

دليل للمدراء التنفيذيين - نسخة الخليج

استمرارية الأعمال بدون أوهام

كيف تحمي التدفق النقدي لشركتك

خريطة عملية لاستمرارية الأعمال للمؤسسات في دول مجلس التعاون الخليجي: من اكتشاف نقاط الضعف

إلى إدارة العمل في اليوم الذي تتوقف فيه الأنظمة.

risk-place.org · ممارسون في استمرارية الأعمال والمرونة المؤسسية وفق المواصفة ISO 22301 وإرشادات

الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث (نكيما) وأفضل الممارسات الدولية

نسخة مجانية. يمكنكم مشاركة هذا الملف دون تعديل داخل مؤسساتكم.

المحتويات

مقدمة. ما هذا الدليل وكيف تستخدمه

الجزء الأول. لماذا التدفق النقدي هش

الجزء الثاني. الخطوة 1. التقييم: أين ستتكسر

الجزء الثالث. الخطوة 2. تحليل الأثر على الأعمال وفق ISO 22301

الجزء الرابع. الخطوة 3. التعزيز: مرونة تقنية المعلومات

الجزء الخامس. الخطوة 3. التعزيز: الأشخاص

الجزء السادس. الجهات التنظيمية والسلطات العامة

الجزء السابع. ماذا تشترط الجهات التنظيمية في الخليج

الجزء الثامن. العمل عندما يتوقف كل شيء

خارطة طريق المرونة في 90 يوماً • عن المؤلفين • ماذا بعد

اختبر مرونة مؤسستك في 5 دقائق — تشخيص مجاني على risk-place.org/quiz.html

مقدمة. ما هذا الدليل وكيف تستخدمه

كُتب هذا الدليل لمالك الشركة وقائدها الأول — وللفريق الذي سيعمل إلى جانبك عندما يحدث خلل ما.

معظم القادة لديهم قائمة أرباح وخسائر وميزانية وخطة مبيعات. النتيجة المالية مرئية. أما المرونة التشغيلية —

القدرة على إبقاء النقد متدفقاً عندما تنكسر حلقة أساسية — فهي دائماً تقريباً نقطة عمياء. تبقى غير مرئية في

التقارير حتى اللحظة التي يصبح فيها الأوان قد فات.

إدارة استمرارية الأعمال (BCM) هي بالضبط النظرة المنهجية إلى تلك النقطة العمياء. الموضوع ليس عن الخوادم الاحتياطية ولا عن «موظفي تقنية المعلومات»، بل عن كيفية استمرار شركتك في الكسب في اليوم الذي يختفي فيه سندها المعتاد.

كيف تستخدم هذا الدليل

هذا الدليل خريطة وطريقة تفكير، وليس مجلداً من النماذج الجاهزة. مهمة هذا الكتاب أن ترى بوضوح، عند الانتهاء منه، أين شركتك مكشوفة وماذا تفعل حيال ذلك خطوة بخطوة. أما المنهجية الكاملة — بالنماذج والأمثلة التطبيقية والتقييم — فتُدرس في برنامج ERGP على risk-place.org.

المنطق يتبع مسار القائد: قيّم أولاً أين قد تنكسر، ثم اعمل على عملياتك الحرجة (تحليل الأثر)، ثم عزّز نصفي المرونة — البنية التقنية والأشخاص — واستعد للتعامل مع الجهات التنظيمية، وأخيراً اعرف ماذا تفعل في اليوم نفسه الذي تتوقف فيه الأنظمة.

لماذا التدفق النقدي هش

النقطة العمياء لدى التنفيذيين والتكلفة الحقيقية للانقطاع

1.1 المالك الذي لا يرى نقاط الضعف في التدفق النقدي

التدفق النقدي للشركة ليس سطرًا في تقرير. إنه بنية حية هشة مركبة من الاستراتيجيات واتفاقيات الشركاء وعلاقات العملاء والعمليات الداخلية والبنية التقنية. مثل برج من قطع الدومينو، يصمد ما دامت كل قطعة في مكانها.

دع خطراً كبيراً واحداً يتحقق — عطل في البرمجيات، هجوم سيبراني، فقدان مورد رئيسي أو تسريب بيانات — وتبدأ البنية في الانهيار. يستغرق التعافي أياماً وأسابيع، وأحياناً لا يحدث أبداً. والضربة لا تقع على قسم تقنية المعلومات بل على محفظتك وسمعتك.

افتراض خطير. «ما دام لدينا موظفو تقنية معلومات، فالشركة محمية.» موظفو الدعم يحدثون البرمجيات ويراقبون مضاد الفيروسات ويستعيدون الملفات. لكن سؤال «ماذا يحدث للنقد الوارد إذا تعطل هذا؟» لا يحلله أحد في معظم الشركات. تلك مسؤولية مباشرة للمالك والرئيس التنفيذي.

