وزارة النقل والاتصالات وتقنية المعلومات
Ministry of Transport, Communications and Information Technology

الدليل الاسترشادي لاستمرارية عمليات تقنية المعلومات

أبريل 2026 م

نصل العالم
Connecting the world

@mtcitoman

الإصدار والتوزيع:

جهة الإصدار	البريد الالكتروني	تاريخ الإصدار
المديرية العامة للسياسات والحوكمة وزارة النقل والاتصالات وتقنية المعلومات	Governance@mtcit.gov.om	2025

سجل الوثيقة:

النسخة	التاريخ	جهة الإصدار	الملاحظات
0.1	2018	هيئة تقنية المعلومات	إطار عمل استمرارية خدمات تقنية المعلومات
0.2	2025	وزارة النقل والاتصالات وتقنية المعلومات	الدليل الاسترشادي لاستمرارية عمليات تقنية المعلومات

قائمة النشر:	
.1	جميع وحدات الجهاز الإداري للدولة
.2	الموقع الإلكتروني للوزارة

الفهرس:

المقدمة 3

الغرض 3

الأهداف.....3

النطاق.....3

المبادئ الأساسية 4

محتويات الدليل الاسترشادي 4

الأدوار والمسؤليات.....5

تحليل تأثير الأعمال (BIA).....6

خطط الاستمرارية.....7

الاختبار والتمارين.....10

مؤشرات الأداء والتحسين المستمر 12

التكامل 12

إدارة الوثيقة.....12

المصادر ذات الصله.....13

1. المقدمة

يوفر هذا الدليل نهج شامل ومنظم لضمان استمرارية عمليات تقنية المعلومات في الوحدات الحكومية والمتعاقدين معها، وذلك بالاستناد إلى أفضل الممارسات والمعايير الدولية المتمثلة في مواصفات المنظمة الدولية للمعايير (ISO).

يهدف الدليل إلى مساعدة الوحدات على بناء قدرات مرنة وفعالة للتعامل مع الأزمات والطوارئ المحتملة التي قد تؤثر على عمليات تقنية المعلومات، وتقليل الخسائر، والحفاظ على سمعة الوحدة وثقة أصحاب المصلحة والمستفيدين.

2.الغرض

توفير نموذج منهجي لإدارة استمرارية عمليات تقنية المعلومات أثناء الازمات والطوارئ

3.الأهداف

- توحيد الممارسات والإجراءات بين الوحدات الحكومية لضمان الامتثال للمعايير المحلية والدولية
- ضمان تكامل خطط الاستمرارية مع العمليات التشغيلية والتقنية للوحدة
- تحديد المسؤوليات والادوار المتعلقة باستمرارية عمليات تقنية المعلومات
- تعزيز قدرات الوحدات الحكومية على تقديم خدماتها اثناء الأزمات والطوارئ

4. النطاق

ينطبق هذا الدليل على جميع وحدات الجهاز الإداري للدولة والمتعاقدين معها، ويغطي الدليل جميع جوانب استمرارية عمليات تقنية المعلومات، بما في ذلك التخطيط، والتنفيذ، والاختبار، والمراجعة، والتحسين المستمر.

5.المبادئ الأساسية

يعتمد هذا الدليل على المبادئ الأساسية المستمدة من معايير ISO ذات الصلة، وخاصة ISO 22301 (إدارة استمرارية الأعمال) وISO/IEC 27001 (إدارة أمن المعلومات) وISO/IEC 27031 (جاهزية تقنية المعلومات والاتصالات لاستمرارية الأعمال).

تشمل هذه المبادئ:

- **إدارة المخاطر كجزء من استمرارية عمليات تقنية المعلومات**
يتم تصميم خطط استمرارية عمليات تقنية المعلومات بناء على نتائج تقييم المخاطر وتحليل تأثير الأعمال، لضمان التعامل مع التهديدات المحتملة بشكل استباقي وفعال.

