

رقم الدورة 1941

دورة ضوابط وسياسات وأطر الأمن السيبراني

الأمن السيبراني وأمن المعلومات
تقنية المعلومات والأمن السيبراني

طريقة التقديم

حضور

المدة

5 أيام



نظرة عامة على الدورة

تقدم دورة ضوابط وسياسات وأطر الأمن السيبراني فهماً متكاملاً وعملياً لكيفية قيام المؤسسات بتأسيس وتنفيذ وحوكمة وتطوير ضوابط الأمن السيبراني والسياسات والمعايير وأطر الأمن بصورة مستدامة. وتركز الدورة على تحويل متطلبات الأمن السيبراني إلى ضوابط منظمة وقابلة للقياس تسهم في حماية أصول المعلومات والبيئات التقنية والعمليات المؤسسية والخدمات الحيوية.

يتعرف المشاركون على العلاقة بين حوكمة الأمن السيبراني وإدارة المخاطر والسياسات الأمنية وأطر الضوابط ومتطلبات الامتثال والأمن التشغيلي. كما تتناول الدورة كيفية اختيار أطر الأمن المناسبة وتكييفها مع طبيعة المؤسسة، وتحديد أهداف الضوابط، وتوزيع المسؤوليات، وتوثيق المتطلبات الأمنية، وإنشاء آليات قابلة للقياس لتقييم فعالية الضوابط.

وتغطي الدورة تطوير وتنفيذ السياسات الأمنية في مجالات متعددة تشمل التحكم في الوصول، وأمن الهوية، وحماية البيانات، وإدارة الحوادث، وإدارة الثغرات، وأمن الشبكات، وأمن نقاط النهاية، وأمن الحوسبة السحابية، ومخاطر الأطراف الثالثة، واستمرارية الأعمال، والتوعية الأمنية. كما يتعلم المشاركون كيفية موازنة السياسات والضوابط مع شهية المخاطر والأولويات المؤسسية والمتطلبات الرقابية والبيئات التقنية.

ومن خلال التمارين العملية وورش تطوير السياسات وربط الضوابط بالأطر الأمنية وتحليل الفجوات وتخطيط التنفيذ، يطور المشاركون القدرات اللازمة لبناء بيئة متماسكة لضوابط الأمن السيبراني، وتحديد نقاط الضعف، وترتيب أولويات المعالجة، وتعزيز الجاهزية للتدقيق، وإنشاء نموذج مستدام لحوكمة الأمن السيبراني.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل دور ضوابط الأمن السيبراني والأطر الأمنية في تعزيز المرونة المؤسسية.
- تحديد المكونات الأساسية لهيكل فعال لحوكمة الأمن السيبراني.

- تقييم مخاطر الأمن السيبراني وتحويلها إلى ضوابط أمنية مناسبة.
- تطوير وإدارة سياسات ومعايير وإجراءات وإرشادات الأمن السيبراني.
- ربط الضوابط الأمنية بالمخاطر المؤسسية والمتطلبات الرقابية وأهداف الأعمال.
- تطبيق مبادئ أطر الأمن السيبراني المعترف بها في برامج الأمن المؤسسية.
- تقييم تصميم وفعالية تشغيل ضوابط الأمن السيبراني.
- تنفيذ تقييمات منهجية لفجوات الضوابط الأمنية.
- ترتيب أولويات تطوير الضوابط وفق مستوى المخاطر والأثر المؤسسي.
- تحديد ملكية الضوابط والمسؤوليات وآليات المساءلة والحوكمة.
- تطوير مؤشرات أداء ومؤشرات مخاطر لقياس فعالية الضوابط.
- تعزيز الجاهزية للتدقيق الأمني وإدارة الأدلة والوثائق.
- موازنة السياسات والضوابط الأمنية عبر البيئات السحابية والهجينة والمحلية.
- تعزيز ضوابط الأمن السيبراني الخاصة بالأطراف الثالثة وسلاسل التوريد.
- إعداد خارطة طريق عملية لتطوير ضوابط الأمن السيبراني وحوكمتها.

الفئة المستهدفة

تستهدف الدورة المتخصصين في الأمن السيبراني وأمن المعلومات، ومديري الأمن السيبراني وتقنية المعلومات، ومهندسي الأمن، ومتخصصي الحوكمة، والمخاطر والالتزام، والمدققين الداخليين، والمتخصصين المسؤولين عن تصميم أو تنفيذ أو الإشراف على ضوابط الأمن السيبراني.

