول على شهادة مدير الحوادث المعتمد من PECB وفقًا لمعيار ISO/IEC 27035، مما يعزز الفرص الوظيفية للمتخصصين في الاستجابة للحوادث ومديري المخاطر وقادة أمن تكنولوجيا المعلومات.

الجمهور المستهدف

- مديرو حوادث أمن المعلومات
- مديرو تكنولوجيا المعلومات وأمن المعلومات
- أعضاء فريق الاستجابة للحوادث IRT
- مديرو المخاطر ومسؤولو الامتثال
- مسؤولو أنظمة وشبكات تكنولوجيا المعلومات
- المدققون الداخليون
- الاستشاريون المشاركون في إدارة حوادث أمن المعلومات
- المحترفون الذين يستعدون للحصول على شهادة مدير الحوادث المعتمد وفقًا لمعيار ISO/IEC 27035

AGILE LEADERS
Training Center

الإدارات التنظيمية المستهدفة

- إدارات أمن المعلومات والأمن السيبراني
- فرق عمليات تكنولوجيا المعلومات وإدارة الشبكات
- فرق الاستجابة للحوادث ومراكز العمليات الأمنية SOCs
- مكاتب إدارة المخاطر والامتثال
- إدارات التدقيق الداخلي والحوكمة
- فرق استمرارية الأعمال والتعافي من الكوارث

القطاعات المستهدفة

- الخدمات المصرفية والمالية
- الرعاية الصحية والصناعات الدوائية
- القطاع الحكومي والعام
- التكنولوجيا والاتصالات
- قطاعات التصنيع وسلسلة التوريد
- البنية التحتية الحيوية والمرافق العامة
- التجارة الإلكترونية والخدمات عبر الإنترنت
- الخدمات الاستشارية والمهنية

مخرجات الدورة التدريبية

بنهاية هذه الدورة التدريبية، سيتمكن المشاركون من:

- شرح دورة حياة الاستجابة للحوادث وفقًا لمعيار ISO/IEC 27035
- تطبيق خارطة طريق تنفيذ معيار ISO/IEC 27035 لبناء عمليات إدارة الحوادث
- إجراء تدريب على تحديد تهديدات أمن المعلومات وتحليل مخاطر الحوادث
- تصميم إجراءات اكتشاف الحوادث والإبلاغ عنها وفقًا لمعيار ISO/IEC 27035
- تنفيذ التدريب على احتواء الحوادث وإزالتها
- تطبيق تقنيات التدريب على التحقيق في حوادث أمن المعلومات
- إدارة مراجعات ما بعد الحادث والتدريب على الدروس المستفادة
- مواءمة المراقبة والتحسين المستمر وفقًا لمعيار ISO/IEC 27035 مع متطلبات معيار ISO/IEC 27001
- الاستعداد لعملية التحضير لامتحان شهادة PECB ISO/IEC 27035

AGILE LEADERS
Training Center

منهجية التدريب

تستخدم هذه الدورة التدريبية نهجًا تعليميًا تفاعليًا وعمليًا يجمع بين إرشادات الخبراء ودراسات الحالة العملية والمناقشات الجماعية والتمارين القائمة على السيناريوهات. يعمل المشاركون على كامل عملية الاستجابة للحوادث، بدءًا من الاكتشاف الأولي للحادث وصولاً إلى التعافي والمتابعة، باستخدام إطار عمل الاستجابة للحوادث وفقًا لمعيار ISO/IEC 27035.

تتضمن الدورة عملاً جماعيًا تفاعليًا حيث يطور المشاركون خطط إدارة الحوادث، ويحددون الأدوار والمسؤوليات، ويبنون استراتيجيات الاتصال باستخدام التدريب على التواصل بشأن حوادث أمن المعلومات. يُجري المشاركون أيضًا عمليات محاكاة للحوادث، مطبقين التدريب على التعامل مع الحوادث والاستجابة لها لاحتواء الحوادث الأمنية وإزالتها والتعافي منها.

طوال فترة التدريب، يراجع المشاركون استراتيجيات المراقبة والتحسين المستمر وفقًا لمعيار ISO/IEC 27035، وتقنيات مراجعة ما بعد الحادث، وعمليات التحضير للتدقيق، مما يضمن التوافق مع معيار ISO/IEC 27035 لتحقيق الامتثال لمعيار ISO/IEC 27001 وبرامج الحوكمة الأوسع.