- **الشمولية والتكامل**
تغطي الخطط جميع عناصر وعمليات تقنية المعلومات والخدمات الحيوية، مع ضمان تكاملها مع خطط استمرارية الأعمال المؤسسية الأخرى لتوفير استجابة موحدة ومنسقة أثناء الطوارئ.
- **التقييم الدوري والتحسين المستمر**
تراجع الخطط بشكل دوري وتحدث بناء على التحسينات التقنية، والتغيرات في الخدمات أو الأعمال، ونتائج الاختبارات والتدريبات، لضمان فاعليتها المستمرة.
- **وضوح الأدوار والمسؤوليات**
تحدد مسؤوليات جميع الموظفين والمستويات الإدارية بوضوح، لضمان استجابة سريعة وفعالة عند حدوث أي حالة طارئة.
- **المرونة والتكيف مع التغيرات**
تصميم الخطط بحيث تكون قادرة على التكيف مع التغيرات التقنية أو التشغيلية أو في البيئة التشريعية والقانونية، مما يضمن استمرارية فعالة للخدمات والعمليات الحيوية.

6. محتويات الدليل الاسترشادي

يحتوي الدليل الاسترشادي لاستمرارية عمليات تقنية المعلومات على النقاط الرئيسية التالية:

1. 6الأدوار والمسؤوليات حسب المستوى

- **<u>الإدارة العليا</u>**

- تحديد سياسات وخطط استمرارية عمليات تقنية المعلومات وضمان توافقها مع أهداف الوحدة.
- اعتماد خطط الاستمرارية وتوفير الموارد اللازمة لتنفيذها.
- مراجعة نتائج اختبارات الخطة والتقارير الدورية واتخاذ القرارات اللازمة لتحسين الاستمرارية.
- مراقبة التزام الفرق والأقسام المعنية بأدوارها ومسؤولياتها خلال الطوارئ.
- تعزيز ثقافة الاستمرارية والوعي بأهمية استمرارية الأعمال لدى جميع الموظفين.

- **رئيس فريق استمرارية عمليات تقنية المعلومات**

  - الإشراف على جميع أنشطة استمرارية عمليات تقنية المعلومات والتنسيق مع الإدارة العليا لضمان التكامل مع خطط استمرارية الأعمال المؤسسية.
  - اتخاذ القرارات التشغيلية أثناء الازمات والطوارئ ومراجعة تحديثات الخطة بشكل دوري.

- **مسؤول تقييم المخاطر وتحليل الأعمال(BIA & Risk Officer)**

  - تحديد الأولويات للخدمات الحيوية وإجراء تحليل تأثير الأعمال وتقييم المخاطر التقنية.
  - تقديم توصيات لتقليل المخاطر وضمان جاهزية الأنظمة.

- **مسؤول خطط الطوارئ والاستعادة(Disaster Recovery & IT Continuity Officer)**

  - تطوير خطط الطوارئ والاستعادة التقنية وتنفيذها أثناء الاختبارات أو الحوادث الفعلية.
  - تحديد خطط الاستعادة لكل العمليات الحيوية وضمان جاهزية الموارد البديلة.

- **مسؤول البنية الأساسية والدعم الفني(Infrastructure & Technical Support Officer)**

  - إدارة الموارد التقنية وضمان جاهزية الأنظمة والشبكات والخوادم.
  - تقديم الدعم الفني أثناء تنفيذ الخطط والتمارين العملية.

- **مسؤول التواصل والإبلاغ(Communication Officer)**

إدارة قنوات الاتصال الداخلي والخارجي أثناء الطوارئ ونقل المعلومات الدقيقة للجهات المعنية.

- **أعضاء داعمون / فرق مساعدة(Support Team Members)**

دعم تنفيذ الخطط أثناء الطوارئ والمشاركة في التمرينات العملية لضمان تكامل الاستجابة وسرعة الاستعادة.

6.2. تحليل تأثير الأعمال (BIA)

يهدف تحليل تأثير الأعمال إلى تحديد الخدمات والأنظمة الحيوية لتقنية المعلومات، وتحديد تأثير تعطلها على العمليات الحيوية. يتضمن ذلك تحديد هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO) لكل خدمة حيوية، كما يهدف هذا التحليل إلى فهم الآثار المحتملة للانقطاعات وتحديد أولويات التعافي ويجب أن يشمل BIA ما يلي:

- **تحديد الخدمات والأنظمة الحيوية**

تحديد جميع خدمات وأنظمة تقنية المعلومات التي تدعم العمليات الحيوية، يتضمن ذلك:

- قائمة بجميع العمليات والأنظمة والخدمات الأساسية للوحدة.
- تصنيفها حسب أهميتها للأعمال واستمرارية الخدمات.