1.2 ما استمرارية الأعمال — ولماذا ليست شأن «موظفي تقنية

المعلومات»

استمرارية الأعمال هي قدرة الشركة على الاستجابة بفعالية للانقطاع، ومواصلة تقديم منتجها أو خدماتها بمستوى مقبول، واستعادة العمليات المتعطلة بأسرع وقت ممكن. الكلمات المفتاحية هي «المنتج» و«المستوى» و«الوقت»،

وليست «الخدام».

النسخ الاحتياطية ومضاد الفيروسات وقناة الاتصال الاحتياطية وسائلٌ. أما الاستمرارية فههدف إداري: كم من المال تخسر في كل ساعة توقف، وبأي سرعة تعود إلى الوضع الطبيعي. لهذا يجب أن تمتلك الإدارة الموضوع، لا تقنية المعلومات وحدها.

حالة قصيرة: «كان لدينا قسم تقني ومضاد فيروسات — وتوقفت الشركة أسبوعاً». ظنت شركة تجارية في المنطقة أنها محمية: لديها مسؤول أنظمة ومضاد فيروسات مرخص. دخلت برمجة فدية عبر بريد موظف عادي وشقّرت القرص المشترك الذي يحوي الطلبات والمخزون. كانت النسخ الاحتياطية تُؤخذ، لكن أحداً لم يجرب استعادتها قط — استغرق التعافي ستة أيام عمل. ما ضاع لم يكن ملفات، بل أسبوع من الشحنات وعميلان.

1.3 كم يكلف يوم توقف واحد

ما لم تُحسب تكلفة التوقف، يبقى الموضوع مجرداً. الحساب بسيط: خذ الإيراد عن فترة، واقسمه على عدد أيام العمل، وأضف ما لا يظهر في الإيراد مباشرة — الغرامات التعاقدية عن الالتزامات الفائتة، وفقدان العملاء، والعمل الإضافي للتعافي، والضرر بالسمعة.

هذا الرقم يغيّر الحوار. شيء أن تقول «من الجيد أن نهتم بالاستمرارية»، وشيء آخر أن تقول «كل يوم تتوقف فيه العملية الرئيسية يكلفنا مبلغاً محدداً، ونحن نعرف كم».

للتوقف ثمن — وهو يرتفع. في مسح عام 2024 قال أكثر من نصف المؤسسات إن آخر انقطاع كبير لديها كلف أكثر

من 100 ألف دولار، وقال واحد من كل خمسة إنه كلف أكثر من مليون دولار (Uptime Institute، التحليل

السنوي للانقطاعات 2024). للشركة التي تعمل بهوامش ضيقة، انقطاع خطير واحد مسألة بقاء لا مسألة راحة.

حالة قصيرة: الرقم الذي أنهى الجدول. حسبت شركة خدمات للمرة الأولى تكلفة يوم توقف لعمليتها الأساسية —

فبلغت نحو شهرين من الأرباح. بعد ذلك حُسم من تلقاء نفسه الجدول حول جدوى قناة احتياطية وتمارين جاهزية:

تكلفة الاستعداد أقل من خسائر يوم واحد. احسب تكلفة التوقف قبل الانقطاع، لا بعده.

1.4 التهديدات الأربعة التي تُسقط الأعمال في أغلب الأحيان

عملياً، يتمزق التدفق النقدي عند أربع نقاط نمطية. سنتناول كلاً منها لاحقاً بالتفصيل؛ الآن نكتفي بتسميتها — ومن شبه المؤكد أن واحدة منها على الأقل ستبدو مألوفة لك.

• **رحيل موظف أساسي.** الشخص الذي تقوم عليه العملية يستقيل أو ينتقل — وترحل معه الترتيبات وكلمات المرور و«كيف تسير الأمور فعلاً». في الخليج، حيث الفرق دولية ومتنقلة وقد يعني الرحيل مغادرة البلد خلال أسابيع، هذا الخطر أكثر حدة منه في أي مكان آخر تقريباً.

• **هجوم سيبراني.** برمجة فدية، اختراق، بريد مسروق. ما يتوقف ليس «التقنية» بل المبيعات والشحنات والمدفوعات. مكانة المنطقة تجعلها هدفاً: قطاعات الطاقة واللوجستيات والمال في الخليج تُهاجم عمداً لا عرضاً.

• **تعطل مورّد رئيسي أو حلقة لوجستية.** يسقط مورّد واحد للمواد أو المكوّنات أو خدمة — أو يُغلق مضيق أو ميناء أو ممر جوي فتتوقف السلسلة كلها. أثبتت السنوات الأخيرة بأي سرعة تتحول اضطرابات الشحن الإقليمية إلى مستودعات فارغة.

