SKILLSLAB
Training Provider

كتيب الدورة

الأمن السيبراني وإدارة المخاطر والامتثال– متقدمة للحوكمة وحماية المعلومات حوكمة والالتزام التنظيمي استراتيجيات

Professional Training Course

Skillslab Training Provider
Skills for Tomorrow's World

info@skillslab-training.com | +966 55 965 3447 | www.skillslab-training.com

وصف الدورة

المقدمة

التنظيمية وتوقعات أصحاب متزايدة الترابط والتعقيد تتطور فيها التهديدات تعمل المؤسسات في بيئات رقمية وإدارة المخاطر والامتثال ضرورية لحماية المصلحة بصورة مستمرة. وتُعد ممارسات حوكمة الأمن السيبرانية والمتطلبات الثقة المؤسسية. ويتطلب تحقيق هذه الأهداف إنشاء المعلومات الحساسة وضمان استمرارية الأعمال وتعزيز السيبراني التدريبي المبادئ وإثبات الالتزام بالقوانين والمعايير المهنية هياكل واضحة للمساءلة وتطبيق ضوابط أمنية مناسبة الأمن السيبراني وإدارة المخاطر والأطر والأدوات العملية اللازمة لبناء منظومة المعمول بها. يقدم هذا البرنامج المؤسسية وإدارة أمن المعلومات وإدارة المخاطر والامتثال. كما يستعرض العلاقة بين الحوكمة متكاملة لحوكمة فعالية الضوابط على أساليب تحديد المخاطر السيبرانية وتقييم الشاملة والاستراتيجية التنظيمية. ويتعرف المشاركون والتدقيق الداخلي وضمان أمن الأطراف الأمنية. ويتناول البرنامج تطوير السياسات ومراقبة الالتزامات التنظيمية وقياس متابعة الأداء التطبيقات العملية كيفية إعداد أطر الحوكمة وسجلات الخارجية وإعداد التقارير الإدارية. وتوضح الامتثال قدراتهم على دعم اتخاذ الأمني. ومن خلال التعلم المنظم ودراسات الحالة المخاطر ومصفوفات الامتثال ولوحات أهداف القرارات المبنية على المخاطر وتعزيز التحسين التطبيقية يطور المشاركون

سيتمكن المشاركون من تحقيق المستمر في حوكمة الأمن السيبراني.

فهم مبادئ حوكمة الأمن الأهداف التالية بنهاية هذه الدورة الدورة التدريبية

- مواءمة استراتيجيات السيبراني وإدارة المخاطر والامتثال وأهميتها في التدريبية:
- الأطر والمعايير والالتزامات التنظيمية وإدارة المخاطر الحوكمة السيبرانية مع الأهداف المؤسسية حماية المؤسسات.

تطبيق

- إنشاء هياكل الدولية المعترف بها في حوكمة الأمن السيبراني الشاملة.
- تحديد فعالة للحوكمة السيبرانية وتطوير السياسات وتحديد وإدارة أمن المعلومات.
- سيبراني وإدارتها باستخدام منهجيات المخاطر السيبرانية وتقييمها وترتيب أولوياتها المسؤوليات وآليات المساءلة.

تطوير برامج امتثال

- تقييم ضوابط أمن تتوافق مع القوانين واللوائح والمعايير المهنية منظمة.
- تعزيز إدارة مخاطر المعلومات وقياس فعاليتها في الحد من المخاطر المعمول بها.

- تصميم لوحات الأطراف الخارجية وضمان أمن الموردين والامتثال المؤسسية.
- تطبيق متابعة الحوكمة السيبرانية وتقارير الامتثال للالتزامات التعاقدية.
- لممارسات الحوكمة وإدارة المخاطر المراقبة المستمرة والتدقيق الداخلي والتحسين ومؤشرات قياس الأداء.

الفئة المنهجي

يستهدف هذا البرنامج التدريبي والامتثال.

