

المبادئ الأساسية لمخاطر الاتصالات والامتثال التنظيمي في قطاع الاتصالات الحيوي

4 – 8 أكتوبر 2027

فرانكفورت

AGILE LEADERS
Training Center

المبادئ الأساسية لمخاطر الاتصالات والامتثال التنظيمي في قطاع الاتصالات الحيوي

المرجع: 108296_103600635 **التاريخ:** 4 – 8 أكتوبر 2027 **المكان:** فرانكفورت **الرسوم:** Euro 5700

نظرة عامة على الدورة:

تزود دورة تدريب مخاطر الاتصالات والامتثال التنظيمي المشاركين بالقدرة على إدارة المخاطر التنظيمية والتشغيلية، ومخاطر الأمن السيبراني، والخصوصية، والاحتيال، والمنافسة، والاستمرارية عبر مؤسسات الاتصالات.

تشرح الدورة الإطار التنظيمي للاتصالات الذي يحكم الترخيص، والطيف الترددي، والربط البيني، والمنافسة، وحماية المستهلك، والخصوصية، وأمن الشبكات. كما توضح كيف يتفاعل التنظيم القطاعي مع قانون المنافسة ولماذا يجب على المشغلين الحفاظ على برامج امتثال فعالة.

باستخدام إرشادات إدارة المخاطر ITU-T X.1055 وNIST، يتعلم المشاركون كيفية إجراء تقييم مخاطر الاتصالات، وتصنيف المخاطر، واختيار الضوابط، وتحديد ملكية المخاطر، وتحديد أولويات إجراءات المعالجة، والإبلاغ عن التعرض للإدارة.

تجمع الدورة بين إدارة مخاطر الاتصالات والتدريب العملي على الامتثال التنظيمي للاتصالات، مما يساعد المشاركين على تحسين حوكمة الاتصالات والامتثال، والامتثال للأمن السيبراني في الاتصالات، والامتثال لخصوصية بيانات الاتصالات، والتدقيق والامتثال في الاتصالات، وإدارة مخاطر الاحتيال في الاتصالات، وأمن شبكات الاتصالات، واستمرارية أعمال الاتصالات.

AGILE LEADERS
Training Center

الجمهور المستهدف:

- مديرو مخاطر الاتصالات والامتثال
- متخصصو الشؤون التنظيمية والقانونية
- المدققون الداخليون ومتخصصو الحوكمة والمخاطر والامتثال GRC
- مديرو الأمن السيبراني وأمن الشبكات
- مسؤولو حماية البيانات والخصوصية
- متخصصو الاحتيال وضمان الإيرادات
- مديرو استمرارية الأعمال
- مديرو عمليات وهندسة الاتصالات
- متخصصو الترخيص والطيف الترددي والربط البيني
- كبار المديرين المسؤولين عن حوكمة الاتصالات

الإدارات التنظيمية المستهدفة:

- الشؤون التنظيمية والترخيص
- إدارة مخاطر المؤسسة
- الشؤون القانونية والامتثال
- التدقيق الداخلي
- الأمن السيبراني وأمن المعلومات
- عمليات الشبكة
- حماية البيانات والخصوصية

AGILE LEADERS
Training Center

الصناعات المستهدفة:

- مشغلو شبكات الهاتف المحمول
- مشغلو الخطوط الثابتة والنطاق العريض
- مقدمو خدمات الإنترنت
- شركات الاتصالات الفضائية
- مشغلو الشبكات الافتراضية المتنقلة
- مقدمو البنية التحتية للاتصالات
- مقدمو مراكز البيانات والخدمات السحابية
- موردو معدات الاتصالات

مخرجات الدورة:

بحلول نهاية هذه الدورة، سيكون المشاركون قادرين على:

- تفسير المتطلبات الرئيسية للإطار التنظيمي للاتصالات.
- إجراء تقييم منظم لمخاطر الاتصالات.
- بناء سجلات مخاطر الاتصالات والامتثال.
- تحديد المخاطر التنظيمية والتشغيلية والسيبرانية والخصوصية والاحتيال.
- تحديد مستوى تقبل المخاطر، والتسامح معها، وملكيتها، وإجراءات معالجتها.
- تعزيز ضوابط حوكمة الاتصالات والامتثال.
- تحسين الامتثال للأمن السيبراني في الاتصالات وأمن شبكات الاتصالات.
- تقييم متطلبات الامتثال لخصوصية بيانات الاتصالات.
- تطبيق أساليب التدقيق والامتثال في الاتصالات القائمة على المخاطر.
- تحسين إدارة مخاطر الاحتيال في الاتصالات.
- دعم استمرارية أعمال الاتصالات والإبلاغ عن الحوادث.
- تقديم معلومات المخاطر والامتثال للإدارة والجهات التنظيمية.