• **توقف البرمجيات.** يتوقف نظام إدارة العملاء أو تخطيط الموارد أو خدمة سحابية — لسبب تقني أو خارجي، بما في ذلك قطع الخدمة من مورّدين أجنب بدوافع العقوبات. إذا كان نظامك الحرج يُدار من ولاية قضائية أخرى، فإن توافره ليس قرارك بالكامل.

من أين تبدأ. لا تحاول إغلاق التهديدات الأربعة دفعة واحدة. خذ التهديد الأكثر واقعية بالنسبة لك وتتبعه عبر الكتاب كله — قيّمه وسعّره وعزّز الحماية منه. ثغرة واحدة مغلقة أئمن من خطة جميلة تغطي كل شيء دفعة واحدة.

الخطوة 1. التقييم: أين ستتكسر

نقاط تركّز المخاطر ومواطن الضعف الحرجة

2.1 كيف يعمل تدفقك النقدي وأين تتركز المخاطر

الخطوة الأولى هي تفكيك الحلقات التشغيلية والإدارية التي يتكوّن منها تدفقك النقدي. أين بالضبط يدخل المال إلى الشركة، وما الذي يجب أن يعمل باستمرار في الدخول.

ثم اعثر على نقاط تركّز المخاطر — المواضع التي يقوم فيها كل شيء على شيء واحد: خادم واحد، مورّد واحد، قناة مبيعات واحدة، شخص أساسي واحد. هذه نقاط الفشل الأحادية. قبل أن تراها تبدو موثوقة؛ وفي يوم الانقطاع تكون هي بالضبط ما يوقف العمل.

اختبار الحلقة — ثلاثة أسئلة. اسأل نفسك عن كل حلقة حرجة: (1) إذا توقفت هذه الوظيفة في الساعة القادمة، هل أستطيع استعادتها؟ (2) كم سيكلف ذلك؟ (3) هل سيعرف العملاء والشركاء؟ إن لم تستطع الإجابة بهدوء عن سؤال واحد منها، فقد وجدت موطن ضعف.

2.2 مواطن الضعف الحرجة: كيف تراها

موطن الضعف ليس «خطراً عاماً» مجرداً بل اعتماداً ملموساً يضرب انقطاعه المال مباشرة. انظر إلى الاعتماد على الأشخاص وعلى الأنظمة وعلى الأطراف المقابلة وعلى الظروف الخارجية. غالباً ما يكون أخطر موطن ضعف هو ذلك الذي يعرفه الجميع ولا يجد أحد وقتاً لإصلاحه.

من المهم هنا ألا تغرق في القوائم. في هذه المرحلة لا تحتاج جدولاً مثالياً بل صورة صادقة: ثلاثة إلى خمسة

مواضع يوقف تعطّلها دخولَ المال. ابدأ التعزيز بها.

حالة قصيرة: الوصفة في يد مورّد واحد. اشترت شركة أغذية مكوّنات أساسياً من مورّد خارجي واحد لسنوات — وكان المورّد يحتفظ أيضاً بالوصفة الدقيقة للخلطة. عندما ضاعف المورّد السعر وأخلّ بالمواعيد، تبين أنه لا بديل يمكن التحول إليه بسرعة: الشركة لا تستطيع إعادة إنتاج الوصفة بنفسها. لم يكن موطن الضعف «المورّد» بل فقدان السيطرة على المعرفة الخاصة.

الخطوة 2. تحليل الأثر على الأعمال وفق ISO 22301

تحليل الأثر بكلمات بسيطة

3.1 ما تحليل الأثر – ولماذا تحتاجه

تحليل الأثر على الأعمال (BIA) هو قلب المواصفة الدولية للاستمرارية ISO 22301 — وقلب الأطر الخليجية

المبنية عليها. إنه يجيب في جوهره عن سؤال واحد: أي العمليات حرجة إلى درجة أننا لن ننجو من فقدانها، وبأي

سرعة يجب إعادتها؟

ينقل تحليل الأثر الحوار من «ماذا لو» إلى الأرقام. تحدد لكل عملية حرجة بأي سرعة تنمو الخسائر أثناء التوقف وما

مدة الانقطاع المحتملة. من التحليل تولد الأولويات: ماذا نستعيد أولاً وماذا يمكن أن ينتظر.

مقياسان أساسيان. RTO (هدف وقت التعافي) — الوقت المستهدف للاستعادة: بأي سرعة يجب أن تعود العملية

للعمل. RPO (هدف نقطة التعافي) — فقد البيانات المقبول: كم من البيانات الحديثة يمكنك تحمل خسارته (مثلاً

«ليس أكثر من الساعة الأخيرة»). RTO يجيب عن «بأي سرعة»، و RPO عن «كم من البيانات يمكن أن يضيع».