مديرو الأمن السيبراني المهنيين الراغبين في تطوير معارفهم المستهدفة

- مسؤولو أمن المعلومات واستراتيجيات الحماية المسؤولون عن تطوير أطر الحوكمة الأمنية ومهاراتهم:
- متخصصو المشرفون على السياسات الأمنية ومتطلبات الامتثال المؤسسية.
- المؤسسية الالتزامات التنظيمية والضوابط الحوكمة والمخاطر والامتثال المسؤولون عن وإدارة المخاطر السيبرانية.

مديرو المخاطر

- المدققون الداخليون المعنيون بتقييم التهديدات الرقمية ودمجها ضمن أطر الأمنية.
- مديرو المسؤولون عن تقييم فعالية الحوكمة السيبرانية إدارة المخاطر.
- مسؤولو الشؤون تقنية المعلومات المعنيون بمواءمة أمن الأنظمة مع والضوابط والامتثال التنظيمي.
- مديرو القانونية والامتثال التنظيمي المرتبطون بأمن الأهداف المؤسسية.
- القيادات استمرارية الأعمال المسؤولون عن المرونة السيبرانية المعلومات وحماية البيانات.
- المتخصصون المخاطر السيبرانية والقرارات التنفيذية وأعضاء مجالس الإدارة المشرفون على وإدارة المخاطر التشغيلية.

المستشارون

- المحتوى في تطوير نضج الحوكمة الأمنية وتحسين الامتثال الاستراتيجية.

فهم مفاهيم حوكمة السيبراني والمواءمة التدريبياليوم الأول: أساسيات حوكمة الأمن المؤسسي.

- استعراض الأهمية الأمن السيبراني وإدارة المخاطر والامتثال الاستراتيجية
- التعرف على الأطر الاستراتيجية لأطر الحوكمة السيبرانية المؤسسي.
- فهم مسؤوليات مجالس والمعايير الدولية لحوكمة الأمن السيبراني وإدارة المتكاملة.
- مواءمة أهداف الأمن الإدارة والإشراف التنفيذي والقيادة أمن المعلومات.
- تحديد شهية المخاطر السيبراني مع الاستراتيجية المؤسسية وأولويات الأمنية.
- إنشاء لجان الحوكمة السيبرانية ومستويات تحملها ومبادئ الأعمال.
- تطوير سياسات أمن المعلومات الأمنية وهياكل التقارير وصلاحيات اتخاذ الحوكمة.
- دمج الحوكمة السيبرانية مع والمعايير والإجراءات ووثائق القرار.

- تمرين عملي لتصميم هيكل إدارة المخاطر الشاملة والحوكمة الحوكمة.
- اليوم الثاني: تقييم حوكمة الأمن السيبراني داخل مؤسسة المؤسسية.

تحديد التهديدات المخاطر السيبرانية ودمجها ضمن إدارة المخاطر افتراضية.

- فهم منهجيات تقييم المخاطر السيبرانية والثغرات الأمنية والأصول المعلوماتية المؤسسية
- تقييم الحيوية.
- إعداد سجلات احتمالية المخاطر السيبرانية وتأثيراتها ومستويات السيبرانية ومعايير قياسها.
- تطبيق أساليب التقييم المخاطر وتطوير أنظمة تصنيف المخاطر التعرض المؤسسي.
- تحديد مالكي المخاطر النوعي والكمي للمخاطر السيبرانية.
- تقييم خيارات معالجة ومسؤوليات المعالجة وإجراءات الإلكترونية.
- دمج المخاطر السيبرانية المخاطر السيبرانية وتحديد أولويات الضوابط التصعيد.
- تقييم مخاطر التقنيات ضمن عمليات إدارة المخاطر المؤسسية الأمنية.
- ورشة تطبيقية لإجراء تقييم الناشئة وتحديات التحول الشاملة.
- اليوم الثالث: أطر متكامل للمخاطر السيبرانية وإعداد خطط الرقمي.

فهم البيئات التنظيمية الامتثال السيبراني والمتطلبات التنظيمية المعالجة.

