

شهادة في مجال تخطيط التعافي من كوارث تكنولوجيا المعلومات

المقدمة

تزود هذه الدورة المشاركين بحلول ملموسة واستراتيجيات ورؤى لتقديم خطة فعالة للبنية التحتية لتكنولوجيا المعلومات وخطة تعافي من الكوارث التكنولوجية بهدف وضع تدابير مرنة لحماية قسم تكنولوجيا المعلومات قى مؤسساتهم. باستخدام عمليات وإجراءات مجربة، سيقوم المشاركون بتحليل المخاطر وتأثيرها على عمليات تكنولوجيا المعلومات التي قد تهددها. كما توفر هذه الدورة إطاراً لبناء القدرة التشغيلية لتقديم استجابة فعالة لحماية مصالح تكنولوجيا المنظمات وأنشطة تضيف القيمة.

هذه الدورة العملية تزود المشاركين باطار يشمل ISO 27031 ، ISO 20000 ، ISO 22301 ITIL التي تتماشى مع المبادئ التوجيهية لمعهد استمرارية الأعمال

المنهجية

إن هذه الدورة على درجة عالية من التفاعلية وتتضمن مناقشات جماعية واستخدام أشرطة الفيديو ودراسات الحالة والتمارين. ويتم تطبيق خلال وبعد الدورة استخدام وسيلة تقييم المخاطر و BIA و نماذج DR للتخطيط ذات التكنولوجيا العالية. كما يتم توفير المعلومات الداعمة، مثل شروط اللجنة التوجيهية المرجعية (TOR) وإدارة التغيير واستراتيجية اختبار DR وعمليات الفحص. تشمل هذه الدورة أيضاً نماذج محددة للتنفيذ التدريجي لتحليل التأثير على العمل (BIA) ، وكذلك الانتهاء من خطة تكنولوجيا المعلومات (DRP) التي يطبقها المشاركون في مؤسساتهم.

أهداف الدورة

سيتمكن المشاركون في نهاية الدورة من:

- الأخذ بعين الاعتبار السياسات والأهداف والغايات والعمليات والإجراءات ذات الصلة بإدارة المخاطر وتحسين تكنولوجيا المعلومات لاستمرارية الأعمال (IRBC)
- تطبيق أفضل الممارسات لبناء البنية التحتية لتكنولوجيا المعلومات والاستدامة التشغيلية، لتوفير البيئة الامنة
- وصف العمليات والإجراءات لتقييم المخاطر وتحديد التهديدات ونقاط الضعف التي يمكن أن تؤثر على المؤسسة
- مراجعة العناصر الرئيسية للأصول والموارد البشرية والتغيير وإدارة سلسلة التوريد المعنية بتكنولوجيا المعلومات
- مناقشة العناصر الرئيسية لبرامج التعافي من كوارث تكنولوجيا المعلومات (DR) ، بما في ذلك إدارة البيانات والعناصر الأساسية اللازمة لتحليل أثر الأعمال (BIA)
- تقدير فترة التعطيل القصوى المسموحة (MTPD) ، ثم تحديد العلاقة بالوقت المستهدف لاسترداد البيانات (RTO) ونقطة الاسترجاع المستهدفة (RPO)
- إنتاج برامج عالية المستوى للتعافي من كوارث تكنولوجيا المعلومات

الفئات المستهدفة

- مدراء تقنية المعلومات والمهنيون، بما في ذلك مدراء التعافي من كوارث تكنولوجيا المعلومات (DR) أو أي شخص مسؤول عن خطط التعافي من الكوارث (DRP) وعن خطط استمرارية الأعمال التجارية (BCP) وعن تقنيات وتدقيق تكنولوجيا المعلومات.
- الكفاءات المستهدفة

- التأكد من جاهزية قسم تكنولوجيا المعلومات لاستمرارية الأعمال
- اجراء تقييم المخاطر
- اجراء تحليل أثرالأعمال
- ادارة الحوادث والتغيير
- تخطيط التعافي من كوارث تكنولوجيا المعلومات
- فحص التعافي من كوارث تكنولوجيا المعلومات
- أنا أتحدث الإنجليزية والعربية!