3.2 إلى ماذا تنظر وكيف يُجرى

يُبنى تحليل الأثر حول العمليات الحرجة لا الإدارات. تنظر لكل عملية إلى ما تنتجه، وعلى أي أشخاص وأنظمة

وموردين تعتمد، وبأي سرعة يتفاقم الضرر إذا توقفت، وما أقصى مدة انقطاع يمكن تحملها (MTPD).

المنطق أهم من الشكل. لا حاجة لتحليل كل شيء: 80% من الخطر يسكن عادة في 20% من العمليات. هدفك أن

تعزل تلك القلة وتفهم اعتماداتها بعمق — وصولاً إلى الشخص المحدد والخدم المحدد والطرف المقابل المحدد.

علامة التحليل الجيد. بعده تستطيع الإجابة عن سؤال مجلس الإدارة بجملة واحدة: «إذا توقفت العملية X غداً، نخسر كذا يومياً، ونعيدها خلال كذا ساعة، وهذا ما نحتاجه لذلك.» إن لم تستطع، فالتحليل لم يكتمل.

حالة قصيرة: العملية التي لا يعرفها إلا شخص واحد. أثناء رسم خريطة العمليات الحرجة تبين أن إصدار فواتير العملاء يقوم كلياً على موظف واحد وملفه الشخصي. عندما كان في إجازة خارج البلاد، لم تصدر الفواتير. لم يضيف التحليل مخاطر جديدة — بل جعل مرئياً اعتماداً لم تلحظه الشركة لسنوات. هذه هي غاية التحليل: إظهار الحرج قبل أن ينكسر.

الخطوة 3. التعزيز: مرونة تقنية المعلومات

النسخ الاحتياطي والسحابة وخطر التركز ونموذج إشارة المرور

4.1 النسخ الاحتياطي والاستعادة

نصف المرونة تقني. والاستمرارية التقنية لا تبدأ من النسخة الاحتياطية نفسها بل من الاستعادة المختبرة. نسخة احتياطية لم تجرّب استعادتها قط هي أمل لا حماية.

الأساس قاعدة «1-2-3»: ثلاث نسخ من البيانات، على وسيطين مختلفين، إحداها خارج الموقع (في مركز بيانات آخر أو في السحابة). للأنظمة الحرجة فعلاً تضيف موقعاً احتياطياً يمكن التحول إليه. لكن أي مخطط لا قيمة له إلا إذا كانت له أهداف RTO و RPO مثبتة بالتمارين.

• نَقِّذ استعادات اختبارية بانتظام، لا نسخاً احتياطية فقط.

• احتفظ بنسخة واحدة على الأقل معزولة مادياً ومنطقياً — حتى لا تصل إليها برمجيات الفدية أيضاً.

• اعرف RPO لكل نظام: كم من البيانات ستخسر فعلياً لو حدث عطل الآن.

4.2 توزيع القدرات الخادمة والسحابة

أين تحتفظ بالأنظمة — في غرفة خوادمك أم في السحابة أم في مزيج هجين — ليس مسألة موضة بل إدارة

خطر. لكل خيار موطن ضعفه: غرفتك الخاصة تعتمد على موقع واحد وتبريده وكهربائه — وهذه ليست مسألة

هامشية في مناخ تبلغ حرارة صيفه خمسين درجة؛ والسحابة تعتمد على المزود والوصلة؛ والهجين أصعب تشغيلاً

لكنه أكثر مرونة.

المبدأ العملي هو التوزيع الجغرافي وغياب نقطة الفشل الأحادية. لا ينبغي أن تعتمد الخدمات الحرجة على مركز بيانات واحد ووصلة واحدة ومزود واحد. وفي الخليج أضف سؤالاً آخر: قواعد إقامة البيانات. عدة جهات تنظيمية تشترط بقاء بيانات معينة داخل البلد — تحقق قبل تصميم البنية لا بعده. واسأل فريقك التقني مباشرة: «إذا توقف مركز البيانات هذا أو هذا المزود يوماً — ماذا يتوقف عندنا بالضبط؟»

ما ينبغي أن تبقى الإدارة في مرمى نظرها، لا التقنية وحدها. قائمة الأنظمة الحرجة وأماكن استضافتها؛ عقود المزودين ومستويات الخدمة المضمونة (SLA)؛ هل يوجد موقع احتياطي وأين؛ من يعيد النظام إلى العمل يوم الجمعة وعلى أي رقم هاتف. هذه معلومات إدارية لا تفاصيل تقنية.