- استعراض معايير إدارة للأمن السيبراني والالتزامات المؤسسية المتعلقة والتشريعية
- تحديد المتطلبات أمن المعلومات وأطر الامتثال بالامتثال.
- تطوير سياسات الامتثال القانونية والتعاقدية والتنظيمية الخاصة بأمن السيبراني.
- إنشاء إجراءات مراقبة السيبراني وسجلات الالتزامات المعلومات.
- تقييم متطلبات حماية الامتثال والتحقق من تطبيق الضوابط التنظيمية.
- إدارة التزامات الامتثال البيانات والخصوصية والتعامل الآمن مع الأمنية.
- إعداد تقييمات الامتثال للأطراف الخارجية وضمان أمن المعلومات.
- تحديد فجوات الامتثال التنظيمي والوثائق والأدلة الموردين.
- تمرين عملي لإعداد وتطوير خطط الإجراءات الداعمة.
- اليوم الرابع: الضوابط مصفوفة الامتثال السيبراني وخطة معالجة التصحيحية.

فهم أهداف الضوابط الأمنية والتدقيق الداخلي وضمان أمن الأطراف الفجوات.

- تصميم أطر الضوابط الأمنية السيبرانية وآليات اختيارها وفقاً الخارجية

- تقييم للمخاطر.
- إعداد خطط التدقيق تصميم الضوابط الأمنية وفعاليتها الإدارية والتقنية والمادية.
- تنفيذ اختبارات الضوابط الداخلي للأمن السيبراني ومعايير التشغيلية.
- تحديد أوجه القصور في وجمع الأدلة وتوثيق نتائج التقييم.
- إعداد نتائج التدقيق والتوصيات الضوابط وتقييم المخاطر المرتبطة التدقيق.
- تقييم مخاطر الموردين وخطط الإجراءات الإدارية بها.
- متابعة أنشطة المعالجة والأطراف الخارجية وفعالية ضوابطهم التصحيحية.
- ورشة تطبيقية لإجراء والتحقق من تنفيذ الإجراءات الأمنية.
- اليوم الخامس: التقارير تقييم للضوابط السيبرانية ومراجعة نتائج التدقيق التصحيحية.

إنشاء عمليات مراقبة السيبرانية ومراقبة الأداء والتحسين المستمر الأمني.

- تطوير مؤشرات المخاطر الحوكمة السيبرانية وإعداد تقارير للحوكمة
- تصميم لوحات متابعة الرئيسية ومقاييس أداء الحوكمة الامتثال.
- إعداد تقارير الأمن تنفيذية للإشراف على المخاطر والامتثال الأمنية.
- مراقبة التغيرات السيبراني لمجالس الإدارة والتوصيات السيبراني.
- تقييم مستوى نضج الحوكمة التنظيمية والمتطلبات الناشئة لحوكمة الأمن الإدارية.
- تعزيز الإشراف على السيبرانية وفعالية الضوابط السيبراني.
- تطوير استراتيجيات الحوادث الأمنية والمساءلة وإجراءات الإبلاغ المؤسسية.
- إعداد خرائط طريق لحوكمة التحسين المستمر لبرامج الحوكمة التنظيمي.
- تمرين ختامي لإعداد وعرض الأمن السيبراني وتحديد أولويات والامتثال.
- مدة الدورة استراتيجية متكاملة للحوكمة السيبرانية وإدارة التنفيذ.

يُنفذ هذا البرنامج التدريبي على المخاطر والامتثال.

يومياً، وبإجمالي خمس وعشرين ساعة تدريبية. يجمع مدار خمسة أيام متتالية، بواقع خمس ساعات تدريبية التدريبية حالات الامتثال ومحاكاة التطبيقية والمناقشات الجماعية وتمارين تقييم البرنامج بين المحاضرات التفاعلية وورش العمل الحوكمة وسجلات المخاطر مواقف الحوكمة المؤسسية. ويعمل المشاركون على إعداد المخاطر السيبرانية ودراسات الداخلي ولوحات التقارير التنفيذية. ويمكن السيبرانية ومصفوفات الامتثال وقوائم التحقق وثائق عملية تشمل هياكل معلومات تدريبية داخلية مخصصة وفقاً لاحتياجات المؤسسات تقديم البرنامج حضورياً أو عن بُعد أو ضمن برامج للتدقيق

يقدم البرنامج خبير معتمد دولياً ومستويات الخبرة المهنية للمشاركين.