- **تحديد الآثار المحتملة**

تقييم الآثار المحتملة لتعطل كل خدمة أو نظام حيوي لتقنية المعلومات، يمكن أن تشمل هذه الآثار:

- الآثار المالية: الخسائر المباشرة وغير المباشرة مثل: الغرامات، تكاليف التعافي.
- الآثار التشغيلية: توقف الخدمات الحيوية أو التأخير في تقديمها العمليات.
- الآثار القانونية والتنظيمية: عدم الامتثال للوائح والمعايير.
- آثار السمعة: فقدان ثقة المستفيدين، والتأثير على الصورة المؤسسية.

- **تحديد الأولويات ومدة التعطل المقبول**

بناء على الآثار المحتملة، يتم تحديد أهداف التعافي لكل خدمة أو نظام حيوي لتقنية المعلومات، تشمل هذه الأهداف:

- هدف وقت الاسترداد (Recovery Time Objective - RTO): الحد الأقصى للوقت الذي يجب أن تستغرقه خدمة أو نظام لتقنية المعلومات للعودة إلى مستوى مقبول من التشغيل بعد التعطل.
- هدف نقطة الاسترداد (Recovery Point Objective - RPO): أقصى قدر من فقدان البيانات الذي يمكن للوحدة أن تتحمله لخدمة أو نظام معين، يحدد هذا مدى حداثة البيانات التي يجب استعادتها.

- **تحديد الموارد الحرجة لاستعادة العمليات**: الأفراد، الأجهزة، الأنظمة، البيانات، المرافق، والاتصالات اللازمة لضمان استعادة التشغيل
- **تحديد الاعتماديات والتبعيات:** التعرف على الروابط بين العمليات والخدمات والأنظمة الأخرى بما في ذلك الأطراف الداخلية والخارجية التي تؤثر على استمرارية الخدمات
- **تحديد المخاطر والتهديدات المرتبطة:**

- تحديد أنواع المخاطر التي قد تؤثر عل الأنظمة، الخدمات، والبيانات بناءا على سياسة ودليل إدارة مخاطر تقنية المعلومات الصادر عن وزارة النقل والاتصالات وتقنية المعلومات.
- تقييم احتمال حدوث كل خطر والتأثير المحتمل

6.3. خطط الاستمرارية

تهدف خطط استمرارية عمليات تقنية المعلومات إلى ضمان استمرارية تشغيل الأنظمة والخدمات الحيوية للوحدة عند حدوث أزمات أو طوارئ، وتقليل المخاطر المرتبطة بتوقف الأنظمة، يتم تصميم هذه الخطط بناء على نتائج تحليل تأثير الأعمال وتقييم المخاطر، ويتم تطوير خطط مناسبة لضمان استمرارية عمليات تقنية المعلومات، ويجب أن تتوافق هذه الخطط مع أهداف التعافي (RTO وRPO) المحددة في تحليل تأثير الأعمال، وتشمل خطط الاستمرارية الرئيسية ما يلي:

- **النسخ الاحتياطي واستعادة البيانات (Backup and Recovery)**

تعتبر خطة النسخ الاحتياطي والاستعادة حجر الزاوية في أي خطة لاستمرارية عمليات تقنية المعلومات، ويجب أن تتضمن هذه الخطة:

- تحديد البيانات والأنظمة الحيوية: تحديد جميع البيانات والتطبيقات والأنظمة التي يجب نسخها احتياطيا بانتظام.
- جدولة النسخ الاحتياطي: تحديد تكرار النسخ الاحتياطي (على سبيل المثال: يومي، أسبوعي، شهري) بناء على RPO للبيانات والأنظمة.
- طرق النسخ الاحتياطي: استخدام طرق نسخ احتياطي مناسبة (على سبيل المثال: تكامل، تفاضلي، تزايدي تعددي) وتخزين النسخ الاحتياطية في مواقع آمنة ومنفصلة جغرافيا.
- اختبار الاستعادة: اختبار إجراءات الاستعادة بانتظام للتأكد من أن البيانات والأنظمة يمكن استعادتها بنجاح وفي الوقت المحدد.

