בנק ישראל
הפיקוח על הבנקים
אגף מדיניות ואסדרה

ה' בכסלו תשע"ט
13 בנובמבר 2018
חוזר ח- 06- 2579

לכבוד
התאגידים הבנקאיים וחברות כרטיסי אשראי

הנדון: מחשוב ענן

(ניהול בנקאי תקין הוראות מס' 357, 362)

מבוא

1. הוראת ניהול בנקאי מס' 362 בנושא "מחשוב ענן" (להלן: "ההוראה"/"הוראת מחשוב ענן") דורשת מהתאגידים הבנקאיים לפנות לפיקוח במקרים מסויימים בבקשת היתר, וזאת לפני שימוש בטכנולוגיות מחשוב ענן. בשנה שחלפה ממועד הפצת הוראת מחשוב ענן, בחן הפיקוח על הבנקים מספר חלופות בנוגע לצורך בדרישת היתר כאמור והגיע למסקנה שניתן להקל על התאגידים בענין זה ולפטור אותם מהצורך בהיתר, בין היתר מהסיבות הבאות:
   1.1. שיפור ובשלות של כלי הגנת הסייבר ואבטחת המידע, בד בבד עם צבירת ניסיון בנושא אצל תאגידים בנקאיים המאפשרים את העברת ניהול הסיכונים הנוגעים לטכנולוגיות מחשוב ענן לתאגידים.
   1.2. ההקלה הרגולטורית עולה בקנה אחד עם היעד הפיקוחי לרתום את הטכנולוגיה החדשנית לשיפור התחרות, לשיפור השירותים ללקוחות התאגידים הבנקאיים ולהתייעלותם.
   1.3. שימוש בטכנולוגיות מחשוב ענן, כמו גם בטכנולוגיות מתקדמות אחרות, עשוי לסייע לתאגידים הבנקאיים בקידום החדשנות ושיפור השירותים ללקוחות.
   1.4. רשויות פיקוח על מוסדות פיננסיים בעולם אינם דורשים היתר מראש אלא מבססים את הרגולציה על ניהול סיכונים.

2. עם זאת, הפיקוח לא הסיר את האיסור לעשות שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ו/או מערכות ליבה.

3. תיקון ההוראה כולל הנחיות נוספות לתאגידים ובנוסף מתייחס ל"**מחשוב ענן מהותי**" (ראה סעיף 9.1).

4. מאחר ומחשוב ענן מהווה מקרה פרטי של מיקור חוץ ונוכח ביטול הצורך לפנות מראש לקבל היתר עבור יישום טכנולוגיות מחשוב ענן, בוטל הצורך לקבל הסכמה של המפקח גם במקרה של אחסון מידע מכל סוג שהוא של לקוחות התאגיד הבנקאי במערכות אשר אינן בשליטתו ועל כן **סעיף 17 ב (2) בהוראה 357**- בטל.

התיקונים להוראה

5. **סעיף 3 להוראה בגרסה הקודמת** – בוטל.
6. נוספו הוראות ניהול בנקאי תקין שהופצו בשנה האחרונה 363 ("ניהול סיכוני סייבר בשרשרת אספקה") והוראה 359A ("מיקור חוץ") ושיש לפעול גם בהתאם אליהן (**סעיף 7 להוראה**).
7. התאגיד הבנקאי ייבחן את הצורך בהסתייעות, לפי העניין, ביועצים חיצוניים מומחים בהפחתת הסיכונים הגלומים בשימוש בטכנולוגיות ענן (**סעיף 9 להוראה – הוחלף המונח "ייבחן להסתייע" ב- "הצורך בהסתייעות"**).

פרק ג': ממשל תאגידי (סעיף 10 -13 (ב) להוראה)

ההנחיות בנושא דירקטוריון והנהלה בכירה הופרדו להנחיות עבור הדירקטוריון (**סעיפים 10 עד 13 להוראה**) ולהנחיות עבור ההנהלה (**סעיפים 13 (א) עד 13 (ב) להוראה**).

דירקטוריון

8. דירקטוריון התאגיד הבנקאי נדרש להנחות את ההנהלה לגבש ולאשר מסמך מדיניות לשימוש בטכנולוגיות מחשוב ענן (**סעיף 10 (ב) להוראה** – הוסר המונח "**לפי העניין**").
9. התיקון כולל שתי הנחיות חדשות לדירקטוריון התאגיד הבנקאי:
   9.1. לאשר כל יישום **מחשוב ענן מהותי** (**סעיף 12 להוראה**). דוגמאות למחשוב ענן מהותי מובאות בנספח א' להוראה.
   9.2. לוודא כי השימוש בטכנולוגיות מחשוב ענן נעשה ע"פ המדיניות שנקבעה ע"י הנהלת התאגיד הבנקאי. (**סעיף 13 להוראה**).

