

# التزام مراقبة المورد الخارجي

## مخاطر التكنولوجيا

الأهمية	وصف الرقابة	نطاق الرقابة	مجال الرقابة
السجلات و/أو الإجراءات غير الكافية المتعلقة بأصول الأجهزة والبرامج التي تخرج من خدمات الدعم أو التكنولوجيا التي أصبحت معتمدة على أجهزة أو برامج القديمة قد تتسبب في تحقيق أداء غير مقبول إلى جانب عدم الاستقرار وظهور ثغرات أمنية وخسارة الأعمال التجارية وتكاليف الترحيل الباهظة.	يتعين على المورد إبلاغ بنك باركليز على الفور بالتغييرات المعروفة في قدرته على تقديم الدعم، سواء أكان مباشرًا أم غير مباشر، فيما يتعلق بأصول تكنولوجيا المعلومات المستخدمة في تقديم الخدمات إلى بنك باركليز، بما في ذلك عندما تتطوي المنتجات على نقاط ضعف أمنية، كما ينبغي أن يضمن ترقية أصول تكنولوجيا المعلومات التي يعتمد عليها أو سحبها في الوقت المناسب.	ضمان ترتيبات الدعم المستمر	1. إدارة التقادم
قد تتسبب حوادث التكنولوجيا التي لم يتم الإبلاغ عنها في الوقت المناسب أو لم تتضمن تفاصيل كافية، أو في حالة عدم اتخاذ الإجراء التصحيحي اللازم، في تعطيل الأنظمة/الخدمات بشكل يمكن تجنبه، أو إحداث تلف في البيانات أو فقدانها. تتطلب الحوادث الجسيمة استجابة معززة وعاجلة باعتبار أنها حوادث تشكل خطرًا كبيرًا على الأعمال التجارية ويمكن أن تؤدي إلى عواقب وخيمة بما في ذلك الأضرار المستمرة وفقدان السمعة والتأثير المالي والتأثير على إجراءات سير العمل الأساسية.	يتعين على المورد تشغيل نظام للتعامل مع الحوادث فيما يتعلق بتشغيل أنظمة تكنولوجيا المعلومات وخدماتها، ما يضمن تحديد كل حوادث التشغيل هذه وتسجيلها وتحديد أولوياتها وتصنيفها ومعالجتها بشكل مناسب على الفور إما عند الاتصال الأول أو عن طريق التصعيد المناسب وفي الوقت المناسب. وينبغي أن يتضمن ذلك إجراءً صارمًا للتعامل مع الحوادث الجسيمة بسرعة وفعالية.	تسجيل الحوادث وتصنيفها ومعالجتها	2. التعامل مع الحوادث
في حالة عدم تحديد المشكلات الأساسية التي تؤدي إلى وقوع حوادث تؤثر في توفير خدمات التكنولوجيا وحلها في الوقت المناسب، فقد يؤدي هذا إلى تعطيل الأنظمة/الخدمات بشكل يمكن تجنبه، أو حدوث تلف في البيانات أو فقدانها.	ينبغي للمورد تشغيل نظام للتحقيق في الوقت المناسب في المشكلات التي تكمن وراء حوادث التكنولوجيا المهمة، ما يضمن تحديد هذه المشكلات وتسجيلها من خلال تحليل السبب الجذري، وحلها الفعال لتقليل احتمالية تكرار الحوادث والحد من تأثيرها. ويتعين على المورد أيضًا التأكد من وجود تحليل استباقي للحوادث الروتينية لتحديد سبب تكرار الحوادث الشائعة والمتكررة بكثرة ومعالجته.	تحديد مشكلات التكنولوجيا وتقييمها وتحليلها ومعالجتها	3. إدارة المشكلات
قد تتسبب عمليات التغيير غير الملائمة لمنع التغييرات غير المصرح بها أو الإدارة بشكل سيئ أو غير المناسبة والتي تطرأ في خدمات التكنولوجيا في تعطيل الخدمة	يتعين على المورد التأكد من أن كل مكونات تكنولوجيا المعلومات المستخدمة في تقديم الخدمات إلى بنك باركليز تدار	فرض رقابة صارمة على التغيير	4. إدارة التغيير