- **خطط التعافي من الكوارث (Disaster Recovery-DR)**

تعتبر خطط التعافي من الكوارث ضرورية لضمان استمرارية العمليات في حالة تعطل الموقع الرئيسي للوحدة. وتعتمد هذه الخطط بناءً على RTO وRPO للخدمات الحيوية والميزانية المتاحة. على سبيل المثال:

- المواقع الساخنة (Hot Sites): مواقع جاهزة بالكامل مع جميع الأجهزة والبيانات والتطبيقات، ويمكن تفعيلها على الفور تقريبًا.
- المواقع الباردة (Cold Sites): مواقع توفر المساحة والبنية التقنية الأساسية (مثل الطاقة والتبريد) ولكنها تتطلب توفير وتركيب الأجهزة والبرامج والبيانات.
- التعافي من الكوارث المعتمد على السحابة (Cloud Sites): استخدام الخدمات السحابية لاستعادة الأنظمة بسرعة ومرونة.

- **المرونة والتكرار (Resilience and Redundancy)**

يهدف مفهوم التكرار والمرونة إلى ضمان استمرار تشغيل الأنظمة والخدمات بشكل مستمر دون انقطاع عند حدوث أي خلل او عطل. يعتمد هذا المفهوم على وجود نسخ إضافية من الأنظمة والخوادم ومسارات الاتصال بالإضافة الى تصميم أنظمة قادرة على التعافي الذاتي بسرعة وكفاءة مما يقلل المخاطر ويضمن استمرارية العمليات بشكل موثوق وفعال:

- المكونات المتكررة: استخدام مكونات متكررة (مثل الخوادم، أجهزة التخزين، مكونات الشبكة، مزودات الطاقة) لضمان عدم وجود نقطة تعطل واحدة.
- توازن التحميل (Load Balancing): توزيع حركة المرور عبر خوادم متعددة لزيادة التوافر وتقليل الضغط على خادم واحد.
- الشبكات المتعددة المسارات: تصميم الشبكات بمسارات متعددة لضمان استمرارية الاتصال في حالة تعطل مسار واحد.

- **التوافر العالي(High Availability – HA)**

تصميم الأنظمة الحيوية بحيث تعمل دون توقف تقريبا حتى عند حدوث أعطال أو مشاكل تقنية، ويهدف إلى تقليل الوقت للتوقف للحد الأدنى، وضمان استمرار الخدمات الحيوية للمستفيدين والموظفين بشكل مستمر، من خلال الآليات التالية:

- تصميم الأنظمة الحيوية للعمل بشكل مستمر: كل نظام حيوي يتم تصميمه بحيث يظل متاحا بشكل دائم مع القدرة على التعامل مع الأعطال التقنية أو ضغط التشغيل دون انقطاع الخدمة.
- تطبيق تقنيات التجميع (Clustering)والنسخ المتزامن (Replication) لضمان التشغيل المتواصل.

- **الاستعانة بمصادر خارجية (Outsourcing)**

قد تقتضي متطلبات استمرارية عمليات تقنية المعلومات، في بعض الحالات، الاستعانة بمصادر خارجية لتوفير بعض الخدمات الحيوية. على سبيل المثال :(خدمات الاستضافة، خدمات الدعم الفني، خدمات الحوسبة السحابية) وعند اعتماد هذا الخيار، يتوجب على الوحدة المعنية اختيار مزودي الخدمة بعناية وفق معايير واضحة، وضمان تضمين العقود المبرمة معهم اتفاقيات مستوى خدمة (SLAs) تنص بشكل صريح على متطلبات الاستمرارية وخطط التعافي.

- **خطط الاتصال والتواصل**

- يلتزم بإعداد خطة تفصيلية للتواصل بين فريق استمرارية عمليات تقنية المعلومات والموردين ذوي الصلة، على أن تشمل العناصر التالية:
- بيانات الاتصال الرسمية والمحدثة لكل مورد، بما في ذلك أرقام الهواتف المباشرة، عناوين البريد الإلكتروني، ووسائل التواصل البديلة للحالات الطارئة.
- تحديد نقاط اتصال رئيسية وبديلة لدى فريق الاستمرارية ولدى الموردين، مع توثيق الأسماء والمناصب.
- وضع آلية واضحة للتصعيد في حال تعذّر التواصل عبر القنوات الأساسية.
- تحديد أطر زمنية للاستجابة، وبيان مسؤوليات كل طرف خلال حالات الانقطاع أو أثناء مرحلة التعافي

