QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1084

الأمن السيبراني والمخاطر الرقمية للمصارف

الخدمات المصرفية الرقمية والتقنيات المالية والذكاء الاصطناعي
التمويل والاستثمار والخدمات المصرفية

المدة
5 ايام

طريقة التقديم
حضوري

شركة كويست ترينينج

quest-training.com

نظرة عامة على الدورة

تُعد دورة الأمن السيبراني والمخاطر الرقمية للمصارف من البرامج التدريبية المتقدمة التي تهدف إلى تزويد القيادات المصرفية، والمتخصصين في الأمن السيبراني، وإدارة المخاطر، وتقنية المعلومات، والامتثال، والمهنيين الماليين بالمعرفة الاستراتيجية والمهارات العملية اللازمة لحماية المؤسسات المالية من التهديدات السيبرانية والمخاطر الرقمية المتزايدة. ومع تسارع التحول الرقمي واعتماد البنوك على الخدمات الإلكترونية، والحوسبة السحابية، والذكاء الاصطناعي، والخدمات المصرفية الرقمية، أصبحت إدارة الأمن السيبراني والمخاطر الرقمية من الركائز الأساسية لاستمرارية الأعمال، وحماية الأصول، وتعزيز ثقة العملاء.

يركز البرنامج على تزويد المشاركين بفهم شامل لمبادئ الأمن السيبراني في القطاع المصرفي، وإدارة المخاطر الرقمية، وأطر الأمن السيبراني، وإدارة الهوية والوصول، وأمن الشبكات، وحماية البيانات، والأمن السحابي، والاستجابة للحوادث، واستمرارية الأعمال، والتعافي من الكوارث، واستخبارات التهديدات السيبرانية، وإدارة مخاطر الأطراف الثالثة، إضافة إلى أفضل الممارسات الدولية في حماية المؤسسات المالية من الهجمات الإلكترونية والجرائم السيبرانية.

كما يستعرض البرنامج العلاقة بين الأمن السيبراني والمخاطر الرقمية وبين التحول الرقمي المصرفي، والتقنيات المالية)FinTech(، والصيرفة المفتوحة، والخدمات المصرفية الرقمية، وإدارة المخاطر المؤسسية، والامتثال التنظيمي، ومكافحة غسل الأموال، وحوكمة البيانات، وإدارة المخاطر التشغيلية، وحماية الخصوصية، واستراتيجيات المرونة المؤسسية. وسيكتسب المشاركون مهارات عملية في تقييم المخاطر السيبرانية، وتصميم الضوابط الأمنية، وتحليل الثغرات، وإدارة الأزمات السيبرانية، ووضع استراتيجيات متكاملة لحماية البنية التحتية الرقمية للمؤسسات المالية.

ومن خلال ورش العمل التطبيقية، ودراسات الحالة، وتمارين محاكاة الهجمات الإلكترونية، وتحليل سيناريوهات واقعية من القطاع المصرفي، سيتمكن المشاركون من تطوير قدراتهم على تعزيز الأمن السيبراني، وتقليل المخاطر الرقمية، ورفع جاهزية المؤسسة للاستجابة للحوادث، وتحسين الامتثال، ودعم مبادرات التحول الرقمي بطريقة آمنة ومستدامة. وبنهاية البرنامج سيكون المشاركون قادرين على إعداد استراتيجيات متكاملة للأمن السيبراني وإدارة المخاطر الرقمية تعزز المرونة المؤسسية وتحافظ على استمرارية الأعمال.

أهداف الدورة

- تحليل مفاهيم الأمن السيبراني والمخاطر الرقمية وتقييم تأثيرها على العمليات المصرفية والأداء المؤسسي بنهاية البرنامج.
- تطوير استراتيجيات شاملة لإدارة الأمن السيبراني والمخاطر الرقمية في المؤسسات المصرفية.
- تقييم التهديدات السيبرانية والثغرات الأمنية والمخاطر الرقمية باستخدام منهجيات معتمدة.
- تطبيق أفضل الممارسات لحماية البنية التحتية الرقمية والأنظمة المصرفية والبيانات الحساسة.
- تصميم ضوابط أمنية وإجراءات وقائية تدعم استمرارية الأعمال والمرونة المؤسسية.
- تحسين عمليات اكتشاف التهديدات والاستجابة للحوادث وإدارة الأزمات السيبرانية.
- تعزيز الحوكمة من خلال تطبيق متطلبات الامتثال، وإدارة المخاطر، وحماية البيانات، والخصوصية.
- تنفيذ مؤشرات الأداء الرئيسية)KPIs(ومؤشرات قياس نضج الأمن السيبراني وإدارة المخاطر الرقمية.
- تقييم أثر التقنيات الحديثة مثل الحوسبة السحابية، والذكاء الاصطناعي، والخدمات المصرفية الرقمية على الأمن السيبراني.
- مواءمة استراتيجيات الأمن السيبراني مع أهداف المؤسسة، والتحول الرقمي، والامتثال التنظيمي، والنمو المؤسسي المستدام.
- الفئات المستهدفة:
- تستهدف هذه الدورة القيادات التنفيذية في البنوك، ومديري الأمن السيبراني، ومديري تقنية المعلومات، ومديري التحول الرقمي، ومديري المخاطر، ومديري العمليات المصرفية، ومديري استمرارية الأعمال، ومسؤولي الامتثال، ومتخصصي مكافحة غسل الأموال، ومديري الأمن المعلوماتي، ومديري البنية التحتية التقنية، ومديري المشاريع، ومديري الخدمات الرقمية، والمراجعين الداخليين، وجميع المهنيين المسؤولين عن حماية الأنظمة والبيانات في المؤسسات المالية.
- كما تناسب العاملين في البنوك المركزية، والجهات الرقابية، والمؤسسات المالية الحكومية، وشركات التقنية المالية)FinTech(، وشركات الأمن السيبراني، والاستشاريين، ومهندسي الحلول التقنية، ومتخصصي إدارة

المخاطر، ومديري الاستراتيجية، وصناع القرار المسؤولين عن الأمن الرقمي، والامتثال، والتحول الرقمي، واستمرارية الأعمال، والابتكار في القطاع المالي.