<p>أو تلف البيانات أو فقدان البيانات أو خطأ في المعالجة أو الاحتيايل.</p>	<p>ضمن إطار نظام صارم للرقابة على التغيير، وهو ما يراعى تماماً الأهداف الآتية:</p> <p>1. عدم إجراء تغيير من دون تفويض مناسب - يلزم الموافقة قبل التنفيذ</p> <p>2. فصل المهام بين منشئ التغيير والمالك وجهة الموافقة والجهة المنفذة</p> <p>3. التغييرات المخطط لها والمُدارة وفق مستوى المخاطر المصاحبة</p> <p>4. التغييرات التي تؤخذ في الاعتبار بشكل كافٍ فيما يتعلق بالتأثير المحتمل على الأداء و/أو قدرة المكونات التكنولوجية المتأثرة</p> <p>5. التغييرات التي تخضع لاختبارات تقنية وتجارية ذات صلة بالتغيير قبل التنفيذ، مع الاحتفاظ بالأدلة عند الضرورة</p> <p>6. التغييرات التي ينبغي اختبارها بعد التنفيذ للتأكد من تسليمها بنجاح من دون أي تأثير غير مخطط له</p>		
<p>قد يؤدي عدم وجود خطط لتعافي النظام أو عدم كفايتها إلى فقدان غير مقبول في خدمة التكنولوجيا بالنسبة للأعمال أو العملاء عقب وقوع حادث يضمن تحديث وثائق المرونة وممارستها الحفاظ على تلبية خطط التعافي لاحتياجات العمل.</p>	<p>ينبغي أن يكون لدى المورد خطة (خطط) تعافي النظام (SRP) لكل نظام/خدمة تكنولوجية مطلوبة لدعم تقديم خدمات من فئة مرونة 0-3 إلى بنك باركليز، إلى جانب الأهداف الزمنية للتعافي (RTO) المطابقة وهدف نقطة التعافي (RPO). ويلزم مراجعة الخطة (الخطط) للتأكد من دقتها مرة واحدة على الأقل كل 12 شهرًا.</p> <p><b>ملحوظة:</b> بالنسبة إلى أنظمة/خدمات التكنولوجيا من فئة المرونة 0-1 التي تم تصميمها في شكل إيجابي/سلبي لتدابير المرونة، يتطلب التحقق من SRP بحيث يظل النظام لفترة طويلة في البيئة التي تمت استعدادتها وأن يعمل بمثابة BAU، وذلك للتأكد من أن كل العناصر تعمل بكفاءة. وهذا في الواقع هو حدث تقاطع الإنتاج (PCO)</p>	<p>خطة تعافي النظام (SRP)</p>	<p>15. مرونة التكنولوجيا</p>