6.4. الاختبار والتمارين

اختبار خطط استمرارية عمليات تقنية المعلومات بانتظام للتأكد من فعاليتها وتحديد أي ثغرات أو أوجه قصور قبل وقوع حادث حقيقي، يمكن أن تشمل الاختبارات تمارين على الطاولة، واختبارات محاكاة، واختبارات كاملة النطاق، تساعد هذه الخطوات في تدريب الفرق، وتحسين الإجراءات، والتحقق من أن الأهداف المحددة في تحليل تأثير الأعمال (BIA) يمكن تحقيقها، تشمل أنواع الاختبارات والتمارين ما يلي:

- **اختبارات المراجعة (Walk-through Tests)**

تتضمن هذه الاختبارات مراجعة خطط استمرارية عمليات تقنية المعلومات بالتنسيق مع الفرق المعنية، وذلك لمناقشة الإجراءات المعتمدة، وتحسين أي جوانب تحتاج إلى توضيح أو مواءمة، وضمان إدراك جميع الأطراف لأدوارهم ومسؤولياتهم بدقة.

- **اختبارات المحاكاة (Simulation Tests)**

تحاكي اختبارات المحاكاة سيناريو حادث أو أزمات طارئة محددة في بيئة خاضعة للرقابة، يتم تفعيل أجزاء من الخطة، وتقوم الفرق المعنية بتنفيذ الإجراءات المحددة، حيث تسمح هذه الاختبارات بتقييم فعالية الإجراءات، وتحديد نقاط الضعف في الخطة، وتدريب الفرق على الاستجابة في بيئة واقعية.

- **اختبارات التوازي (Parallel Tests)**

في اختبارات التوازي، يتم تشغيل العمليات العادية في الموقع الأساسي بينما يتم تفعيل خطة التعافي في الموقع البديل بشكل متزامن، حيث يتم استخدام بيانات حية أو بيانات طبق الأصل لتقييم قدرة الموقع البديل على دعم العمليات دون التأثير على العمليات الجارية.

- **اختبارات المقاطعة (Cutover Tests)**

تتضمن اختبارات المقاطعة تحويل العمليات الفعلية من الموقع الأساسي إلى الموقع البديل، هذا هو النوع الأكثر شمولاً وواقعية من الاختبارات، ولكنه ينطوي على مخاطر أعلى حيث يتم إيقاف العمليات في الموقع الأساسي.

- **التوثيق والمراجعة بعد الاختبار**
  - بعد كل اختبار أو تمرين، يجب توثيق النتائج بدقة، بما في ذلك:
  - السيناريو الذي تم اختباره.
  - الفرق المشاركة.
  - النتائج المرصودة
  - الدروس المستفادة.
  - التوصيات للتحسين.

6.5. مؤشرات الأداء والتحسين المستمر

يعد التحسين المستمر أحد المكونات الأساسية لضمان فعالية واستدامة خطط استمرارية عمليات تقنية المعلومات. ويقوم هذا النهج على التقييم الدوري والتطوير المنهجي للخطط والإجراءات، بما يضمن توافقها مع المتغيرات التقنية والتنظيمية والتشغيلية. ويتحقق ذلك من خلال ما يلي:

- مراجعة وتحديث الخطط والإجراءات بشكل دوري استنادًا إلى التغيرات والدروس المستفادة.
- تنفيذ اختبارات وتمارين محاكاة لقياس الجاهزية وكفاءة الاستجابة وتصحيح أوجه القصور.
- تحليل الدروس المستفادة من الحوادث والتجارب لتحسين الأداء المستقبلي.
- تحديث تحليل المخاطر وتأثير الأعمال (BIA) لتحديد التهديدات الجديدة وتعديل الأولويات.

