

חובת פיקוח על ספקים חיצוניים תכנון התאוששות

1. הגדרות:

אירוע שיבוש	רשימה של השפעות מקרה עם גורם אגנוסטי שספקים בחרו כדי לבצע פעולות מתקנות באמצעות יישום תוכנית התאוששות ועמידות ויישום יכולות. שיבושים כגון אירועי סייבר, אסונות טבע או אירועים מעשה ידי אדם יכולים להפריע לפעילות של ישות מסוימת.
תקרית	אירוע משבש שניתן לנהל כחלק מפעולות יומיומיות, באמצעות הפעלה של תוכנית התאוששות.
תוכנית התאוששות	תוכנית התאוששות הנן מסמכים המפרטים את הצעדים והפעולות שיש לנקוט כדי להחזיר שירות למצב תפעולי. הן עשויות להיקרא 'תוכניות המשכיות עסקית' וכדומה.
תכנון התאוששות	התהליך או התכנון התאוששות של שירותים עסקיים, תהליכים עסקיים ויחסי תלות הבסיסיים.
יעד זמן התאוששות	פרק הזמן שחולף בין כשל בלתי צפוי או הפרעה לשירותים לבין חידוש הפעילות.
יעד נקודת התאוששות	יעד נקודת התאוששות (PRO) הוא מונח שמוגדר כ"מצב היעד לזמינות נתונים בתחילת תהליך השחזור". זו מדידה של אובדן נתונים מרבי נסבל לעסק במצב התאוששות.
דרגת עמידות	קטגוריית העמידות היא דירוג המשמש את Barclays כדי להחיל דרישות עמידות על שירות בהתאם לדרגת החומרה ולהשפעה. קטגוריית העמידות מניבה יעד זמן התאוששות (RTO), יעד נקודת התאוששות (RPO) ודרישה לתדירות אימות.
נזק בלתי נסבל	הנקודה שבה הפרעה לשירות הופכת לבלתי נסבלת מנקודת המבט של לקוחות/צרכנים, שווקים פיננסיים או הבטיחות והיציבות של Barclays.
יחסי תלות של משאבים	אותם יחסי תלות (טכנולוגיה, שירות של צד שלישי, כוח עבודה) שנדרשים כדי לספק את השירותים העסקיים.

2. מטריצת ביקורת עמידות:

שירותי הספק מוקצים לקטגוריית עמידות ספציפית (0-4) שמשקפת את יעדי ההתאוששות של Barclays דורשת מהספק לעמוד בהם בהתאם להשפעה שהפרעה בשירות עלולה לגרום ל-Barclays. ככל שדירוג קטגוריית העמידות גבוה יותר (כלומר מספר נמוך יותר), נדרשת רמה גבוהה יותר של יכולת עמידות או התאוששות, בהתאם לרמת הקריטיות של השירות. על הספק להבטיח ששירותיו עומדים בדרישות ההתאוששות כמפורט במטריצת ביקורת העמידות לקטגוריית העמידות הרלוונטית שנקבעה על-ידי Barclays לשירותים הכלולים בהתחייבות החוזית. מטריצת ביקורת העמידות מציינת אילו בקורות רלוונטיות בהתאם לקטגוריית העמידות. פרטי דרישת הפיקוח מפורטים בסעיף 3 (אמצעי פיקוח).