AGILE LEADERS
Training Center

منهجية التدريب:

تستخدم الدورة مناقشات يقودها المدرب، ودراسات حالة في الاتصالات، وتمارين جماعية، وسيناريوهات مخاطر، وأنشطة رسم خرائط الامتثال.

يدرس المشاركون أمثلة حقيقية تتضمن انتهاكات المنافسة، والتسعير غير العادل، وإخفاقات الخصوصية، وحوادث الشبكة، والاحتيال، والاضطراب التشغيلي. ويطبقون دورة مخاطر ITU-T X.1055 لتقييم المخاطر، واختيار الضوابط، ومراقبة الفعالية، وتحسين معالجة المخاطر.

تساعد التمارين القائمة على NIST المشاركين على تحديد أولويات مخاطر الأمن السيبراني، وتعيين مالكي المخاطر، واختيار الاستجابات، واستكمال سجلات المخاطر.

تشمل الأنشطة الجماعية تحليل الفجوات التنظيمية، وتطوير سجل المخاطر، وتقييم الضوابط، وتصعيد الحوادث، وتخطيط التدقيق، والتقارير الإدارية. وتعزز جلسات التغذية الراجعة التطبيق العملي في مكان العمل.

صندوق أدوات الدورة:

- مثال على سجل مخاطر الاتصالات
- قائمة التحقق من الامتثال التنظيمي
- دليل تقييم مخاطر الاتصالات
- نموذج تحليل فجوات الامتثال
- أمثلة على مستوى تقبل المخاطر والتسامح معها
- مثال على رسم خرائط ضوابط الاتصالات
- مثال على سجل مخاطر الأمن السيبراني

AGILE LEADERS
Training Center

جدول أعمال الدورة:

اليوم الأول: الإطار التنظيمي للاتصالات وحوكمة الامتثال

- **الموضوع 1:** الغرض وهيكل الإطار التنظيمي للاتصالات
- **الموضوع 2:** أدوار الجهات التنظيمية، والمشغلين، وسلطات المنافسة، والهيئات الدولية
- **الموضوع 3:** الترخيص، والطيف الترددي، والربط البيني، والتزامات الخدمة الشاملة
- **الموضوع 4:** الامتثال التنظيمي للاتصالات عبر خدمات الاتصالات
- **الموضوع 5:** مسؤوليات حوكمة الاتصالات والامتثال
- **الموضوع 6:** بناء برنامج فعال لإدارة الامتثال في الاتصالات
- **تأمل ومراجعة:** رسم خرائط الالتزامات التنظيمية وتحديد ملكية الامتثال الداخلية.

اليوم الثاني: إدارة مخاطر الاتصالات وتقييم المخاطر

- **الموضوع 1:** مبادئ إدارة مخاطر الاتصالات
- **الموضوع 2:** تحديد أصول وأنظمة وخدمات الأطراف الثالثة في الاتصالات
- **الموضوع 3:** تقييم مخاطر الاتصالات باستخدام التهديدات ونقاط الضعف والاحتمالية والتأثير
- **الموضوع 4:** المخاطر التشغيلية والشبكية والمعلوماتية والمادية ومخاطر الامتثال
- **الموضوع 5:** مستوى تقبل المخاطر، والتسامح معها، والمخاطر الكامنة، والمخاطر المتبقية
- **الموضوع 6:** معالجة المخاطر، واختيار الضوابط، والتحسين المستمر
- **تأمل ومراجعة:** تطوير سيناريوهات مخاطر الاتصالات وتحديد أولوياتها.

اليوم الثالث: الامتثال التنظيمي والمنافسة والخصوصية والاحتيال

- **الموضوع 1:** التفاعل بين تنظيم الاتصالات وقانون المنافسة
- **الموضوع 2:** تحديد الأسعار، وتقاسم السوق، وتبادل المعلومات، والاتفاقيات المقيدة
- **الموضوع 3:** مخاطر الوضع المهيمن، والتسعير غير العادل، والتجميع، والوصول إلى البنية التحتية
- **الموضوع 4:** الامتثال لخصوصية بيانات الاتصالات لبيانات المشتركين وحركة المرور
- **الموضوع 5:** إدارة مخاطر الاحتيال في الاتصالات وضمان الإيرادات
- **الموضوع 6:** حماية المستهلك، والشفافية، وجودة الخدمة
- **تأمل ومراجعة:** تقييم حالة سلوك في الاتصالات وتحديد مخاطر الامتثال.

