

دورة قانون DORA للمرونة التشغيلية الرقمية للمؤسسات المالية

21 – 25 نوفمبر 2027

المنامة

AGILE LEADERS
Training Center

دورة قانون DORA للمرونة التشغيلية الرقمية للمؤسسات المالية

المرجع: 99799_103600318 **التاريخ:** 21 – 25 نوفمبر 2027 **المكان:** المنامة **الرسوم:** Euro 6500

نظرة عامة على الدورة:

دورة قانون DORA للمرونة التشغيلية الرقمية للمؤسسات المالية هي برنامج شامل مصمم لمساعدة المهنيين في القطاع المالي على تحقيق الامتثال لقانون المرونة التشغيلية الرقمية DORA مع تعزيز المرونة الرقمية، وإدارة مخاطر تكنولوجيا المعلومات والاتصالات، والامتثال للأمن السيبراني. مع تحول DORA إلى إطار تنظيمي رئيسي، يجب على المؤسسات التكيف مع المتطلبات الصارمة لإدارة المخاطر المالية، وتطوير مرونة تشغيلية قوية، وإجراء تقييمات معمقة للمخاطر للتخفيف من تهديدات تكنولوجيا المعلومات والاتصالات.

تقدم هذه الدورة تجربة تعليمية تفاعلية مع استراتيجيات تدريبية واقعية للامتثال، ودراسات حالة، وأفضل الممارسات لتقييم مخاطر تكنولوجيا المعلومات والاتصالات. سيتعلم المشاركون كيفية مواءمة مؤسساتهم مع المتطلبات التنظيمية لـ DORA، وتطبيق أطر عمل الأمن السيبراني للمؤسسات المالية، وإدارة مخاطر تكنولوجيا المعلومات والاتصالات للطرف الثالث بفعالية. بنهاية هذه الدورة، سيكون الحاضرون مستعدين جيدًا لاجتياز دورة شهادة DORA عبر الإنترنت واتخاذ خطوات استباقية للحد من الثغرات الأمنية في تكنولوجيا المعلومات والاتصالات.

الجمهور المستهدف:

- المديرون التنفيذيون وصناع القرار في المؤسسات المالية
- مسؤولو الامتثال والمديرون التنظيميون
- محترفو تكنولوجيا المعلومات والأمن السيبراني
- محترفو إدارة المخاطر
- الاستشاريون المتخصصون في الامتثال بالقطاع المالي

الإدارات التنظيمية المستهدفة:

- الامتثال والشؤون التنظيمية
- أمن تكنولوجيا المعلومات وإدارة المخاطر
- فرق الأمن السيبراني والمرونة التشغيلية
- وحدات التدقيق الداخلي والحوكمة
- فرق إدارة موردي الطرف الثالث

AGILE LEADERS
Training Center

القطاعات المستهدفة:

- الخدمات المصرفية والمالية
- التكنولوجيا المالية والمدفوعات الرقمية
- شركات التأمين والاستثمار
- الهيئات التنظيمية والوكالات الحكومية
- شركات الاستشارات المتخصصة في امتثال الأمن السيبراني

مخرجات الدورة:

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم متطلبات امتثال DORA وتأثيرها على المؤسسات المالية
- تطوير استراتيجيات المرونة التشغيلية الرقمية لحماية الأصول المالية
- تطبيق أفضل ممارسات إدارة مخاطر تكنولوجيا المعلومات والاتصالات للتخفيف من التهديدات السيبرانية
- تعزيز امتثال الأمن السيبراني من خلال أطر تنظيمية فعالة
- إجراء تقييمات شاملة للمخاطر وتدقيق مزودي خدمات تكنولوجيا المعلومات والاتصالات من الطرف الثالث
- تعزيز قدرات الاستجابة للحوادث وتحسين إجراءات إدارة الأزمات
- الاستعداد لاجتياز دورة شهادة DORA عبر الإنترنت والنجاح فيها

منهجية التدريب:

تعتمد هذه الدورة على نهج تفاعلي وجذاب، يجمع بين الجلسات التي يقودها المدرب، ودراسات الحالة الواقعية، وورش العمل التطبيقية. سيشارك المشاركون في:

- تمارين قائمة على السيناريوهات لتقييم أطر عمل الأمن السيبراني للمؤسسات المالية
- مناقشات تركز على استراتيجيات تطبيق DORA
- تقييمات عملية للمخاطر لتحليل الثغرات الأمنية في تكنولوجيا المعلومات والاتصالات
- أنشطة لعب الأدوار لمحاكاة الإشراف على الطرف الثالث بموجب DORA
- اختبارات وتقييمات لتتبع التقدم وضمان استيعاب المعرفة

أدوات الدورة:

سيحصل المشاركون على مجموعة متنوعة من الموارد، تشمل:

- كتيبات عمل رقمية وقوائم تحقق للامتثال
- تقارير تحليل دراسات الحالة
- قوالب أطر سياسات DORA
- أدوات ومنهجيات تقييم المخاطر
- الوصول إلى مواد تعليمية عبر الإنترنت والتحديثات التنظيمية

جدول أعمال الدورة:

اليوم الأول: مقدمة إلى DORA والمرونة التشغيلية الرقمية

- **الموضوع 1:** نظرة عامة على قانون المرونة التشغيلية الرقمية DORA
- **الموضوع 2:** الأهداف الرئيسية ونطاق امتثال DORA للمؤسسات المالية
- **الموضوع 3:** المفاهيم الأساسية لإدارة مخاطر تكنولوجيا المعلومات والاتصالات والمرونة الرقمية
- **الموضوع 4:** متطلبات الحوكمة والمتطلبات التنظيمية لتطبيق DORA
- **الموضوع 5:** التخطيط والإعداد لاستراتيجية امتثال ناجحة لـ DORA
- **الموضوع 6:** فهم إدارة المخاطر المالية في بيئة رقمية
- **تأمل ومراجعة:** النقاط الرئيسية ومناقشة خطوات التنفيذ الأولية

اليوم الثاني: إدارة مخاطر وحوادث تكنولوجيا المعلومات والاتصالات بموجب DORA

- **الموضوع 1:** تحديد المخاطر المتعلقة بتكنولوجيا المعلومات والاتصالات في المؤسسات المالية
- **الموضوع 2:** تطوير نهج قائم على المخاطر لإدارة مخاطر تكنولوجيا المعلومات والاتصالات
- **الموضوع 3:** إطار إدارة حوادث تكنولوجيا المعلومات والاتصالات والتزامات الإبلاغ
- **الموضوع 4:** امتثال الأمن السيبراني وأفضل الممارسات للمؤسسات المالية
- **الموضوع 5:** التوقعات التنظيمية للامتثال لأمن ومرونة تكنولوجيا المعلومات والاتصالات
- **الموضوع 6:** تقنيات تقييم المخاطر المالية للمواءمة التنظيمية
- **تأمل ومراجعة:** سيناريوهات عملية ودروس مستفادة من حوادث مخاطر تكنولوجيا المعلومات والاتصالات

اليوم الثالث: إدارة مخاطر تكنولوجيا المعلومات والاتصالات للطرف الثالث وإطار الإشراف

- **الموضوع 1:** اختبار المرونة التشغيلية الرقمية لمزودي خدمات تكنولوجيا المعلومات والاتصالات من الطرف الثالث
- **الموضوع 2:** إدارة مخاطر تكنولوجيا المعلومات والاتصالات للطرف الثالث في القطاع المالي
- **الموضوع 3:** إطار الإشراف ودور المشرف الرئيسي
- **الموضوع 4:** تبادل المعلومات والاستخبارات لمرونة الأمن السيبراني
- **الموضوع 5:** الالتزامات القانونية والتعاقدية بموجب DORA لموردي الطرف الثالث
- **الموضوع 6:** أطر مراقبة المخاطر والإبلاغ عنها لأمن سلسلة توريد تكنولوجيا المعلومات والاتصالات
- **تأمل ومراجعة:** التحديات والاستراتيجيات في إدارة مخاطر الطرف الثالث