<p>يُعد فقدان البيانات أحد أكبر التهديدات التي نتعرض لها إذ قد يحدث ذلك نتيجة لأفعال ضارة أو فشل في النظام. ويُعد وضع خطة لهذا السيناريو أمرًا مهمًا يساعد على تحديد مصادر البيانات والتبعيات وفهمها.</p>	<p>ينبغي أن يكون لدى المورد خطة (خطة) لسلامة البيانات وتعافيها (DIRP) لكل نظام/خدمة تكنولوجية مطلوبة لدعم تقديم خدمات من فئة مرونة 1-0 إلى بنك باركليز. ويلزم مراجعة الخطة (الخطة) للتأكد من دقتها مرة واحدة على الأقل كل 12 شهرًا.</p>	<p>خطة سلامة البيانات وتعافيها (DIRP)</p>	<p>5ب. مرونة التكنولوجيا</p>
<p>ينبغي أن يكون لدى مراكز البيانات مصادر طاقة بديلة، وروابط شبكة، وما إلى ذلك، وأن تكون متباعدة بما يكفي لتقليل مخاطر تأثر مراكز البيانات بحدث واحد في الوقت نفسه.</p>	<p>يتعين على المورد التأكد من أن كل نظام/خدمة تكنولوجية مطلوبة لدعم تقديم خدمات من فئة مرونة 3-0 إلى بنك باركليز والتي تتسم بالمرونة عبر مراكز البيانات وبعيدة بما يكفي لتقليل مخاطر تأثر مراكز البيانات بحدث واحد في الوقت نفسه.</p>	<p>تنوع مراكز البيانات</p>	<p>5ج. مرونة التكنولوجيا</p>
<p>من الممكن أن يكون لأنظمة التكنولوجيا التي يقدمها المورد تأثير في رحلات عملاء بنك باركليز. يُعد ضمان قدرة الموردين الذين يدعمون عمليات بنك باركليز التجارية على وضع خطط مرونة مناسبة يمكن اختبارها أمرًا بالغ الأهمية، فضلاً عن كونه تفويضًا تنظيميًا لبنك باركليز لتطبيق الحوكمة الملائمة في إدارة موردينا.</p> <p>يُمثل تقاطع الإنتاج (PCO) طريقة للتحقق من أن الممثل السليبي لنظام تم تكوينه بشكل إيجابي-سليبي يعمل كما هو متوقع وبالقدرة المطلوبة في عملية BAU. بالإضافة إلى ذلك، يتحقق PCO أيضًا من أن أي اعتماد على أنظمة أولية أو نهائية يستمر في العمل كما هو متوقع.</p>	<p>يتعين على المورد اختبار خطة (خطة) تعافي النظام (SRP) والتحقق منها لإثبات إمكانية تعافي الأنظمة/الخدمات التكنولوجية لتلبية متطلبات من فئة المرونة 3-0 لدى بنك باركليز.</p> <p>بالنسبة إلى كل نظام/خدمة تكنولوجية مطلوبة لدعم تقديم خدمات من فئة المرونة 1-0 المصممة في شكل إيجابي/سليبي لتدابير المرونة، يلزم تنشيط البيئة السلبية بعد خطة SRP الموثقة واستخدامها كبيئة إنتاج BAU، لفترة طويلة بما يكفي لإثبات القدرة ووظيفة التكامل الكامل (تقاطع الإنتاج).</p> <p>ينبغي أن تكون متطلبات تكرار التحقق مدعومة من قِبل فئة المرونة ذات الصلة، أي:</p> <ul style="list-style-type: none"> <li>- فئة المرونة 0: ينبغي إجراء التحقق من خطة SRP كل 12 شهرًا ولـ PCO كل 3 أشهر</li> <li>- فئة المرونة 1: ينبغي إجراء التحقق من SRP وPCO كل 12 شهرًا</li> <li>- فئة المرونة 2-3: ينبغي إجراء التحقق من SRP كل 24 شهرًا</li> </ul> <p>إذا فشل أي اختبار في تحقيق الحد الأدنى من متطلبات التعافي لفئة المرونة القابلة للتطبيق، فسيتعين على المورد إخطار بنك باركليز على الفور وتقديم خطط إصلاح تفصيلية (متضمنة الإجراءات التي يتعين اتخاذها وتواريخ الإنجاز المطابقة). ويتعين على المورد إخطار بنك</p>	<p>التحقق من خطة تعافي النظام (SRP)</p>	<p>5د. مرونة التكنولوجيا</p>

	باركليز قبل تنفيذ PCO.		
تُعد البيانات عنصرًا مهمًا يمكن أن يتأثر بصورة سلبية بعدة طرق. وينبغي ممارسة الخطة الموثقة لاستعادة البيانات أو تعافيها أو إعادة إنشائها للتأكد من أنها دقيقة وقابلة للتطبيق.	<p>ينبغي للمورد اختبار خطة (خطط) سلامة البيانات وتعافيها (DIRP) والتحقق منها لكل نظام/خدمة تكنولوجية مطلوبة لدعم تقديم خدمات من فئة مرونة 1-0 إلى بنك باركليز، إلى جانب الأهداف المقابلة المتعلقة بفترة التعافي (RTO) وهدف نقطة التعافي (RPO). يلزم إجراء عملية التحقق كل 12 شهرًا.</p> <p>إذا فشلت أي خطة في تحقيق الحد الأدنى من متطلبات التعافي لفئة المرونة القابلة للتطبيق، فسيتعين على المورد إخطار بنك باركليز على الفور وتقديم خطط إصلاح تفصيلية (متضمنة الإجراءات التي يتعين اتخاذها وتواريخ الإنجاز المطابقة).</p>	التحقق من DIRP	5. مرونة التكنولوجيا
قد يتسبب عدم كفاية التدابير اللازمة لرصد مستويات أداء و/أو قدرة موارد تكنولوجيا المعلومات والفتل في الحفاظ عليها متماشية مع المتطلبات الحالية والمستقبلية في انخفاض و/أو انقطاع غير مقبول في خدمات التكنولوجيا وفقدان الأعمال.	<p>يتعين على المورد تحديد المستويات المناسبة للأداء والقدرة لكل مكونات تكنولوجيا المعلومات الرئيسية المستخدمة في تقديم الخدمات إلى بنك باركليز، بما يتماشى مع احتياجات العمل المشار إليها. كما يتعين عليه أيضًا التأكد من وضع التنبيهات والحدود المناسبة وفق المكونات الرئيسية، للتحذير من احتمال تجاوز الحدود، ومراجعة هذه التنبيهات والحدود بشكل دوري لضمان توافق تقديم الخدمات مع احتياجات بنك باركليز.</p>	الحفاظ على توافق احتياجات بنك باركليز التكنولوجية	6. إدارة الأداء والقدرة
كما يمكن لعدم كفاية تعريف و/أو توثيق احتياجات الأعمال/العملاء أن يتسبب في أداء غير مقبول في خدمات التكنولوجيا وفقدان الأعمال.			