4.3 خطر التركيز والأطراف الثالثة

من أكثر مخاطر الاستمرارية حادثة التركيز — كم من أعمالك يقوم على طرف خارجي واحد. مزود سحابة واحد، منصة برمجية واحدة، مورد برمجيات حرج واحد. حين يتعطّلون تتعطّل أنت — عادة دون إنذار ودون ذنب منك. اتضح هذا بشكل مؤلم في يوليو 2024، عندما أدى تحديث معيب لمنتج أمني واسع الانتشار إلى تعطيل ملايين حواسيب ويندوز دفعة واحدة — فتوقفت رحلات جوية واضطربت مستشفيات وبنوك ومتاجر حول العالم، ومنها ناقلات ومطارات خليجية. لم يكن خطأ شركة واحدة، ومع ذلك توقفت آلاف الأعمال معاً.

الجواب هو إدارة الاعتماد. ارسم خريطة الأنظمة الحرجة التي تقوم على مزود واحد أو برمجيات مورد واحد، واسأل ماذا يحدث لو مرّ ذلك المزود بيوم سيئ. وللمواقع الأساسية خطط مسبقاً: مزود أو منطقة بديلة، والقدرة على العمل بوضع منخفض، وقبل كل شيء حق إخراج بياناتك.

• احتفظ بسجل للأطراف الثالثة الحرجة ودرجة اعتمادك على كل منها.

• لكل اعتماد حرج «خطة بديلة»: ما الذي يحل محله وكم يستغرق التحول.

• الإجراءات المؤسسية الصحيحة: ضمان حقوق تصدير البيانات وإبقاء البيانات الحرجة حيث تتحكم أنت

— لا مورّد واحد.

حالة قصيرة: عندما أوقف انقطاع مورّد واحد الوردية. شغلت شركة عملياتها كلها على منصة سحابية واحدة دون بديل. عندما مرّ المزود بانقطاع استمر ساعات، توقف استقبال الطلبات والشحن والفوترة دفعة واحدة — لم يكن ببساطة مكان آخر تذهب إليه. ما أنقذ الموقف عادةً قديمة بتصدير البيانات الأساسية محلياً كل أسبوع. كان الدرس باهظاً: البيانات الحرجة يجب أن تسكن حيث تتحكم أنت، ولا ينبغي لمزود واحد أن يستطيع إيقاف أعمالك كلها.

4.4 نموذج إشارة المرور: أحمر، كهرماني، أخضر

لكيلا يتحول التعافي إلى فوضى، تُقسّم الاستجابة إلى ثلاث مراحل متتابعة — مثل إشارة المرور. هذا نموذجنا العملي المجرب في عمليات حقيقية: بسيط وسهل الشرح للفريق ومريح لبناء الخطة حوله.

أحمر — الساعات الأولى: أوقف النزيف وأبلغ. الاستجابة الفورية: فعل الفريق، ونبه الأشخاص المعنيين، واحتو الضرر، وشغل خطة الاتصالات. الهدف إيقاف النزيف.

كهرماني — الوضع المؤقت: واصل العمل بينما تتعافى. انتقل إلى الحلول الالتفافية والقدرات الاحتياطية، وحافظ على حد أدنى حرج من الإنتاج، ونقذ الخطة بأدوار ومواعيد واضحة.

أخضر — التعافي الكامل. أعد الأنظمة والعمليات إلى وضعها الطبيعي، واستعد البيانات، وراجع الحادث وحدّ الخطط للمرة القادمة.

قوة النموذج أن كل فرد في الفريق يفهم في أي مرحلة توجد الشركة وما المطلوب منه الآن. أولاً أوقف النزيف، ثم عش مؤقتاً، ثم عد إلى الوضع الطبيعي. لا يمكن تخطي المراحل.

ما تفحصه في تقنيّتك هذا الأسبوع. هل لديك نسخة احتياطية حديثة للبيانات الحرجة — ومتى استعدتها فعلياً آخر مرة؟ كم نظاماً يعتمد على مركز بيانات واحد أو مزود واحد؟ أي برمجيات حرجة تأتي من مورّد واحد وماذا

يحدث لو مرّ بيوم سيئ؟ ثلاث إجابات صادقة ستريك أين أنت مكشوف.

الخطوة 3. التعزيز: الأشخاص

لماذا «يتوقف» الفريق عن العمل في الأزمة — وكيف تغيّر ذلك

5.1 ماذا يفعل التوتر بالناس

النصف الثاني من المرونة هو الأشخاص. قد تملك خططاً مثالية وخوادم احتياطية، لكن القرارات في الانقطاع

الحقيقي يتخذها بشر أحياء تحت الضغط. وهنا تتولى البيولوجيا الأمر.

يطلق التوتر الحاد استجابة «القتال أو الهروب»: ينتقل الدماغ من التحليل العقلاني إلى ردود فعل سريعة حدسية.