اليوم الرابع: الامتثال للأمن السيبراني والمرونة التشغيلية

- **الموضوع 1:** دمج الامتثال للأمن السيبراني في الاتصالات مع مخاطر المؤسسة
- **الموضوع 2:** أمن شبكات الاتصالات ومخاطر توفر الخدمة
- **الموضوع 3:** التهديدات السيبرانية، والوصول غير المصرح به، والانقطاعات، وفشل التكوين
- **الموضوع 4:** ضوابط الأمان، والمراقبة، وإدارة الوصول، والاستجابة للحوادث
- **الموضوع 5:** استمرارية أعمال الاتصالات، والتكرار، والتعافي من الكوارث
- **الموضوع 6:** تصعيد الحوادث السيبرانية والإبلاغ التنظيمي
- **تأمل ومراجعة:** تحديد أولويات المخاطر السيبرانية واختيار إجراءات المعالجة المناسبة.

AGILE LEADERS
Training Center

اليوم الخامس: تدقيق الاتصالات والمراقبة والإبلاغ

- **الموضوع 1:** تخطيط تدقيق الاتصالات والامتثال القائم على المخاطر
- **الموضوع 2:** اختبار الامتثال، وجمع الأدلة، والتحقق من المشكلات
- **الموضوع 3:** مؤشرات المخاطر الرئيسية، ومقاييس التحكم، وعتبات التحذير
- **الموضوع 4:** مخاطر الأطراف الثالثة، والموردين، والاستعانة بمصادر خارجية، والخدمات السحابية
- **الموضوع 5:** التقارير التنفيذية، وتقارير مجلس الإدارة، والتقارير التنظيمية
- **الموضوع 6:** تطوير خطة لتحسين مخاطر الاتصالات والامتثال
- **تأمل ومراجعة:** تقديم ملف مخاطر موحد وخطة عمل للامتثال.

الأسئلة الشائعة:

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

لا توجد مؤهلات رسمية مطلوبة. يعد الفهم الأساسي لعمليات الاتصالات، والتنظيم، والمخاطر، والامتثال، والتدقيق، والأمن السيبراني، والشؤون القانونية، أو إدارة الشبكات مفيدًا.

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

تستمر جلسة كل يوم بشكل عام حوالي 4-5 ساعات، مع فترات راحة وأنشطة تفاعلية. يمتد إجمالي مدة الدورة على مدار أسبوع، أي ما يقرب من 20-25 ساعة من التدريب.

ما الفرق بين الامتثال التنظيمي للاتصالات وإدارة مخاطر الاتصالات؟

يركز الامتثال التنظيمي للاتصالات على تلبية الالتزامات القانونية، والترخيص، والمنافسة، والخصوصية، والأمن السيبراني، والمستهلك.

تتمتع إدارة مخاطر الاتصالات بنطاق أوسع وتغطي الإخفاقات التشغيلية، وتعطل الشبكة، والحوادث السيبرانية، والاحتيال، وتعرض الموردين، والضرر بالسمعة. تدمج الدورة كلا التخصصين بحيث يتم إدارة التزامات الامتثال من خلال تقييم المخاطر المنظم، والضوابط، والمراقبة، والإبلاغ.

AGILE LEADERS
Training Center

كيف تختلف هذه الدورة عن دورات مخاطر الاتصالات والامتثال التنظيمي الأخرى:

تجمع هذه الدورة بين الامتثال التنظيمي وإدارة المخاطر العملية بدلاً من التعامل معهما كموضوعين منفصلين.

يدرس المشاركون الترخيص، والمنافسة، والربط البيني، والأمن السيبراني، والخصوصية، والاحتيال، ومرونة الشبكة، والتدقيق، واستمرارية الأعمال ضمن برنامج متكامل واحد. يستخدم المحتوى إرشادات ITU الخاصة بالاتصالات لتقييم المخاطر ومعالجتها ومراقبتها وتحسين الضوابط.

تُستخدم إرشادات NIST أيضًا لتعزيز تحديد أولويات مخاطر الأمن السيبراني، والملكية، واختيار الاستجابة، والتقارير التنفيذية.