الأهمية	وصف الرقابة	نطاق الرقابة	مجال الرقابة
قد تؤدي الأنظمة والخدمات مضمونة الجودة والمختبرة بشكل غير كافٍ إلى خسارة الأداء الوظيفي بشكل حاسم غير متوقع في خدمات التكنولوجيا وإجراءات سير العمل.	يتعين على المورد التأكد من أن كل أنظمة وخدمات تكنولوجيا المعلومات المستخدمة في تقديم الخدمات إلى بنك باركليز يمكن إثبات أنها خضعت لعمليات ضمان جودة صارمة وشاملة وقابلة للتكرار، بما في ذلك، على سبيل المثال لا الحصر، الاختبارات الوظيفية وغير الوظيفية، واختبار أمان التطبيقات الثابت و ضمان جودة التعليمات البرمجية إما من خلال مراجعة الأقران أو من خلال الأدوات الآلية.	فرض ضمان الجودة القابل للتكرار	7. تطوير تطبيقات التكنولوجيا
قد يؤدي عدم كفاية الاتفاق على السلوك الوظيفي وغير الوظيفي للنظام إلى الانحراف عن سلوك نظام بنك باركليز المتوقع، ما يؤدي إلى مخاطر تهدد إجراءات سير العمل والإجراءات التشغيلية.	ينبغي أن يوافق المورد على تعريفات مخرجات العمل المقبولة بصورة متبادلة إما على أساس مرة واحدة أو بشكل مستمر والتي يتم من خلالها تقديم الإصدارات الجديدة أو المُحدثة من أنظمة وخدمات تكنولوجيا المعلومات وقبولها من قبل بنك باركليز.  ويلزم أن تتضمن صيغة هذه التعريفات جوانب وظيفية وغير وظيفية كافية للأنظمة والخدمات، ويمكن أن تتخذ أي صيغة مناسبة متفق عليها بصورة متبادلة مثل أدلة النظام الحالية، أو وثائق المتطلبات التفصيلية المتفق عليها بصورة متبادلة، أو قصص المستخدمين، أو حالات الاستخدام، أو أي صيغة أخرى مناسبة.  ويتعين على المورد أن يعمل مع بنك باركليز لضمان قبول مخرجات العمل سواء بشكل كلي أو جزئي متفق عليه بصورة متبادلة إما على أساس مرة واحدة أو بشكل مستمر استناداً إلى قبول بنك باركليز للأعمال لهذه التعريفات المتفق عليها مسبقاً.	قبول مخرجات العمل	