في الحياة اليومية ينقذنا ذلك؛ وفي إدارة الأزمة يرفع احتمال خطأ قاتل. الشخص إما ينشغل بأمور لا لزوم لها أو

يتجمد.

لماذا يهم معرفة هذا مسبقاً. لا يمكنك «تمالك نفسك» بالإرادة في اللحظة التي يكون العقل قد انطفأ فيها. لكن

يمكنك التدريب مسبقاً على أفعال بسيطة حتى تنطلق تلقائياً، وتوزيع الأدوار بحيث لا يعتمد كل شيء على شخص

واحد مُثَقِّل.

5.2 كيف يتصرف الناس في الأزمة

يتفاعل الناس بأشكال مختلفة، ولكن متوقعة. بعضهم يندفع للفعل دون خطة («قتال»)، وبعضهم يتجنب وينسحب

(«هروب»)، وبعضهم يتجمد وينتظر الأوامر («تجمّد»). ليس أي من هذا سوء نية — إنها فسيولوجيا يجب العمل

معها لا معاقبتها.

وفي الفريق الدولي — وهو القاعدة في الخليج — أضف طبقة أخرى: في الأزمة يعود الناس إلى لغتهم الأولى وإلى

عادات التراتبية في ثقافتهم الأم. الخطة التي تفترض أن الجميع سيعارض المدير بإنجليزية طليقة في الثالثة فجراً هي خطة على الورق. اجعل تعليمات الأزيمة قصيرة ومرئية وتمرناً عليها.

خطر منفصل هو الاحتراق الوظيفي المتراكم. تصنفه منظمة الصحة العالمية ظاهرة مهنية بثلاث علامات: إنهاك عاطفي، وتنامي السخرية، وانخفاض الفعالية. الفريق المحترق يدخل الأزيمة بلا احتياطي — وينكسر أسرع.

علامات الإنذار المبكر في الفريق. إنهاك عاطفي، ونكات ساخرة عن العمل والعملاء، وهبوط في الجودة لدى أشخاص أقوياء عادة. هذه ليست «كسلاً» بل إشارة إلى أن الاحتياطي ينفد. رصدها مهمة القائد قبل الأزيمة لا أثناءها.

5.3 كيف تجهّز الفريق

جاهزية الأشخاص تُبنى على ثلاثة أشياء: أدوار واضحة، وتمارين، وتقنيات بسيطة لضبط النفس. الأدوار — ليعرف كل فرد رقعته ولا ينتظر أن يقرر شخص واحد. التمرين — لتصبح الأفعال الصحيحة تلقائية.

• **تمارين المحاكاة المكتبية:** مثلوا «على الورق» تعطل خادم أو إغلاق مكتب. البروفة الحية وحدها تُظهر ما يعمل في الخطة وما لا يعمل.

• **وقفة الثواني العشر:** وقفة قصيرة قبل قرارٍ تحت الضغط تخفض بشكل ملموس احتمال خطأ حرج. تقنية بسيطة يمكنك استخدامها في الاجتماع مباشرة.

• لا تكبت مشاعر الفريق — وجّه طاقة التوتر إلى مهام ملموسة من الخطة.

حالة قصيرة: تمرين أنقذ يوماً حقيقياً. أجرت شركة تمريناً مكتبياً على تعطل مستودع — على الورق، من يفعل ماذا في الساعات الأولى. فظهر أن نصف الفريق لا يعرف أين الخطة ولا بمن يتصل. بعد شهرين وقع انقطاع حقيقي، وتعامل الفريق نفسه معه بهدوء: كانوا عاشوه مرة. التمارين رخيصة، وتعيد ثقة لا تُشتري لحظة الحادث الحقيقي.

الجهات التنظيمية والسلطات العامة

لمن تبليغ عند الحادث — وكيف تستعد

6.1 لمن تبليغ وعن ماذا

في الحادث الجسيم الجانب التقني نصف المهمة فقط. النصف الآخر هو الاتصال: من يجب ومن ينبغي أن تخبره، وبماذا، وبحلول متى. الصمت أو الرسائل المشوشة كثيراً ما تضر بالسمعة وبالعلاقة مع السلطات أكثر من الانقطاع نفسه.

حدد دائرة المتلقين وترتيبهم مسبقاً. عادةً: الجهة التنظيمية المختصة وهيئات الرقابة (خلال المهل المطلوبة)، والعملاء والشركاء الذين تتأثر الالتزامات تجاههم، وشركة تأمينك، ووسائل الإعلام عند الحاجة، ودائماً موظفوك أنفسهم كي لا يعرفوا الخبر من الخارج.

قاعدة المهل. كثير من الجهات التنظيمية يحدد مهلاً صارمة للإبلاغ عن الحادث — أحياناً ساعات لا أيام. عليك معرفتها قبل الحادث: البحث عنها أثناء الانقطاع متأخر جداً. وللقطاعات الخاضعة للرقابة في الخليج هذا اشتراط إلزامي لا مجاملة.