הנהלה בכירה

10. התיקון מוסיף לתכולת המדיניות לשימוש בטכנולוגיות מחשוב ענן שעל הנהלת התאגיד הבנקאי לגבש, גם את סוגי היישומים בהם נדרש **אישור של הדירקטוריון** ("מחשוב ענן מהותי") וכן את סוגי היישומים הדורשים אישור הנהלה בלבד (**סעיף 13 (א) להוראה**).
11. **סעיף 13 (ב) להוראה** – מחליף את סעיף 11 להוראה בגרסה הקודמת.

פרק ד': יישומי מחשוב ענן המחייבים קבלת היתר (סעיפים 14 - 17 להוראה בגרסה הקודמת) – בוטל.

פרק ה': ניהול סיכונים (סעיף 17 (א) -22 להוראה)

12. ההנחיות בתהליך ניהול והערכת הסיכונים מתייחסות ל- "**מחשוב ענן מהותי**" **(סעיף 21-18 להוראה).**

פרק ו': הסכם התקשרות עם ספק שירותי הענן (סעיף 24-23 להוראה)

13. **במחשוב ענן מהותי** בנוסף להוראת ניהול בנקאי תקין מס' 357, נדרש התאגיד הבנקאי, בהסכם ההתקשרות עם הספק, לעמוד גם בהוראת ניהול בנקאי תקין מס' 363 **(סעיף 23 להוראה).**

14. התיקון מוסיף עוד שתי התחייבויות של הספק שאמורות להיכלל בהסכם ההתקשרות עם התאגיד הבנקאי, בין היתר:

14.1. מתן אפשרות לתאגיד הבנקאי, על בסיס הערכת הסיכונים, לבצע ביקורות אצל ספק מחשוב הענן (**סעיף 23 ג' להוראה**).

14.2. מתן אפשרות לפיקוח על הבנקים לבצע ביקורות אצל ספק שירות הענן כאשר מדובר במחשוב ענן מהותי (**סעיף 23 ד' להוראה**).

פרק ז' : מכתב ההיתר (סעיפים 25 - 26 להוראה בגרסה הקודמת) – בוטל.

פרק ח': דיווח לפיקוח (סעיף 27 א' ו27 ב' להוראה)

15. התיקון דורש מהתאגידים הבנקאיים להעביר לפיקוח על הבנקים בכתב, אחת לשנה (בסיום שנה קלנדרית) שני סוגי דיווחים:

15.1. רשימה מעודכנת של יישומי מחשוב הענן שהתאגיד הבנקאי יישם ממועד הדיווח האחרון, לרבות מועד היישום ושם ספק שירותי הענן. כמו כן, בהתייחס **ל- "מחשוב ענן מהותי"**, הרשימה צריכה לכלול גם את מיקומם הגיאוגרפי של שרתי הענן **(סעיף 27 א' להוראה)**.

15.2. דיווח על יישומי מחשוב ענן עתידיים שהתאגיד הבנקאי מתכנן ליישם. הפיקוח ישקול לפי הצורך לבחון פרטים בדיווח כגון, שם הספק ומיקום השרתים כדי להתייחס לסיכון סיסטמי פוטנציאלי העלול להיגרם כתוצאה מריכוז יישומים של המגזר הבנקאי אצל אותו ספק ובאותו אתר (**סעיף 27 ב' להוראה**). הדיווח יכלול את כל היישומים המתוכננים.

נספחים

16. בהוראה זו נוסף נספח חדש. נספח א' שבהוראה הקודמת שונה **לנספח ב'** ונוסף **נספח א' חדש** להוראה הנוכחית.

17. התיקון כולל נספח המפרט דוגמאות **ל"מחשוב ענן מהותי"**. הדוגמאות מתייחסות למקרים עבורם נדרש בעבר התאגיד הבנקאי לפנות לפיקוח בבקשת היתר **(נספח א' להוראה)**.

18. נוספו היבטים רלבנטיים לנספח שמפרט דוגמאות להיבטי מחשוב ענן שיש לקחת בחשבון בהערכת סיכונים **(נספח ב' להוראה)**.

תחילה

19. תחילת התיקונים להוראה החל מיום פרסומם.

עדכון הקובץ

20. מצ"ב דפי עדכון לקובץ ניהול בנקאי תקין, להלן הוראות העדכון:

להוציא עמוד	להכניס עמוד
357-1-14 [7] (7/16)	357-1-15 [8] (11/18)
362-1-9 [1] (7/17)	362-1-10 [2] (11/18)

בכבוד רב,

ד"ר חדוה בר

המפקחת על הבנקים

ניהול טכנולוגיית המידע

תוכן העניינים

פרק א': כללי

מבוא

1. (א) מערך טכנולוגיית המידע הוא מרכיב מרכזי בתפעול ובניהול התקין של תאגיד בנקאי, לאור היותו של המידע, על כל היבטיו והשלכותיו, בעל השפעה מכרעת על יציבות התאגיד הבנקאי והתפתחותו.