<p>قد يؤدي عدم وجود نسخ احتياطية لبيانات الأعمال أو التحكم فيها بشكل سيء إلى تعطل الأنظمة/الخدمات أو فقدان البيانات أو الإفصاح عن البيانات بشكل غير مناسب.</p>	<p>يتعين على المورد التأكد من أن كل أنظمة وخدمات تكنولوجيا المعلومات المستخدمة في تقديم الخدمات إلى بنك باركليز لديها ما يكفي من عمليات النسخ الاحتياطي والاستعادة التي تعمل بما يتماشى مع احتياجات بنك باركليز والتي أثبتت فعاليتها بشكل دوري.</p>	<p>تشغيل الإجراءات المناسبة والفعالة للنسخ الاحتياطي والاستعادة</p>	<p>8. ترتيبات النسخ الاحتياطي للأنظمة والبيانات</p>
<p>قد يؤدي عدم وجود نسخ احتياطية لبيانات الأعمال أو التحكم فيها بشكل سيئ إلى تعطل الأنظمة/الخدمات أو فقدان البيانات أو الإفصاح عن البيانات بشكل غير مناسب.</p>	<p>يتعين على المورد التأكد من أن كل وسائط النسخ الاحتياطي المرتبطة بتقديم الخدمات إلى بنك باركليز، إلى جانب الترتيبات الخاصة بالتعامل مع هذه الوسائط وتخزينها، تظل آمنة وموثوقة في كل الأوقات.</p>	<p>ضمان الحصول على وسائط نسخ احتياطي آمنة وموثوقة</p>	
<p>قد تتسبب إدخلالات السجل غير الملائمة المدرجة في مكونات التكنولوجيا (الأجهزة والبرامج)، بما في ذلك الملكية المحددة وتبعيات الجهات الخارجية في وجود خدمات وبيانات غير آمنة أو غير موثوقة. ويؤدي استخدام المكونات غير الإنتاجية في تقديم خدمات الإنتاج إلى ظهور مخاطر لأنها قد لا تكون مصممة أو مدارة وفق معايير الإنتاج.</p>	<p>يتعين على المورد التأكد من عدم الاعتماد على خدمات الإنتاج المقدمة إلى بنك باركليز في أي مكونات غير إنتاجية حتى يتسنى تجنب تقديم الخدمات غير الآمنة أو غير الموثوقة.</p>	<p>عزل بيئة الإنتاج</p>	<p>9. إدارة التكوين</p>
<p>قد تتسبب إدخلالات السجل غير الملائمة أو غير المكتملة (مع التبعيات/عمليات المسح ذات الصلة بعناصر التكوين الأخرى) في وجود خدمات وبيانات غير آمنة أو غير مستقرة نتيجة لتقييم الحوادث وتأثير التغيير غير الفعال.</p>	<p>ينبغي للمورد الاحتفاظ بإدخال سجل كامل ودقيق لكل أصول التكوين داخل النطاق والمستخدم في تقديم الخدمات إلى بنك باركليز (بما في ذلك الملكية والتبعيات/عمليات المسح الأولية / النهائية). ويلزم أن يكون لدى المورد ضوابط مطبقة تضمن الصيانة المستمرة لدقة البيانات واكتمالها.</p>	<p>تسجيل تفاصيل التكوين وصيانتها</p>	

<p>قد تتسبب إدخلالات السجل غير الملائمة المدرجة في أصول أجهزة التكنولوجيا، بما في ذلك الملكية المحددة وتبعيات الجهات الخارجية في وجود خدمات وبيانات غير آمنة أو غير موثوقة. قد يؤدي عدم تطهير أصول الأجهزة والتخلص منها بطريقة آمنة إلى حدوث أضرار مالية وتنظيمية والإضرار بالسمعة.</p>	<p>يلزم أن يكون لدى المورد ضوابط مطبقة تضمن التسجيل والصيانة المستمرة لبيانات أصول الأجهزة طوال دورة حياة الأصول.</p> <p>ينبغي للمورد الاحتفاظ بإدخال سجل كامل ودقيق لكل أصول أجهزة تكنولوجيا المعلومات المستخدمة في تقديم الخدمات إلى بنك باركليز).</p>	<p>تسجيل تفاصيل أصول الأجهزة وصيانتها</p>	<p>10. إدارة أصول الأجهزة</p>
<p>من المهم أن يحصل المورد على تأكيد رسمي يفيد بأنه تم التخلص من الأصول بشكل صحيح (بما في ذلك التدمير الآمن لبيانات البنك) ويقوم بتسجيل هذا التأكيد. قد يؤدي عدم تطهير أصول الأجهزة والتخلص منها بطريقة آمنة إلى حدوث أضرار مالية وتنظيمية والإضرار بالسمعة.</p>	<p>يتعين تطهير كل الأصول التي يتم التخلص منها بشكل كامل من كل بيانات بنك باركليز والتخلص منها بشكل آمن من خلال عملية رسمية للتخلص من الأصول، والتي تتوافق مع متطلبات معايير بنك باركليز الأمنية ذات الصلة.</p>	<p>عملية التخلص من الأصول</p>	
<p>من المهم أن يكون لدى المورد ضوابط تضمن إجراء تحقيقات شاملة في الأصول المفقودة، وفي حالة عدم العثور عليها، يتم إبلاغ بنك باركليز للتوقيع على المخاطر. قد يؤدي فقدان أصول الأجهزة ومن ثم الفشل في تطهيرها والتخلص منها بطريقة آمنة إلى حدوث أضرار مالية وتنظيمية والإضرار بالسمعة.</p>	<p>ينبغي إجراء تحقيق في كل الأصول "المفقودة أو المسروقة" بصورة صحيحة، وإبلاغ بنك باركليز بها للتوقيع على المخاطر إذا لم يتم العثور عليها.</p>	<p>الأصول المفقودة</p>	