اليوم الرابع: التحسين المستمر والامتثال التنظيمي

- **الموضوع 1:** برامج التدريب والتوعية للمرونة الرقمية في المؤسسات المالية
- **الموضوع 2:** السلطات المختصة والإنفاذ التنظيمي لامتثال DORA
- **الموضوع 3:** مراقبة وقياس وتقييم المرونة التشغيلية
- **الموضوع 4:** تقنيات التدقيق الداخلي لضمان أمن وامتثال تكنولوجيا المعلومات والاتصالات
- **الموضوع 5:** أفضل الممارسات للتحسين المستمر في أطر عمل الأمن السيبراني
- **الموضوع 6:** استراتيجيات المرونة الرقمية للمديرين التنفيذيين الماليين ومديري المخاطر
- **تأمل ومراجعة:** دراسات حالة ومراجعة استراتيجيات الامتثال الداخلية

اليوم الخامس: تعزيز المرونة الرقمية واستراتيجيات الامتثال المستقبلية

- **الموضوع 1:** مناهج متقدمة لإدارة مخاطر الأمن السيبراني في القطاع المالي
- **الموضوع 2:** دمج امتثال DORA في استراتيجيات المرونة على مستوى المؤسسة
- **الموضوع 3:** الاتجاهات والتحديات الناشئة في حوكمة تكنولوجيا المعلومات والاتصالات للمؤسسات المالية
- **الموضوع 4:** تطوير خطة عمل لامتثال المرونة الرقمية على المدى الطويل
- **الموضوع 5:** تقليل الثغرات الأمنية في تكنولوجيا المعلومات والاتصالات وتعزيز إدارة المخاطر
- **الموضوع 6:** الاستعداد للتحديثات التنظيمية المستقبلية وتهديدات الأمن السيبراني المتطورة
- **تأمل ومراجعة:** الرؤى النهائية للدورة، ومناقشة، والنقاط الرئيسية

الأسئلة الشائعة:

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

لا توجد متطلبات مسبقة إلزامية، ولكن يُفضل وجود فهم أساسي للوائح المالية أو أمن تكنولوجيا المعلومات والاتصالات أو إدارة المخاطر.

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

تستمر جلسة كل يوم حوالي 4-5 ساعات، مع فترات راحة وأنشطة تفاعلية. تمتد مدة الدورة الإجمالية على مدى أسبوع، بما يقارب 20-25 ساعة من التدريس.

ما هو دور الإشراف على الطرف الثالث في امتثال DORA؟

يعد الإشراف على الطرف الثالث أمرًا بالغ الأهمية بموجب DORA حيث يجب على المؤسسات المالية ضمان امتثال مزودي خدمات تكنولوجيا المعلومات والاتصالات لمتطلبات المرونة التشغيلية. تقدم هذه الدورة استراتيجيات لتقييم وإدارة مخاطر الطرف الثالث بفعالية.

كيف تختلف هذه الدورة عن دورات امتثال DORA الأخرى:

تتميز هذه الدورة بتقديمها نهجًا تفاعليًا وواقعيًا للتدريب على امتثال DORA للمؤسسات المالية. على عكس الدورات القياسية التي تركز فقط على الجانب النظري، فإننا ندمج:

- دراسات حالة حية مصممة خصيصًا لقطاع إدارة المخاطر المالية
- محاكاة لأطر عمل الأمن السيبراني لمساعدة المشاركين على تطبيق المعرفة في الوقت الفعلي
- ورش عمل حول الامتثال التنظيمي تغطي استراتيجيات تطبيق DORA
- إعداد شامل للاختبار لتحقيق شهادة DORA

لم يُصمم هذا البرنامج للتعليم فحسب، بل لتمكين المهنيين الماليين من تعزيز المرونة في الأمن السيبراني، وتقليل الثغرات الأمنية في تكنولوجيا المعلومات والاتصالات، وتطوير استراتيجيات امتثال قابلة للتنفيذ.