השפעה לא משמעותית	השפעה נמוכה	השפעה בינונית	השפעה גבוהה	השפעה יוצאת דופן	הערכת השפעת סיכונים
4	3	2	1	0	דרגת עמידות
אין שחזור מתוכנן	עד 24 שעות	עד 12 שעות	עד 4 שעות	עד שעה	יעד RTO
אין שחזור מתוכנן	עד 24 שעות	עד 30 דקות	עד 15 דקות	עד 5 דקות	יעד RPO
קטגוריית עמידות 4	קטגוריית עמידות 3	קטגוריית עמידות 2	קטגוריית עמידות 1	קטגוריית עמידות 0	תדירות בדיקה טכנולוגית
אין שחזור מתוכנן	לפחות כל 24 חודשים	לפחות כל 12 חודשים	לפחות פעמיים בשנה	לפחות פעמיים בשנה	אימות תוכנית שחזור המערכת
אין שחזור מתוכנן	אופציונלי	לפחות כל 12 חודשים	אימות שנתי באמצעות מעבר על שולחן העבודה	אימות שנתי של תוכנית בסביבה המדמה סביבת ייצור	אימות תוכנית שחזור נתונים
אין שחזור מתוכנן	אופציונלי	אופציונלי	אימות שנתי באמצעות מעבר על שולחן העבודה	אימות שנתי באמצעות מעבר על שולחן העבודה	אימות תוכנית בנייה מחדש של פלטפורמה ויישומים
קטגוריית עמידות 4	קטגוריית עמידות 3	קטגוריית עמידות 2	קטגוריית עמידות 1	קטגוריית עמידות 0	בקרת ספקים – ישימות
○	✓	✓	✓	✓	1. דרישת מיפוי ליחסי תלות של משאבים להכללה בתוכנית השחזור
○	✓	✓	✓	✓	2. אירועים מפריעים במסגרת תוכנית השחזור
○	✓	✓	✓	✓	3. תכנון התאוששות עסקית ודרישת אימות
○	○	○	✓	✓	4. דרישות בדיקה משולבות
○	✓	✓	✓	✓	5. תוכניות שחזור מערכת ודרישת אימות
○	○	○	✓	✓	6. תוכניות שחזור נתונים ודרישות אימות
○	✓	✓	✓	✓	7. גיוון במרכז הנתונים ודרישות מספק שירותי ענן
○	○	○	✓	✓	8. דרישות במסגרת תוכנית בנייה מחדש של פלטפורמה ויישומים
○ = אופציונלי			✓ = נדדש		

אם מזוהות בעיות כלשהן במהלך ביצוע הבדיקה או במקרה של אי עמידה בדרישות שמזוהה במהלך בדיקת של אמצעי הפיקוח, יהיה על הספק להודיע על כך ל- Barclays באופן מיידי (בדרך כלל, לא יאוחר מ-10 יום) ולתקן את הבעיות שזוהו עד לתאריך המוסכם.

3. אמצעי פיקוח:

על הספק ליישם גישה מובנית לעמידות (המשכיות עסקית והתאוששות לאחר אסון) הנתמכת במסמך מדיניות ותקנים המסדירים דרישות לעמידות תפעולית וטכנית, בהתאם לשיטות העבודה המומלצות בתעשייה ולדרישות הרגולציה, על פי הצורך. על הנהלת הארגון הבכירה לפקח על הגישה המובנית לעמידות ולקיים בדיקות והערכות שנתיות של רמת יעילות הגישה.