أدوات الدورة التدريبية

- دليل التدريب على معيار ISO/IEC 27035
- نماذج سياسات وإجراءات إدارة الحوادث
- نماذج التواصل والتصعيد بشأن الحوادث
- قوائم التحقق لاكتشاف الحوادث والإبلاغ عنها
- مصفوفة أدوار ومسؤوليات إدارة الحوادث
- نماذج لتقييم مخاطر الحوادث
- نماذج توثيق مراجعة ما بعد الحادث والدروس المستفادة
- دليل التحضير لامتحان شهادة ISO/IEC 27035
- دراسات حالة توضح أفضل الممارسات في إدارة الحوادث وفقًا لمعيار ISO/IEC 27035
- أدوات تتبع ومراقبة الحوادث أمثلة

AGILE LEADERS
Training Center

جدول أعمال الدورة التدريبية

اليوم الأول: مقدمة والمبادئ الأساسية لإدارة الحوادث

- الموضوع 1: نظرة عامة على الدورة التدريبية وعملية الحصول على الشهادة وفقًا لمعيار ISO/IEC 27035
- الموضوع 2: فهم أساسيات التدريب على إدارة حوادث أمن المعلومات
- الموضوع 3: دورة حياة الاستجابة للحوادث وفقًا لمعيار ISO/IEC 27035 وتكاملها مع معيار ISO/IEC 27001
- الموضوع 4: التدريب على تحديد أدوار ومسؤوليات إدارة الحوادث
- الموضوع 5: تطوير سياسات وإجراءات إدارة الحوادث
- الموضوع 6: التدريب على تحديد تهديدات أمن المعلومات والتقييم الأولي للمخاطر
- تأمل ومراجعة: مراجعة متطلبات شهادة مدير الحوادث المعتمد وفقًا لمعيار ISO/IEC 27035 والنقاط الرئيسية

اليوم الثاني: اكتشاف الحوادث والإبلاغ عنها وتقييمها

- الموضوع 1: تقنيات اكتشاف الحوادث وأفضل ممارسات المراقبة وفقًا لمعيار ISO/IEC 27035
- الموضوع 2: إرشادات حول برامج الإبلاغ عن الحوادث وتتبعها
- الموضوع 3: التدريب على إجراءات التواصل والتصعيد بشأن الحوادث
- الموضوع 4: التدريب على تقييم الحوادث واتخاذ القرارات
- الموضوع 5: التدريب على إجراء تقييم لأحداث أمن المعلومات
- الموضوع 6: التدريب على إعداد وثائق إدارة الحوادث ونماذج الإبلاغ
- تأمل ومراجعة: مراجعة عمليات اكتشاف الحوادث والإبلاغ عنها

اليوم الثالث: الاستجابة للحوادث وإزالتها

- الموضوع 1: تدريب فريق الاستجابة للحوادث IRT وعمليات تفعيله
- الموضوع 2: التدريب على التعامل مع الحوادث والاستجابة لها باستخدام معيار ISO/IEC 27035
- الموضوع 3: أفضل ممارسات التدريب على احتواء الحوادث وإزالتها
- الموضوع 4: أساليب التدريب على التحقيق في حوادث أمن المعلومات
- الموضوع 5: الاعتبارات القانونية والتنظيمية في الاستجابة للحوادث
- الموضوع 6: دمج الاستجابة للحوادث مع إدارة المخاطر وفقًا لمعيار ISO/IEC 27035
- تأمل ومراجعة: مراجعة استراتيجيات وتقنيات الاستجابة للحوادث

اليوم الرابع: مراجعة ما بعد الحادث والتحسين المستمر

- الموضوع 1: التدريب على إجراء مراجعة ما بعد الحادث والدروس المستفادة
- الموضوع 2: تطبيق إطار التحسين المستمر لمعيار ISO/IEC 27035 على إدارة الحوادث
- الموضوع 3: التدريب على التدقيق الداخلي والمراجعة لبرامج الحوادث وفقًا لمعيار ISO/IEC 27035
- الموضوع 4: تقنيات المراقبة والتحسين المستمر لعمليات الحوادث
- الموضوع 5: دراسات حالة وأمثلة واقعية على إدارة الحوادث وفقًا لمعيار ISO/IEC 27035
- الموضوع 6: مواءمة معيار ISO/IEC 27035 مع معيار ISO/IEC 27001 وأطر الحوكمة الأخرى
- تأمل ومراجعة: مراجعة استراتيجيات التحسين المستمر والتدقيق