كما تناسب العاملين في حوكمة الأمن السيبراني وإدارة مخاطر المؤسسات والامتثال الرقابي والتدقيق وضمان التقنية واستمرارية الأعمال وأمن الحوسبة السحابية وحماية البنية التحتية والمعلومات.

وتكتسب الدورة أهمية خاصة للمديرين وصناع القرار المسؤولين عن بناء هياكل حوكمة الأمن السيبراني، ورفع

مستوى نضج الضوابط، والاستعداد للتدقيق والتقييمات الأمنية، ومواءمة برامج الأمن السيبراني مع المخاطر المؤسسية والأهداف الاستراتيجية.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- شرح أهداف وهيكل ضوابط الأمن السيبراني والأطر الأمنية.
- التمييز بين السياسات والمعايير والإجراءات والإرشادات والضوابط الأمنية.
- تطوير هيكل متكامل للسياسات الأمنية داخل المؤسسة.
- تحديد وتوثيق أهداف ضوابط الأمن السيبراني.
- ربط مخاطر الأمن السيبراني بالضوابط الوقائية والكاشفة والتصحيحية المناسبة.
- تقييم فعالية ونضج ضوابط الأمن السيبراني القائمة.
- تنفيذ تقييمات فجوات الضوابط والأطر الأمنية.
- إعداد مصفوفات للضوابط والحفاظ على إمكانية تتبع العلاقة بين المخاطر والمتطلبات والضوابط.
- تحديد ملكية الضوابط والمسؤوليات والمساءلة بين الإدارات التقنية والتشغيلية.
- تطوير مؤشرات أداء ومؤشرات مخاطر وتقارير إدارية للأمن السيبراني.
- إعداد الأدلة والوثائق المناسبة لعمليات التدقيق والتقييم الأمني.
- مواءمة الضوابط الأمنية عبر البيئات السحابية والهجينة والتقليدية.
- تحديد نقاط الضعف في ضوابط أمن الأطراف الثالثة وسلاسل التوريد.
- إنشاء آليات للمراقبة المستمرة والتحسين المستمر.
- إعداد خارطة طريق ذات أولويات لتنفيذ وتطوير ضوابط الأمن السيبراني.

■ المحاوّر التدريبيّة

محاوّر الدورة

اليوم الأول

حوكمة الأمن السيبراني والضوابط والأطر الأمنية

- مفهوم حوكمة الأمن السيبراني ودورها المؤسسي.
- العلاقة بين مخاطر الأمن السيبراني والحوكمة والامتثال والضوابط.
- مفهوم الضوابط الأمنية وأهدافها.
- الضوابط الوقائية والكاشفة والتصحيحية والتعويضية.
- السياسات والمعايير والإجراءات والإرشادات الأمنية.
- أطر الأمن السيبراني ودورها في بناء البرامج الأمنية المؤسسية.
- اختيار الإطار الأمني المناسب ومواءمته مع احتياجات المؤسسة.
- هياكل الحوكمة الأمنية وتوزيع المسؤوليات.
- ملكية الضوابط ونماذج المسؤولية والمساءلة.
- تقييم نضج الأمن السيبراني وبيئة الضوابط.
- التطبيق العملي: تقييم هيكل حوكمة الأمن السيبراني في مؤسسة افتراضية وتحديد أهم فجوات الضوابط والمسؤوليات.

اليوم الثاني

السياسات والمعايير الأمنية وتصميم الضوابط

- مبادئ تطوير السياسات الأمنية الفعالة.
- بناء الهيكل المتكامل للسياسات الأمنية.

اليوم الثاني — تابع

- تحديد نطاق السياسة وملكيته ومسؤولياتها وآليات تطبيقها.
- سياسات أمن المعلومات والاستخدام المقبول للموارد التقنية.
- سياسات الهوية والتحكم في الوصول والمصادقة.
- سياسات حماية البيانات وتصنيف المعلومات.
- سياسات أمن الشبكات ونقاط النهاية والبنية التحتية.
- سياسات إدارة الثغرات والتحديات الأمنية.
- سياسات الاستجابة للحوادث وإدارة الأحداث الأمنية.
- سياسات أمن الحوسبة السحابية والعمل عن بُعد.
- متطلبات الأمن السيرياني للأطراف الثالثة والموردين.
- الاستثناءات الأمنية والموافقات والمراجعة الدورية للسياسات.
- التطبيق العملي: تطوير هيكل متكامل لسياسات الأمن السيرياني وإعداد متطلبات لعدد من السياسات الأمنية الأساسية لمؤسسة افتراضية.