מדוע זה חשוב	תיאור הפיקוח	כותרת פיקוח
<p>ספקים צריכים להבין ולתעד את יחסי התלות שלהם במשאבים כדי לספק את השירות שלהם ל-Barclays. יחסי התלות של משאבים חייבים להיות חלק מתוכנית ההתאוששות העסקית של הספק כדי לוודא שהם כלולים כדי למתן את השפעת התקריות ולמנוע פגיעה באספקת השירות ל-Barclays.</p>	<p>על הספק להגדיר ולתעד יחסי תלות של משאבים שהם קריטיים לאספקת השירות ל-Barclays. יש לשמור את יחסי התלות ולבדוק אותם מדי 12 חודשים או במקרה של שינוי מהותי.</p> <p>יחסי תלות של משאבים שיש לשקול כוללים:</p> <ul style="list-style-type: none"> טכנולוגיה ונתונים (באופן פנים ארגוני ואצל קבלני משנה שמספקים אותם). קבלני משנה המספקים חומרים (שעשויים להשפיע באופן מהותי על רמת הביצועים ועל אספקת השירות ל-Barclays). כוח עבודה (אובדן אנשים, אין לשקול אסטרטגיית התאוששות באזור העבודה או יכולת עבודה מהבית). 	<p>1. דרישת מיפוי ליחסי תלות של משאבים להכללה בתוכנית השחזור</p>
<p>Barclays מציבה דרישה מסחרית (ומבוססת סיכונים) על פיה יש להימנע ו/או להדגים יכולת התאוששות בזמן מאירועי שיבוש משמעותיים, כלומר, להדגים עמידות נאותה. Barclays נדרשת לקבל ערובות על מנת שתוכל להבטיח לבעלי העניין כי במקרה של הפרעות, השירות ימזער את השפעתן (בין אם מדובר בהשפעה על לקוחות, בהשפעה פיננסית ו/או בהשפעה על המוניטין).</p>	<p>על הספק לקבוע מהו ההיקף של אירועים משבשים לצורכי תכנון ההתאוששות ומהי רמת התכנון הנדרשת כדי להבטיח שניתן יהיה לספק את השירותים במסגרת רמות השירות המוסכמות ויעדי זמן השחזור המתאימים. על הספק לוודא שאירועי שיבוש שממשיכים לשקף את נוף הסיכונים/האיומים הנוכחי, ייבחנו בהתאם לרמת החומרה והסבירות ונתמכים על-ידי תובנות בינה ותובנות מהענף.</p> <p>על הספק לכלול את אירועי השיבוש הבאים בהיקף התכנון לכל הפחות.</p> <ul style="list-style-type: none"> אובדן של מבנים על פני מספר מיקומים, עם השפעה ישירה על אספקת השירותים ל-Barclays. (מבנים ותשתיות קשורות אינם זמינים). תרחיש של אובדן נתונים, כולל השחתת נתונים, אירועי סייבר וההשפעה האפשרית שלהם על אספקת השירותים ל-Barclays. אובדן משאבי כוח אדם אשר ישפיעו על אספקת של רמות שירות מוסכמות (כגון מגיפה, אירוע גאופוליטי, כשל קריטי בתשתיות לאומיות וכו'). אובדן שירותי טכנולוגיה (אובדן של מרכזי נתונים או של אזור המכוסה על ידי ספק שירותי ענן). אובדן קבלן משנה המספק חומרים (שירותים או אספקה). <p>יש לבדוק אירועי שיבוש מדי שנה, על בסיס מתמשך, כדי לבחון את מסגרות התכנון והבדיקה וללמוד כיצד הן מתפתחות לאורך זמן.</p>	<p>2. אירועים מפריעים במסגרת תוכנית השחזור</p>