- رفع مستوى الجاهزية البشرية والتنظيمية عبر التدريب المستمر والتوعية.
- تطوير البنية التقنية من خلال اعتماد تقنيات داعمة كالنسخ الاحتياطي والتعافي السحابي.
- مراقبة مؤشرات الأداء لتقييم كفاءة التنفيذ وتحديد فرص التحسين الاستباقية

7. التكامل

يعد التكامل بين إدارة مخاطر تقنية المعلومات واستمرارية عمليات تقنية المعلومات أمرا حيويا وضروريًا لضمان حماية واستمرارية الخدمات والعمليات الحيوية. حيث يوفر دليل إدارة المخاطر الأساس لفهم التهديدات وتقييم المخاطر ووضع خطط للحد منها، بينما يترجم دليل الاستمرارية هذه التقييمات إلى خطط عملية تضمن استمرار العمليات والخدمات الحيوية واستعادة الأنظمة والخدمات عند الأزمات والطوارئ.

8. إدارة الوثيقة

تعود ملكية هذا الدليل إلى وزارة النقل والاتصالات وتقنية المعلومات وسيخضع للمراجعة كلما اقتضت الحاجة ذلك.

9. المصادر ذات الصلة

- ISO 22301:2019
- ISO/IEC 27001:2022
- ISO/IEC 27031:2025
- ITIL4

ملحق1: التعاريف والمصطلحات

الوزارة	وزارة النقل والاتصالات وتقنية المعلومات
عمليات تقنية المعلومات	هي مجموعة من الأنشطة والإجراءات المنظمة والمسؤولة عن إدارة وتشغيل وصيانة البنية التحتية لتقنية المعلومات والخدمات المرتبطة بها، بما يضمن استمرارية الخدمات، توافرها، وأدائها وفق متطلبات الأعمال والمستخدمين النهائيين .وتشمل هذه العمليات عادة إدارة الشبكات، الخوادم، قواعد البيانات، التطبيقات، الأمن السيبراني، النسخ الاحتياطي والاستعادة، والمراقبة الدورية للأداء والحوادث.
المخاطر	احتمالية وقوع أحداث أو ظروف غير متوقعة ناتجة عن تهديدات أو ثغرات في الأنظمة أو العمليات أو الموارد التقنية، وقد تؤثر سلبًا على سرية أو سلامة أو توفر المعلومات أو على استمرارية الأعمال وتحقيق الأهداف التشغيلية والتنظيمية
النسخ الاحتياطي	إجراء نسخ احتياطية دورية للبيانات والأنظمة لضمان استمرارية العمل في حالة حدوث أعطال أو فقدان للبيانات
التدقيق	مراجعة الأنشطة والتغييرات على الأنظمة لتحديد أي انحرافات أو خروقات محتملة.
المراجعات الدورية	تقييم دوري للضوابط والإجراءات لضمان فعاليتها ومواكبتها للتغيرات في بيئة العمل والمخاطر
هدف وقت الاسترداد (RTO)	هو الحد الأقصى المسموح لمدة توقف العمليات او الخدمات بعد الازمات والحالات الطارئة، أي الوقت الذي يجب خلاله استعادة التشغيل الى الحالة الطبيعية أو مستوى مقبول من الخدمة
هدف نقطة الاسترداد (RPO)	. الحد الأقصى المسموح لفقدان البيانات في حالة حدوث انقطاع او طارئ، أي اللحظة الزمنية التي يمكن قبول فقدان البيانات بعدها دون التأثير على العمليات الحيوية للوحدة
تحليل تأثير الأعمال (BIA)	هو عملية منهجية لتحديد الخدمات والعمليات الحيوية للوحدة، وتقييم الآثار المحتملة للتوقف عنها، وتحديد الأولويات الزمنية والموارد اللازمة لاستعادتها، بهدف دعم اتخاذ القرارات الاستراتيجية في استمرارية عمليات تقنية المعلومات.
الموارد البديلة	كافة المواقع، الأجهزة، الأنظمة، البيانات، الاتصالات، والكوادر الاحتياطية التي يمكن استخدامها لضمان استمرارية الخدمات الحيوية للوحدة عند حدوث أي انقطاع او حادث طارئ.