اليوم الخامس: التحضير للشهادة والمراجعة النهائية

- الموضوع 1: مراجعة المفاهيم الرئيسية للتحضير لامتحان شهادة PECB ISO/IEC 27035
- الموضوع 2: مراجعة أفضل الممارسات في إدارة الحوادث ودراسات الحالة وفقًا لمعيار ISO/IEC 27035
- الموضوع 3: مراجعة فرص التطوير الوظيفي لمدير الحوادث المعتمد وفقًا لمعيار ISO/IEC 27035
- الموضوع 4: المراجعة النهائية لخارطة طريق التنفيذ والتحضير للتدقيق وفقًا لمعيار ISO/IEC 27035
- الموضوع 5: الامتحان النهائي للحصول على الشهادة
- تأمل ومراجعة: الملاحظات النهائية من الزملاء وخطط عمل المشاركين

الأسئلة الشائعة

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

لا توجد متطلبات مسبقة رسمية لهذه الدورة التدريبية. ومع ذلك، ستكون المعرفة الأساسية بأمن المعلومات أو إدارة المخاطر أو عمليات الاستجابة للحوادث مفيدة. هذه الدورة مثالية لأولئك الذين يسعون للحصول على شهادة مدير الحوادث المعتمد وفقًا لمعيار ISO/IEC 27035.

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

تستمر كل جلسة يومية حوالي 4-5 ساعات، وتشمل العروض التقديمية والتمارين التفاعلية والمناقشات الجماعية. تبلغ المدة الإجمالية للتدريب المعتمد وفقًا لمعيار ISO/IEC 27035 حوالي 20-25 ساعة على مدار أسبوع.

AGILE LEADERS
Training Center

كيف يتكامل معيار ISO/IEC 27035 مع معياري ISO/IEC 27001 و ISO/IEC 27005؟

يكمل معيار ISO/IEC 27035 معيار ISO/IEC 27001 من خلال تعزيز قدرات الاستجابة للحوادث ضمن نظام إدارة أمن المعلومات الأوسع. كما أنه يدعم معيار ISO/IEC 27005 من خلال معالجة المخاطر المتعلقة بالحوادث ومواءمة عمليات إدارة الحوادث مع أطر إدارة المخاطر في المؤسسة.

بماذا تختلف هذه الدورة عن غيرها من الدورات التدريبية المعتمدة في إدارة حوادث أمن المعلومات ISO/IEC 27035

تتميز هذه الدورة التدريبية بتقديمها نهجًا عمليًا وتطبيقيًا لإدارة دورة حياة الاستجابة للحوادث بالكامل، بدءًا من الاكتشاف وحتى الدروس المستفادة. على عكس الدورات الأخرى، تدمج هذه الدورة التدريب المعتمد مع دراسات حالة واقعية، مما يساعد المشاركين على تطبيق تقنيات تحديد التهديدات وتقييم المخاطر واحتواء الحوادث في سيناريوهات واقعية.

تركز الدورة أيضًا بشكل كبير على التواصل بشأن الحوادث، والإبلاغ عنها، ومواءمة الامتثال مع معياري ISO/IEC 27001 و ISO/IEC 27005. لا يتعلم المشاركون كيفية تطوير خطط الاستجابة للحوادث فحسب، بل يتعلمون أيضًا كيفية إدارة فرق الاستجابة للحوادث وضمان التحسين المستمر باستخدام إطار التحسين المستمر لمعيار ISO/IEC 27035. بالإضافة إلى التحضير الشامل لامتحان شهادة PECB ISO/IEC 27035، يضمن هذا التدريب أن يكون المشاركون مستعدين تقنيًا ومعتمدين مهنيًا، مما يجعله مثاليًا لمديري الحوادث ومسؤولي المخاطر وقادة الأمن.