מדוע זה חשוב	תיאור הפיקוח	כותרת פיקוח
<p>עסקים מצופים לקבוע תוכניות שחזור מתועדות ולהשלים את האימות, כדי להבטיח ל-Barclays שהתוכניות פועלות כמתוכנן וכוללות את כל יחסי התלות כדי להוכיח שניתן לספק את רמות השירות המוסכמות ושהשירותים עומדים בדרישות העמידות שנקבעו על-ידי Barclays.</p>	<p>הספק חייב לשמור על תוכניות התאוששות לאירועי השיבוש המוגדרים שלו כדי לתמוך ביעדי ההתאוששות שלו.</p> <p>על תוכניות השחזור לתעד את שלבי השחזור המפורטים ואת תגובת הספק במסגרת תוכניות ההתאוששות כדי שניתן יהיה למתן את ההשפעה ו/או למנוע פגיעה באספקת השירות ל-Barclays.</p> <p>יש לטפל בתחומים הבאים לכל הפחות:</p> <ul style="list-style-type: none"> ▪ דרכים אפשריות לעקיפת הבעיה. ▪ פרוטוקולי החלטה. ▪ תקשורת ותחומים עסקיים בעדיפות לחידוש/שימור רמת שירות בת-קיימא מינימלית. ▪ יחסי תלות. <p>יש לבדוק ולאמת את תוכניות ההתאוששות כל 12 חודשים או במקרה של שינוי מהותי, כדי לוודא שניתן לספק רמות שירות מוסכמות ולהבטיח שהשירותים עומדים בדרישות קטגוריית העמידות, כפי שנקבעה על ידי Barclays.</p> <p>אם תוכנית כלשהי מאפשרת לעמוד ברמות השירות המוסכמות או בדרישות קטגוריית העמידות החלה, נדרש הספק להודיע על כך באופן מיידי ל-Barclays (בדרך כלל, עד 10 ימים) ולספק תוכניות תיקון מפורטות (לרבות פעולות שיש לבצע ותאריכי סיום הולמים).</p>	<p>3. תכנון התאוששות עסקית ודרישת אימות</p>
<p>תרגול משותף עוזר להבטיח את קיומם של פרוטוקולים הולמים לתכנות ההתאוששות, תוך אימוץ אסטרטגיות תקשורת יעילות ואף מאפשרים, הן לספקים והן ל-Barclays, לנקוט בתגובה מתואמת לניהול הפרעות לפעילות העסקית השוטפת ומזעור ההשפעה על לקוחות Barclays ועל מערכות פיננסיות רחבות יותר.</p> <p>יש דרישות רגולטוריות מ-Barclays לבצע בדיקת המשכיות עסקית עם ספקי שירות של צד שלישי.</p>	<p>על מנת להבטיח כי יחסי תלות בין Barclays לבין שירותי הספק מובנים בהקשר של התאוששות השירות, על הספק, בהתאם לבקשה של Barclays ובתאריך מוסכם מחדש, ליטול חלק בבדיקה משולבת שנועדה לאמת את רמת העמידות/המשכיות של יחסי התלות בין הספק ל-Barclays.</p> <p>Barclays לא תבקש לבצע בדיקה כגון זה יותר מפעם אחת כל שנתיים, אלא אם בדיקות משולבות קודמות הצביעו על חסרונות מהותיים או במקרה של תקרית שהובילה לשיבוש באספקת השירותים.</p>	<p>4. דרישות בדיקה משולבת</p>
<p>היעדר תוכניות התאוששות מערכת או אי תאימות של תוכניות כאלה עלול להוביל לאובדן בלתי מתקבל על הדעת של שירות טכנולוגי המסופק ל-Barclays או ללקוחותיה בשל תקרית. יש להבטיח שכל מסמכי התייעוד של רמת העמידות עדכניים ולקיים תרגולות כדי להבטיח שתוכניות ההתאוששות תואמות לצרכים העסקיים.</p>	<p>על הספק ליישם תוכנית שחזור מערכת המפרטת את הפעולות הנדרשות לשחזור המערכות שהוא מפעיל והחזרתן למצב תפעולי תקין לאחר ההפרעה. יש לבדוק ולאמת את התוכניות כדי להוכיח (בהתאם לראיות) שניתן לשחזר את המערכת במסגרת יעד זמן ההתאוששות ויעד נקודת ההתאוששות המוגדרים, כנדרש בהתאם לקטגוריית העמידות של Barclays שנקבעה.</p> <p>עבור מערכות שכוללות תצורה אקטיבית/פסיבית, יש להפעיל את הסביבה הפסיבית ולהשתמש בה כסביבת ייצור של BAU למשך פרק זמן ארוך מספיק שיאפשר להוכיח יכולת ואינטגרציה פונקציונלית מלאה. (שבוע לכל הפחות)</p>	<p>5. תוכניות שחזור מערכת ודרישת אימות</p>