خبرة السيبراني وإدارة أمن المعلومات وإدارة المخاطر يتمتع بخبرة عملية واستشارية واسعة في حوكمة الأمن المدرب والتدقيق الداخلي وتقييم تطبيقية في أطر الحوكمة السيبرانية والمعايير المؤسسية والامتثال التنظيمي. يمتلك المدرب ويركز أسلوب التدريب على الممارسات المخاطر ومراقبة الامتثال وتطوير مستويات الأمن الدولية لأمن المعلومات بفاعلية داخل الواقعية والتمارين التطبيقية بما يضمن قدرة المهنية المعترف بها دولياً ودراسات الحالة المؤسسي. الأسئلة المشاركين على توظيف المعارف المكتسبة

ما الهدف الرئيسي من دورة مؤسساتهم.

1. تهدف الدورة إلى تطوير القدرات العملية لإنشاء أطر حوكمة الأمن السيبراني وإدارة المخاطر والامتثال؟ الشائعة هل الدورة مناسبة الالتزام بالمتطلبات التنظيمية الحوكمة السيبرانية وإدارة المخاطر الرقمية وضمان
2. دون الأمن السيبراني؟ نعم، يركز البرنامج على الحوكمة للمهنيين الذين لا يمتلكون خبرة تقنية متقدمة في والتشريعية. ما المعايير والأطر اشتراط خبرة متقدمة في العمليات وإدارة المخاطر والامتثال والإشراف الأمني
3. عن المعهد معايير إدارة أمن المعلومات وإدارة مخاطر أمن الدولية التي يتناولها البرنامج؟ يستعرض البرنامج التقنية. هل تتضمن الوطني الأمريكي للمعايير والتكنولوجيا ومبادئ المعلومات وإطار الأمن السيبراني الصادر
4. إعداد سجلات المخاطر السيبرانية الدورة تطبيقات عملية في الحوكمة والامتثال؟ نعم، حوكمة تقنية المعلومات. ما ومصفوفات الامتثال وهياكل الحوكمة وقوائم التدقيق تشمل التطبيقات
5. التدريبي؟ يناسب البرنامج الجهات الحكومية المؤسسات التي يمكن أن تستفيد من هذا البرنامج وأطر التقارير الإدارية. تمثل التقنية والمؤسسات الخاضعة للمتطلبات والمؤسسات المالية وشركات الطاقة ومزودي الخدمات

الخاتمة

المعقدة. ركائز أساسية لحماية الأصول المعلوماتية وتعزيز حوكمة الأمن السيبراني وإدارة المخاطر والامتثال التنظيمية.

أطر الحوكمة وتقييم يوفر هذا البرنامج التدريبي منهجيات منظمة وأدوات المساءلة المؤسسية في البيئات الرقمية

ويطور المشاركون قدراتهم على إعداد المخاطر السيبرانية وتعزيز الالتزام بالمتطلبات عملية تساعد المهنيين على تطوير

مخاطر الأطراف الخارجية والتواصل بشأن التهديدات مع السياسات الأمنية وتقييم فعالية الضوابط وإدارة التنظيمية.

الأمن السيبراني. ومن الداخلي ومراقبة الأداء والتحسين المستمر اللازمة الإدارة العليا. كما يعزز البرنامج مهارات التدقيق

التشغيلية وتحسين جاهزيتها خلال تطبيق المعارف والتقنيات المكتسبة تستطيع لبناء منظومة مستدامة لحوكمة

المبنية على المخاطر. التنظيمية ودعم اتخاذ القرارات الاستراتيجية المؤسسات تعزيز مرونتها

تواصل معنا

الأسعار الجماعية، يُرجى التواصل معنا: للاستفسار عن التسجيل أو المواعيد القادمة أو

الموقع الإلكتروني www.skillslab-training.com

البريد الإلكتروني info@skillslab-training.com

واتساب +966 559 653 447

Generated by Skillslab Training

info@skillslab-training.com | واتساب: +966 559 653 447

www.skillslab-training.com