

## شهادة في مجال تخطيط التعافي من كوارث تكنولوجيا المعلومات

### المقدمة

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

هذه الدورة العملية تزود المشاركين بطار يشمل ISO 27031 ، ISO 20000 ، ITIL ISO 22301 والتي 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 العالمية. 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 لเทคโนโลยيا المعلومات والاستدامة التشغيلية، ل توفير البيئة الآمنة
- وصف العمليات والإجراءات لتقييم المخاطر وتحديد التهديدات و نقاط 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 وتقديق تكنولوجيا المعلومات.
- الكتفاءات المستهدفة

التأكد من جاهزية قسم تكنولوجيا المعلومات لاستمرارية الأعمال

- اجراء تقييم المخاطر
- اجراء تحليل أثر الأعمال
- ادارة الحوادث والتغيير
- تخطيط التعافي من كوارث تكنولوجيا المعلومات
- فحص التعافي من كوارث تكنولوجيا المعلومات
- أنا أتحدث الإنجليزية والعربية!

### البنية التحتية لـ تكنولوجيا المعلومات

- قضية المرونة
- ISO 27031 العلاقة مع نظام إدارة أمن المعلومات (ISMS)
- مركز البيانات والبنية التحتية لـ تكنولوجيا 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 تكنولوجيا BIA

### خطط الاسترداد الإداري

العمليات والإجراءات لإدارة سلسلة التوريد باستخدام نهج 3PQ طريقة استبيان الطرف الثالث(التي تتعاشى مع BSI 7000

- بيانات الموضع الداخلية والخارجية وتزيين المعلومات بما في ذلك ترتيبات الاستجابة في حالات الطوارئ
- تغيير إدارة العمليات والإجراءات 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

- بناء خطط للتعافي من كوارث تكنولوجيا المعلومات
- التخطيط للملكية والهيكل وأدوار ومسؤوليات تكنولوجيا المعلومات لفريق DR
- مصادر البيانات والمعلومات والتأثيرات الداخلية والخارجية
- اعتبارات أفضل الممارسات باستخدام ISO 27301 ، وكذلك ISO 20000 وITIL
- إدارة واستعادة حوسنة المستخدم النهائي والتواصل التكنولوجي والاتصالات والبنية التحتية
- خيارات الاسترداد
- التطوير والتنفيذ والاختبار
- الملكية وهيكلة 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 التعزيز
- إنشاء قيادة وتنسيق والاتصالات (3C)
- توضيح دور مركز عمليات الشبكة (NOC)
- الاستجابة للطوارئ وخططة الاحتياج
- 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 (TOR)
- مراجعة إدارة التجاوز والتحسين المستمر
- دمج DR في عمليات تنظيم دورة وإنشاء فرق افتراضية
- توثيق DR والتعامل مع وظائف التدقيق الداخلية والخارجية