النسخ الاحتياطي الكامل (Full Backup):	إنشاء نسخ شاملة لجميع البيانات والأنظمة الحيوية بشكل دوري
النسخ التفاضلي والتزايدي (Differential & Incremental):	نسخ التغييرات منذ آخر نسخ كامل أو تزايدي لتقليل حجم البيانات المستنسخة وتسريع الاستعادة.
التخزين المتعدد (Multi-Site Storage):	تخزين النسخ الاحتياطية في مواقع متعددة آمنة (Onsite, Offsite, Cloud)
التجميع	ربط مجموعة من الخوادم بحيث تعمل كوحدة واحدة إذا تعطل أحد الخوادم يتولى الاخر المهام تلقائيا دون توقف الخدمة
النسخ المتزامن	نسخ البيانات بشكل مستمر بين خوادم متعددة لضمان توافر نسخ احتياطية جاهزة فورا عند الحاجة
الأحداث الطارئة	انقطاع غير مخطط له في الخدمة أو انخفاض في جودتها، ويهدف التعامل معه إلى إعادة الخدمة إلى وضعها الطبيعي بأسرع وقت ممكن لتقليل الأثر على الأعمال
خطة استمرارية تقنية المعلومة	هي وثيقة منهجية ومتكاملة تتضمن الإجراءات والخطط والتدابير اللازمة لضمان استمرار تشغيل خدمات وأنظمة وتقنيات المعلومات الحيوية خلال الأحداث الطارئة أو الانقطاعات، ولتمكين استعادة الخدمات إلى مستوياتها المقبولة خلال المدة الزمنية المستهدفة(RTO)

ملحق2: نموذج تحليل تأثير انقطاع الأعمال(BIA)

معلومات عامة

- اسم الوحدة / القسم:
- المسؤول عن التحليل:
- تاريخ التحليل:
- نطاق التحليل:
  - الأنظمة:
  - العمليات:
  - الخدمات الحيوية:

تحديد العمليات الحيوية

رقم العملية	اسم العملية	الهدف / الغرض	الوصف	المسؤول العملية	تكرار العملية	ملاحظات
1						
2						
3						

تقييم التأثير على الأعمال

العملية	الفئة	التأثير المالي	التأثير التشغيلي	التأثير على السمعة	التأثير القانوني / الامتثال	مجموع التقييم
	منخفض / متوسط / عالي					
	منخفض / متوسط / عالي					
	منخفض / متوسط / عالي					

تحديد متطلبات استمرارية الأعمال

العملية	الحد الأقصى للانقطاع المقبول(MTPD)	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)	الموارد المطلوبة

تقييم المخاطر المرتبطة بكل عملية

العملية	المخاطر المحتملة	الاحتمالية	التأثير	خطة الاستجابة المقترحة
		منخفض / متوسط / عالي	منخفض / متوسط / عالي	
		منخفض / متوسط / عالي	منخفض / متوسط / عالي	
		منخفض / متوسط / عالي	منخفض / متوسط / عالي	

الأولويات والتوصيات

- ترتيب العمليات حسب الأهمية وتأثيرها على الأعمال.
- اقتراح إجراءات استمرارية لكل عملية حرجة.
- تحديد الموارد البديلة أو الحلول التقنية المطلوبة.
- تحديث الخطة بشكل دوري حسب التغيرات التشغيلية

مخرجات التحليل

- قائمة العمليات الحيوية وأولوياتها.
- RTO و RPOلكل عملية.
- متطلبات استمرارية الأعمال لكل نظام وموارد داعمة.
- توصيات لتعزيز الاستعداد والحد من تأثير الانقطاع.

ملحق3: اختبار خطة استمرارية عمليات تقنية المعلومات

معلومات عامة

-اسم الوحدة / القسم:

-المسؤول عن الاختبار:

-تاريخ الاختبار المخطط:

-تاريخ الاختبار الفعلي:

نوع الاختبار:

- اختبار ورقي(Tabletop Exercise)
- اختبار جزئي(Partial Test)
- اختبار كامل(Full-scale Test)

أهداف الاختبار

-التحقق من فعالية خطة استمرارية الأعمال.

-تحديد الفجوات في الإجراءات والموارد.

-تقييم جاهزية الفرق والتقنيات.

-تحديث الخطة بناءً على النتائج والدروس المستفادة.