اليوم الثالث

ربط الأطر الأمنية وتقييم المخاطر والضوابط

- فهم هيكل أطر الأمن السيرياني ومكوناتها.
- ربط مخاطر الأعمال والأمن السيرياني بالضوابط المناسبة.
- تحديد وتصنيف الضوابط الأمنية.
- إعداد مصفوفات ضوابط الأمن السيرياني.
- ربط المتطلبات والضوابط بين الأطر الأمنية المختلفة.
- تحديد الضوابط المتكررة أو المتداخلة.
- تقييم تصميم الضوابط الأمنية.

اليوم الثالث — تابع

- تقييم فعالية تشغيل الضوابط.
- منهجيات اختبار الضوابط الأمنية.
- جمع الأدلة وتوثيق نتائج الاختبارات.
- تحليل فجوات الأمن السيرياني.
- ترتيب أولويات معالجة نقاط الضعف وفق المخاطر.
- التطبيق العملي: إعداد مصفوفة للضوابط الأمنية وربط المخاطر المحددة بالضوابط المناسبة وتنفيذ تقييم منهجي لفجوات الضوابط.

اليوم الرابع

تنفيذ الضوابط والامتثال والعمليات الأمنية

- تنفيذ ضوابط الأمن السيرياني عبر بيئات المؤسسة.
- ضوابط أمن الهوية وإدارة الوصول.
- ضوابط الوصول المميز والمصادقة.
- ضوابط أمن الشبكات والبنية التحتية.
- ضوابط حماية نقاط النهاية وإدارة الثغرات.
- ضوابط حماية البيانات والتشفير.
- ضوابط المراقبة الأمنية وتسجيل الأحداث.
- ضوابط اكتشاف الحوادث والاستجابة لها.
- ضوابط أمن البيئات السحابية والهجينة.
- ضوابط أمن الأطراف الثالثة وسلاسل التوريد.
- ضوابط استمرارية الأعمال والتعافي من الكوارث.
- مراقبة الامتثال والاستعداد للتدقيق.

اليوم الرابع — تابع

- إدارة أوجه القصور وخطط المعالجة والتصحيح.
- التطبيق العملي: تقييم بيئة ضوابط أمن سيرياني افتراضية وإعداد خطة معالجة قائمة على المخاطر لنقاط الضعف المكتشفة.

اليوم الخامس

حوكمة الضوابط والقياس والتحسين المستمر

- بناء نموذج مستدام لحوكمة ضوابط الأمن السيرياني.
- إدارة دورة حياة الضوابط الأمنية.
- المراجعة الدورية وإعادة تقييم الضوابط.
- المراقبة المستمرة لفعالية الضوابط.
- مؤشرات أداء الأمن السيرياني ومؤشرات المخاطر.
- قياس فعالية الضوابط ومستوى النضج.
- إعداد لوحات المتابعة والتقارير التنفيذية.
- الاستعداد للتدقيق الأمني وإدارة الأدلة.
- متابعة خطط المعالجة والإجراءات التصحيحية.
- إدارة الاستثناءات المتعلقة بالسياسات والضوابط.
- دمج الضوابط الأمنية مع إدارة مخاطر المؤسسة.
- إعداد خارطة طريق لتطوير وتحول برنامج الأمن السيرياني.
- إنشاء آليات للتحسين المستمر.
- الورشة الختامية: إعداد برنامج متكامل لضوابط وسياسات وأطر الأمن السيرياني يشمل الحوكمة، وهيكل السياسات، وأهداف الضوابط، ومواءمة الأطر الأمنية، وتقييم المخاطر، واختبار الضوابط، وتحليل الفجوات، والامتثال، وقياس الأداء، والمعالجة، والمراقبة المستمرة، وخارطة طريق تنفيذية ذات أولويات.



للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

<https://quest-training.com/courses/cybersecurity-controls-policies-security-frameworks-training-course>

الموقع الإلكتروني: <https://quest-training.com>

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440