מדוע זה חשוב	תיאור הפיקוח	כותרת פיקוח
	<p>לשירותים שכוללים תצורה פעילה/פעילה, יש צורך לבצע אימות כדי להוכיח את היכולת להמשכיות תפעולית במקרה של אובדן צומת, מופע או אזור זמינות (במקרה של אירוח בענן) במערכת (לפרק זמן של 60 דקות לכל הפחות).</p> <p>דרישות תדירות האימות מוגדרות במסגרת קטגוריית העמידות שנקבעה עבור המערכת. עיין במטריצת ביקורת העמידות.</p>	
<p>אובדן נתונים הוא אחד האיומים הגדולים ביותר העומדים בפני Barclays – הוא עלול להתרחש בשל פעולות זדוניות או בשל כשל מערכת. יישום תכנון הולם שנועד להתמודד עם תרחיש כזה הוא קריטי ואף עוזר לזהות ולהבין מהם מקורות הנתונים ואת מהות יחסי התלות.</p>	<p>על הספק ליישם תוכניות שחזור נתונים עבור כל המערכות טכנולוגיות שתומכות באספקת השירותים ל-Barclays. יש לבדוק את התוכניות כדי להבטיח רמת דיוק הולמת לפחות פעם אחת בכל 12 חודשים או במקרה של שינוי מהותי ואף לשקול, לכל הפחות, את התחומים הבאים:</p> <ul style="list-style-type: none"> ▪ מקורות זרימת נתונים (במעלה ובמורד הזרם) ▪ מקורות גיבוי ושכפול ▪ דרישות סנכרון נתונים לאחר שחזור <p>על הספק לבדוק ולאמת את תוכניות שחזור הנתונים עבור כל המערכות הטכנולוגיות שתומכות באספקת השירותים ל-Barclays ולהוכיח (בהתאם לראיות) שהתהליך מאפשר שחזור נתונים למצב תפעולי צפוי, במסגרת יעדי נקודות השחזור הנדרשים.</p>	<p>6. תוכניות שחזור נתונים ודרישות אימות</p>
<p>יש לפרוס מערכות טכנולוגיות במרכזי נתונים שונים כדי להתגונן מפני השבתת פעילות של מרכז הנתונים. דרישה זו גם חלה על מערכות המתארחות אצל ספק שירותי ענן – כשל אזורי.</p>	<p>על הספק לוודא את רמת העמידות של כל מערכת טכנולוגית הדרושה לצורכי אספקת השירות ל-Barclays במרכז הנתונים ולהבטיח שהיא רחוקה מספיק מבחינה גאוגרפית כדי להפחית את הסיכון ששני מרכזי נתונים יושפעו בו-זמנית מאירוע יחיד.</p> <p>כשמערכת טכנולוגית מתארכת אצל ספק שירותי ענן, יש להבטיח את זמינות המערכת באזורי זמינות שונים כדי להפחית את הסיכון להשבתת פעילות AZ. מערכות קריטיות נדרשות להדגים יכולות התאוששות מכשלים באזור של ספק שירותי הענן.</p>	<p>7. גיוון במרכז הנתונים ודרישות מספק שירותי ענן</p>
<p>יש להקפיד שהשירותים הטכנולוגיים והסדרי התמיכה כוללים תוכניות התאוששות מתאימות, המאפשרות להתמודד עם אירועי סייבר או עם אירועי שלימות נתונים.</p>	<p>על הספק ליישם תוכנית בנייה מחדש של פלטפורמות ואפליקציות עבור כל מערכת טכנולוגית הדרושה לצורכי אספקת השירות ל-Barclays ולהכפיף לבדיקה, אישור ובחינה לפחות פעם אחת בכל 12 חודשים או במקרה של שינוי מהותי.</p> <p>תוכניות אלה מיועדות להתמודד עם מצבים שבהם לא ניתן להשתמש באפשרויות שחזור/התאוששות מסורתיות ויש לבנות שוב את המערכת מן היסוד.</p> <p>על התוכנית לכלול את התחומים הבאים:</p> <ul style="list-style-type: none"> ▪ מערכת הפעלה/תוכנת תשתית ▪ פריסה והגדרת תצורה של אפליקציות 	<p>8. דרישת לגבי תוכניות בנייה מחדש של פלטפורמות ואפליקציות</p>

מדוע זה חשוב	תיאור הפיקוח	כותרת פיקוח
	<ul style="list-style-type: none"> ▪ הגדרות תצורה/אמצעי פיקוח של מסגרות אבטחה ▪ יחסי תלות של המערכת האקולוגית וביצוע מחודש של אינטגרציה ▪ דרישות נתונים (תוכנית שחזור נתונים) ▪ התאמת יחסי התלות לביצוע ולתזמון תוכניות ההתאוששות ▪ שחזור מישור בקרה (למשל Active Directory) <p>אימות של התוכנית חייב להיות מוכח לפחות באמצעות תרגיל שולחני (Table-Top Exercise) כדי להוכיח היתכנות.</p>	