نطاق الاختبار

العنصر	التغطية	الملاحظات
الأنظمة الحيوية	✓ / ✗	
البيانات	✓ / ✗	
الموارد البشرية	✓ / ✗	
الشبكات والاتصالات	✓ / ✗	
المرافق البديلة	✓ / ✗	

السيناريوهات المقترحة للاختبار

رقم السيناريو	نوع الحادث	وصف مختصر	الأنظمة المتأثرة	الهدف من الاختبار
1	انقطاع الكهرباء	انقطاع الكهرباء عن المركز الرئيسي	الخوادم والاتصالات	اختبار استجابة النظام البديل
2	فقدان البيانات	تلف قاعدة البيانات الرئيسية	قاعدة البيانات	اختبار استعادة البيانات من النسخ الاحتياطي
3	حادث أمني	هجوم سيبراني	جميع الأنظمة	اختبار إجراءات الأمن والتعافي
4	كوارث طبيعية	فيضان / حريق	المرافق الحيوية	اختبار خطط الطوارئ البديلة

خطوات الاختبار

1. إعلان بدء الاختبار للفرق المشاركة.
2. تنفيذ السيناريو حسب النوع المخطط.
3. تسجيل الملاحظات أثناء الاختبار) وقت الاستجابة، المشكلات، الإجراءات الفعّالة.(
4. قياس الأداء مقابل RTO وRPO
5. جمع التعليقات من جميع الفرق المشاركة.
6. إعداد تقرير الدروس المستفادة.

مؤشرات الأداء للاختبار

المؤشر	الهدف	القياس الفعلي	التعليق / الإجراءات التصحيحية
زمن استعادة الأنظمة	≤ RTO		
فقدان البيانات	≤ RPO		
نسبة الإجراءات المنفذة بنجاح	≥ 90%		
جاهزية الفريق	100%		
اكتمال الموارد البديلة	100%		

التوصيات بعد الاختبار

-تحديث خطة استمرارية الأعمال حسب الفجوات المكتشفة.
-إعادة تدريب الفرق على الإجراءات الناقصة.
-مراجعة العقود مع مزودي الخدمات البديلة إذا لزم الأمر.
-إعادة اختبار العناصر الحرجة خلال 6 أشهر.

ملحق4: نموذج مؤشرات الأداء الفعلي لخطة استمرارية عمليات تقنية المعلومات (IT Business Continuity KPIs)

المؤشر	الوصف	الهدف/المعيار المخطط	القياس الفعلي	التعليق / الإجراءات التصحيحية
زمن التعافي الفعلي (Actual Recovery Time)	الوقت الفعلي المستغرق لاستعادة النظام بعد حادث	≤ RTO المخطط لكل نظام	مثال: 3 ساعات مقابل RTO المخطط 2 ساعة	إذا تجاوزت الفعلي، مراجعة إجراءات التعافي أو تحسين البنية التحتية
نسبة الانحراف عن RTO (%)	النسبة المئوية للفارق بين الوقت الفعلي وRTO المخطط	≤ 10%	مثال: 50% زيادة عن RTO المخطط	تحليل أسباب التأخير وتحديث خطط التعافي
نسبة تنفيذ الاختبارات السنوية (Annual Test Execution Rate)	النسبة المئوية للاختبارات المجدولة التي تم تنفيذها فعليًا	100%	مثال: 80%	وضع جدول جديد للاختبارات المتأخرة وتوثيق الدروس المستفادة
نسبة نجاح اختبارات استمرارية الأعمال (%)	النسبة المئوية للاختبارات التي حققت الأهداف المحددة	≥ 90%	مثال: 85%	تحسين إجراءات التعافي وتصحيح نقاط الفشل
نسبة تغطية الأنظمة بخطط استمرارية الأعمال (IT Systems Coverage)	نسبة الأنظمة الحيوية التي لديها خطة استمرارية	100%	مثال: 95%	استكمال الخطط للأنظمة غير المغطاة
زمن استجابة الفريق للازمات والحالات الطارئة (Incident Response Time)	الوقت الفعلي للاستجابة للانقطاع أو الخلل	دقيقة 30 ≤	مثال: 45 دقيقة	تدريب إضافي للفريق وتحسين آليات الإنذار المبكر

عدد الحوادث التي تجاوزت RTO/RPO	عدد الحوادث التي لم يتم التعافي منها ضمن الأطر المخططة	0	مثال: 2 حالات طارئة	مراجعة الخطة لكل نظام والتأكد من جاهزية البنية الأساسية
تكرار تحديث خطط الاستمرارية	عدد المرات التي تم فيها تحديث خطط الاستمرارية في السنة	تحديث ≥ 1 سنوي	مثال: مرة واحدة فقط	وضع خطة مراجعة دورية وتحسين التغطية