الأهمية	وصف الرقابة	نطاق الرقابة	مجال الرقابة
<p>قد تتسبب إداخلات السجل غير الملائمة المدرجة في أصول برامج التكنولوجيا، بما في ذلك الملكية المحددة في وجود خدمات وبيانات غير آمنة أو غير موثوقة. وقد يؤدي الفشل في إدارة استخدام البرامج مقابل الاستحقاق إلى حدوث أضرار مالية وتنظيمية والإضرار بالسمعة.</p>	<p>يتعين على المورد الاحتفاظ بسجل كامل ودقيق لكل أصول البرامج وعمليات التثبيت ذات الصلة داخل النطاق المستخدمة في تقديم الخدمات إلى بنك باركليز (بما في ذلك الملكية). وينبغي للمورد الحفاظ على دقة البيانات واكتمالها بداية من الشراء ووصولاً إلى التخلص منها (ومن التثبيت إلى إزالة التثبيت). كما ينبغي للمورد التأكد أيضاً من أن استخدام البرنامج يظل متمشياً مع بنود الترخيص المحدد.</p>	<p>تسجيل تفاصيل أصول/تثبيت البرامج وصيانتها. ترخيص أصول البرامج</p>	<p>11. إدارة أصول البرامج</p>

## تعريفات مرونة التكنولوجيا

الهدف الزمني للتعافي (RTO)	RTO هو الوقت المنقضي بين الإخفاق أو الانقطاع غير المتوقع للخدمات واستئناف العمليات.
هدف نقطة التعافي (RPO)	RPO هو الحالة المستهدفة لتوافر البيانات في بداية عملية التعافي. وهو مقياس للحد الأقصى من فقدان البيانات المسموح به في حالة التعافي.
تقاطع الإنتاج (PCO)	PCO هو عبارة عن تنشيط الممثل البديل (DR) للأنظمة المصممة في تكوين إيجابي-سليبي واستخدامه كممثل إنتاج على مدى فترة زمنية طويلة للتحقق من الأداء الوظيفي الكامل والقدرة الكاملة.
خطة تعافي النظام	تتمثل خطة تعافي النظام في مستند يحدد العناصر والتفاصيل التقنية الخاصة بكيفية تعافي نظام أو أي مكون فشل في العودة إلى حالة التشغيل.
خطة سلامة البيانات وتعافيها	تمثل خطة سلامة البيانات وتعافيها مستندًا ينص على الخطوات الواجب اتخاذها لتعافي البيانات المفقودة بسبب فشل النظام أو بقصد إلحاق الضرر بها. وينبغي أن تتناول الخطة السيناريوهات بخيارات ذات صلة (على سبيل المثال إعادة تشغيل البيانات من أنظمة أخرى أو استعادة البيانات من أرشيفات الأشرطة أو إعادة إنشاء البيانات).

متطلبات المرونة التي تفرضها بنك باركليز حسب مصفوفة فئة المرونة

فئة المرونة	0	1	2	3
الهدف الزمني للتعافي (RTO)	يصل إلى 5 دقائق	يصل إلى 4 ساعات	يصل إلى 12 ساعة	يصل إلى 24 ساعة
هدف نقطة التعافي (RPO)	يصل إلى 5 دقائق	يصل إلى 15 دقيقة	يصل إلى 30 دقيقة	يصل إلى 24 ساعة

الإصدار 10.0، بتاريخ أكتوبر 2020