البنية التحتية لتكنولوجيا المعلومات

- قضية المرونة
- ISO 27031 العلاقة مع نظام إدارة أمن المعلومات (ISMS)
- مركز البيانات والبنية التحتية لتكنولوجيا المعلومات
- الاستدامة التشغيلية
- معيار البنية التحتية لموقع مركز البيانات
- عناصر الاستدامة التشغيلية
- سياسة واستراتيجية البنية التحتية
- الاستراتيجية - كيف وعمقها
- متطلبات السياسة
- حماية الموقع والبناء
- حماية الشبكة ونظم المعلومات
- تقييم المخاطر وتحليل أثر الأعمال (BIA)
- تقييم مخاطر الموقع والبناء
- تحليل) PESTEL السياسي والاقتصادي والاجتماعي والتكنولوجي والقانوني والبيئي(
- أنواع BIA الاستراتيجية والتكتيكية والتشغيلية
- طرق تنفيذ تكنولوجياBIA

خطط الاسترداد الإداري

- العمليات والإجراءات لإدارة سلسلة التوريد باستخدام نهج (3 PQ طريقة استبيان الطرف الثالث) التي تتماشى مع PAS BSI 7000
- بيانات الموقع الداخلية والخارجية وتخزين المعلومات بما في ذلك ترتيبات الاستجابة في حالات الطوارئ
- تغيير إدارة العمليات والاجراءات للمتطلبات اليومية
- اجراءات التحكم بالمخاطر لدعم الأنظمة والمعدات
- فهم تكنولوجيا التعافي من الكوارث (DR) واستعراض الأنشطة الرئيسية
- دورة حياة DR ، بما في ذلك الموارد والتدريب
- تقنية المعلومات DR كجزء من نظام إدارة أمن المعلومات
- نطاق عناصر تكنولوجيا المعلومات والمتطلبات

خط التعافي من كوارث تكنولوجيا المعلومات

- بناء خطط للتعافي من كوارث تكنولوجيا المعلومات
- التخطيط للملكية والهيكل وأدوار ومسؤوليات تكنولوجيا المعلومات لفريق DR
- مصادر البيانات والمعلومات والتبعيات الداخلية والخارجية
- اعتبارات أفضل الممارسات باستخدام ISO 27301 ، وكذلك ISO 20000 و ITIL
- إدارة واستعادة حوسبة المستخدم النهائي والتواصل التكنولوجي والاتصالات والبنية التحتية
- خيارات الاسترداد
- التطوير والتنفيذ والاختبار
- الملكية وهيكل الخطة
- أدوار ومسؤوليات الرئيس وقادة الفرق
- القيادة والتنسيق والاتصالات والاستعلامات (C3i)
- دور مركز القيادة والضروريات
- المعدات والمعلومات الداعمة
- إنتاج تقارير الحالة (SITREPS)
- أنواع الاختبارات / الممارسات
- الاستجابة للحوادث الكبرى
- تعريف "الحادث" وعملية التصعيد
- إنشاء قيادة والتنسيق والاتصالات (C3)
- توضيح دور مركز عمليات الشبكة (NOC)
- الاستجابة للطوارئ وخطة الاحتجاج
- دعم المعلومات والتجهيزات والأنظمة المطلوبة
- إنتاج تقارير الحالة (SITREPS) ، أنشطة الدخول والأدوات
- مراجعة تقرير ما بعد الحادث
- التعلم من الحوادث
- قيمة المراجعة بعد وقوع الحادث
- المشاركة العملية في الحوادث

التدقيق والصيانة

- ما هي وظيفة تدقيق تكنولوجيا المعلومات؟
- اللجنة التوجيهية والشروط المرجعية ل (TOR)
- مراجعة إدارة التجاوز والتحسين المستمر
- دمج DR في عمليات تنظيم دورة وإنشاء فرق افتراضية
- توثيق DR والتعامل مع وظائف التدقيق الداخلية والخارجية