الفئة المستهدفة

This course is designed for banking executives, Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), cybersecurity managers, information security professionals, IT managers, digital transformation managers, banking operations managers, risk managers, compliance officers, AML professionals, business continuity managers, internal auditors, infrastructure specialists, security analysts, project managers, and professionals responsible for cybersecurity and digital risk management within financial institutions.

The program is equally valuable for central bank professionals, financial regulators, government financial institution leaders, FinTech professionals, cybersecurity consultants, technology architects, cloud security specialists, data governance professionals, operational risk specialists, legal and regulatory professionals, and decision-makers responsible for digital resilience, regulatory compliance, secure digital transformation, and technology governance across the financial sector.

مخرجات التعلم

- بنهاية البرنامج سيكون المشارك قادرًا على:
- تطوير استراتيجية متكاملة للأمن السيبراني وإدارة المخاطر الرقمية في المؤسسات المصرفية.
- تقييم المخاطر السيبرانية والثغرات الأمنية ووضع خطط فعالة لمعالجتها.
- تطبيق ضوابط أمنية لحماية الأنظمة المصرفية والبنية التحتية الرقمية.
- تصميم خطط للاستجابة للحوادث السيبرانية واستمرارية الأعمال والتعافي من الكوارث.

- تقييم المخاطر المرتبطة بالحوسبة السحابية، والخدمات الرقمية، والأطراف الثالثة.
- تعزيز الامتثال التنظيمي من خلال تطبيق أفضل ممارسات الأمن السيبراني وحوكمة البيانات.
- إعداد لوحات مؤشرات تنفيذية لقياس أداء الأمن السيبراني ومستوى المخاطر الرقمية.
- دمج الأمن السيبراني مع برامج التحول الرقمي وإدارة المخاطر المؤسسية.
- تقييم أثر التقنيات الناشئة على المخاطر الرقمية واستراتيجيات الحماية.
- إعداد خارطة طريق عملية لتعزيز الأمن السيبراني، وتقليل المخاطر الرقمية، وتحسين المرونة المؤسسية، ودعم النمو المستدام للمؤسسة المالية.

محاور الدورة

المحتوى التدريبي:

اليوم الأول

أساسيات الأمن السيبراني في القطاع المصرفي

- تطور التهديدات السيبرانية في القطاع المالي.
- مبادئ الأمن السيبراني وأطر العمل العالمية.
- البنية التحتية الرقمية للمؤسسات المصرفية.
- الحوكمة وإدارة الأمن السيبراني.
- تطبيق عملي: تقييم الوضع الحالي للأمن السيبراني في المؤسسة.

اليوم الثاني

إدارة المخاطر الرقمية وحماية الأصول

- منهجيات تقييم المخاطر الرقمية.
- إدارة الهوية والوصول.
- حماية البيانات والخصوصية.
- أمن الشبكات والبنية التحتية التقنية.
- تطبيق عملي: تحليل المخاطر الرقمية ووضع الضوابط المناسبة.

اليوم الثالث

حماية العمليات المصرفية الرقمية

- أمن الخدمات المصرفية الرقمية والقنوات الإلكترونية.
- الحوسبة السحابية وإدارة مخاطرها.
- أمن الأطراف الثالثة وسلسلة التوريد الرقمية.
- استخبارات التهديدات السيبرانية.
- تطبيق عملي: تصميم ضوابط أمنية لحماية العمليات المصرفية.

اليوم الرابع

الاستجابة للحوادث والامتثال

- إدارة الحوادث السيبرانية والاستجابة لها.
- استمرارية الأعمال والتعافي من الكوارث.
- المتطلبات التنظيمية والامتثال في الأمن السيبراني.
- قياس الأداء باستخدام مؤشرات الأمن السيبراني وإدارة المخاطر.

اليوم الرابع — تابع

- تطبيق عملي: إعداد خطة استجابة لحادث سيبراني.

اليوم الخامس

بناء مؤسسة مصرفية رقمية آمنة

- إعداد استراتيجية مؤسسية للأمن السيبراني.
- إدارة التغيير وتعزيز ثقافة الأمن السيبراني.
- الاتجاهات المستقبلية في الأمن السيبراني والتقنيات الرقمية.
- التحسين المستمر والمرونة المؤسسية.
- الورشة الختامية: إعداد خارطة طريق متكاملة للأمن السيبراني وإدارة المخاطر الرقمية، تشمل استراتيجية الحماية، وإدارة المخاطر، وحوكمة الأمن، والامتثال التنظيمي، وحماية البيانات، وإدارة الهوية، واستمرارية الأعمال، والاستجابة للحوادث، وقياس الأداء، وإدارة التغيير، بما يعزز المرونة المؤسسية، ويحمي الأصول الرقمية، ويدعم التحول الرقمي الآمن، ويضمن النمو المستدام للمؤسسة المالية.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: https://quest-training.com/courses/cybersecurity-digital-risk-for-banks

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440