6.2 كيف تستعد مسبقاً

اتصالات الأزمة لا ترتجل — بل تُعدّ. الحد الأدنى: خطة اتصالات بقائمة المتلقين والمهل، ومتحدث رسمي واحد معيّن، ونماذج رسائل متفق عليها مسبقاً للسيناريوهات النمطية — بالعربية والإنجليزية، لأن جهتك التنظيمية وموظفيك وعملاءك في الخليج قد يتوقع كل منهم لغة مختلفة.

• صوت واحد: في الحادث يتحدث باسم الشركة شخص واحد معيّن — لا من صادف وجوده في المحادثة

أو على وسائل التواصل.

• ما لا تفعله: قبل اتّضح الحقائق — لا تقرّ بالذنب، ولا تذكر أرقام أضرار ارتجلاً، ولا تعد بمواعيد لا تعرفها.

• احتفظ بجهات اتصال محدّثة للجهات التنظيمية والعملاء الرئيسيين وشركة التأمين في متناول اليد —

وورقياً أيضاً تحسباً لتعطّل الأنظمة.

حالة قصيرة: خمسة أصوات بدل صوت واحد. في خضمّ حادثٍ كتب عدة موظفين عن المشكلة في آن واحد —

كلُّ روايته. تلقى العملاء والشركاء رسائل متناقضة، وكبر القلق حتى صار أكبر من الانقطاع نفسه. الدرس بسيط:

المتحدث الواحد المعيّن أهم من سرعة ردود الأفراد، ونموذج الرسالة المتفق عليه مسبقاً يوفر ساعات في اللحظة

الحاسمة.

ماذا تشترط الجهات التنظيمية في الخليج

المواصفات والمتطلبات — ولماذا تهتم الأعمال

7.1 الإطار الذي يُتوقع منك معرفته

استمرارية الأعمال في دول مجلس التعاون ليست مجرد حس سليم — فهي لعدد متزايد من المؤسسات اشتراط رسمي. معرفة هذا الإطار مفيدة مرتين: تحميك من الملاحظات والغرامات، وتمنحك بنية جاهزة للتنظيم.

• **ISO 22301** هي المرجع الدولي لأنظمة إدارة استمرارية الأعمال، والعمود الفقري الذي تُبنى عليه

المتطلبات الإقليمية. وتُطلب الشهادة بها بشكل متزايد في المناقصات الحكومية ومناقصات الشركات

الكبرى في الخليج.

• **الإمارات العربية المتحدة:** الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث (نكيما) تدير المواصفة

الوطنية لاستمرارية الأعمال (AE/SCNS/NCEMA 7000) وتتوقع من الجهات الحيوية تشغيل برامج

استمرارية موثقة متوائمة معها.

• **المملكة العربية السعودية:** البنك المركزي السعودي (ساما) يلزم البنوك والمؤسسات المالية بتشغيل إطار

لإدارة استمرارية الأعمال بحوكمة محددة وتحليل أثر واختبارات وتقارير؛ ويضيف نظام حماية البيانات

الشخصية واجبات تتعلق بحوادث البيانات.

• **المراكز المالية والجهات القطاعية** — مصرف الإمارات المركزي، وسلطة دبي للخدمات المالية في مركز

دبي المالي العالمي، وسلطة تنظيم الخدمات المالية في سوق أبوظبي العالمي، ومصرف قطر المركزي

ونظراؤها — تنشر قواعدها الخاصة بالمرونة التشغيلية والإسناد الخارجي للمؤسسات الخاضعة لرقابتها.

المتطلبات تتطور؛ قبل إعداد الوثائق الداخلية تحقق من الإصدار الساري لكل إطار ينطبق عليك. غاية هذا الفصل ليست أرقام المراجع بل النمط: الاستمرارية في الخليج تنتقل من ممارسة جيدة إلى التزام خاضع للرقابة.

نظرة الأعمال. المواصفة المعترف بها ليست أوراقاً لذاتها. برنامج عامل وفق ISO 22301 أو متوائم مع نكيما يكسبك مصداقية في المناقصات ومع البنوك وشركات التأمين والعملاء الكبار — تُظهر أنك شريك موثوق. وفي منطقة تتنافس على الثقة والعلاقات طويلة الأمد، هذا أصل تجاري لا كلفة امتثال.

العمل عندما يتوقف كل شيء

سيناريو عملي: لا نظام عملاء ولا نظام موارد غداً

8.1 السيناريو: غداً يتوقف نظام العملاء ونظام الموارد

تخيّل الأمر حرفياً: تصل صباحاً وأنظمتك الرئيسية — إدارة العملاء وتخطيط الموارد — لا تعمل. لا يهم السبب: عطل أو هجوم أو قطع خارجي. السؤال الوحيد: كيف تواصل الكسب اليوم لا بعد أسبوع؟ الخبر الجيد أن بوسعك الاستعداد لهذا، والاستعداد لا يكلف شيئاً تقريباً.

غاية الوضع المؤقت ليست إعادة إنتاج كل وظائف الأنظمة بل الحفاظ على حد أدنى حرج: استقبال الطلب، وشحنه، وقبض الثمن، والاحتفاظ بالعميل. كل ما عدا ذلك يمكن أن ينتظر.

•الاتصال: قناة احتياطية متفق عليها مسبقاً — تطبيق مراسلة عمل أو محادثة جماعية، وقائمة بأرقام

الهواتف الشخصية للأشخاص الأساسيين، ومكالمات جماعية. رتب هذا قبل الأزمة.

•الطلبات والسجلات: نموذج بسيط دون اتصال (جدول أو ورقة) تُدوّن فيه الطلبات والشحنات

والمدفوعات ما دامت الأنظمة غائبة، ثم يُنقل إلى النظام لاحقاً.

•الأدوار: من يستقبل الطلبات، ومن يؤكد الشحن، ومن يتواصل مع العملاء، ومن مع التقنية. لا ينبغي أن

يحمل شخص واحد كل شيء.

•العملاء: رسالة قصيرة صادقة — «نعمل بوضع خاص، نستقبل الطلبات، قد يحدث تأخير» — خير من

الصمت.

•العودة إلى الوضع الطبيعي: عند عودة الأنظمة يُدقَّق كل ما أُنجز يدوياً ويُدخَّل بعناية — كي لا تضيع

بيانات المرحلة الانتقالية.

حالة قصيرة: نصف يوم على الورق بدل أسبوع توقف. فقدت شركة تجارية الوصول إلى نظام عملائها وهاتفها

يوماً كاملاً بسبب انقطاع لدى المزود. بدل صرف الموظفين إلى بيوتهم، نقل المدير استقبال الطلبات إلى تطبيق

مراسلة وجدول بسيط، ووَزَع الأدوار وأُذِر العملاء الرئيسيين. عملت الشركة بنحو سبعين بالمئة من طاقتها — بدل

الصفـر. ومساءً أُدخِلت البيانات إلى النظام. كان الفرق بين «استعدنا» و«ارتبكنا» يساوي إيراد يوم كامل.

خارطة طريق المرونة في 90 يوماً

المرونة لا تُبنى في يوم، لكنها لا تحتاج سنوات أيضاً. الأفق الواقعي لأولى النتائج ثلاثة أشهر.

الأيام 1-30. انظر

احسب تكلفة يوم توقف. اعثر على ثلاثة إلى خمسة مواطن ضعف حرجة ونقاط فشل أحادية. أجرِ التقييم الذاتي

المجاني على risk-place.org.

الأيام 31-60. عزّز

اختبر الاستعادة من نسخة احتياطية. أغلق أخطر الاعتمادات — في التقنية وفي الأشخاص. وزّع الأدوار للحادث.

الأيام 61-90. تمرّن

أجرِ تمريناً مكتبياً على تعطل نظام أساسي. أعدّ خطة اتصالات — بلغتي العمل — وخطة استجابة بنموذج إشارة

المرور. اتفق على القنوات الاحتياطية.

عن المؤلفين

أعد هذا الدليل فريق risk-place — ممارسون في استمرارية الأعمال والمخاطر التشغيلية. يستند عملنا إلى

أفضل الممارسات الدولية والمواصفة ISO 22301، مع خبرة تطبيقية في بناء برامج الاستمرارية لدى مؤسسات

صناعية وخدمية كبرى وتدريب فرق القيادة على التصرف تحت الغموض والضغط. نتحدث لغة المال لا لغة الأوراق.

ماذا بعد. هذا الكتاب خريطة. أما الممارسة فهي ما يساعدك على قطع الطريق أسرع وبلا أخطاء.

برنامج ERGP — الشهادة التنفيذية في حوكمة المرونة المؤسسية — يتناول التقييم وتحليل الأثر والعمليات

المرنة وقيادة الأزمات والحوكمة في 94 فصلاً وستة وحدات، متاح كاملاً بالعربية والإنجليزية مع شهادة قابلة

للتحقق. التفاصيل: risk-place.org

ويمكنك البدء الآن: التشخيص المجاني يُظهر مستوى جاهزيتك خلال 5 دقائق —

risk-place.org/quiz.html

© risk-place.org · استمرارية الأعمال والمرونة المؤسسية · يجوز مشاركة هذه النسخة المجانية دون تعديل.