(ב) בשל גורמים אלו על הנהלת תאגיד בנקאי לייחס את החשיבות הראויה, הן בהירכיה הניהולית והן במשאבים הכספיים ומשאבי האנוש הנחוצים, לניהול תקין של מערך טכנולוגיית המידע.

(ג) מבלי לפגוע בכלליות האמור לעיל, נקבעה הוראה זו הכוללת הנחיות פרטניות וכלליות.

(ד) הוראה זו תואמת את העקרונות בתחום הבנקאות האלקטרונית, שפירסמה הועדה הבינלאומית לפיקוח על הבנקים (ועדת באזל) ביולי 2003.

תחולה

2. הוראה זו תחול על תאגידים בנקאיים, וכן על תאגידים כאמור בסעיפים 11(א)(3א), 11(א)(3ב) ו-11(ב) לחוק הבנקאות (רישוי), התשמ"א-1981 שהואגדו בישראל (להלן: תאגיד בנקאי).

פרק ב': פיקוח וניהול

דירקטוריון

3. (א) דירקטוריון של תאגיד בנקאי יקיים דיון תקופתי ויקבע את מדיניות ניהול טכנולוגיית המידע של התאגיד הבנקאי, בהתאם לאמור בסעיף 6(ד) להוראת ניהול בנקאי תקין מס' 301 (דירקטוריון).

(ב) מדיניות ניהול טכנולוגיית המידע תכלול, בין היתר, התייחסות ל:

(1) אבטחת מידע;

(2) עקרונות גיבוי והתאוששות במצבים של תקלות ואסונות;

(3) מיקור חוץ;

(4) מדיניות פיתוח, לרבות על-ידי משתמשי קצה;

(5) בטל;

הנהלה

4. (א) הנהלת תאגיד בנקאי תמנה מנהל אחד שיהיה חבר הנהלה או כפוף למנכ"ל, אשר יישא באחריות למכלול נושאי טכנולוגיית המידע (להלן: מנהל טכנולוגיית המידע). מנהל זה יהיה בעל הכשרה מקצועית מתאימה וניסיון מוכח בתחום טכנולוגיית המידע וניהולו.

(א1) על אף האמור בסעיף קטן (א), המפקח על הבנקים רשאי להתיר, במקרים חריגים, למנהל טכנולוגיית המידע בתאגיד הבנקאי לשמש מנהל טכנולוגיית המידע גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(3א), 11(א)(3ב), ו-11(ב) לחוק הבנקאות (רישוי).

(ב) הנהלת תאגיד בנקאי תמנה מנהל אבטחת מידע, כמפורט בסעיף 9.

(ג) הנהלת תאגיד בנקאי תקיים דיון שנתי ביישום מדיניות ניהול טכנולוגיית המידע ותקצובה, ותקבל את ההחלטות הנגזרות, תוך הבחנה בין נושאים רלבנטיים לטווח הקצר לבין נושאים רלבנטיים לטווח הארוך.

(ד) הנהלת תאגיד בנקאי תייחד דיון שנתי ליישום מדיניות אבטחת המידע על כל היבטיה.

(ה) בקביעת המבנה הארגוני של היחידה המופקדת על ניהול טכנולוגיית המידע בתאגיד הבנקאי, ובהגדרת התפקידים של עובדי יחידה זו, תקיים הנהלת התאגיד הבנקאי הפרדת תפקידים וסמכויות נאותה.

(ו) הנהלת תאגיד בנקאי תגדיר את סוגי הפעילויות והאירועים שלגביהם יש לספק התראה להנהלה ולגורמים מוסמכים אחרים, לרבות אלו המחייבים התראה בזמן אמת.

נהלים

5. תאגיד בנקאי יקבע נהלים מפורטים לכל שלב ולכל תהליך המטפלים בניהול, תפעול, אבטחה, גיבוי, שרידות ובקרה של טכנולוגיית המידע, ויקיים בקרה נאותה על ביצועם. נהלים אלה יעודכנו באופן שוטף בהתאם לשינויים החלים הן בסביבה העסקית הרלבנטית והן בסביבה הטכנולוגית.

תיעוד, רישום ומעקב

6. (א) תאגיד בנקאי יקיים תיעוד מתאים ועדכני למערך טכנולוגיית המידע שלו.

(ב) (1) תאגיד בנקאי יקיים נתיב ביקורת שיתבסס על רישום ממוכן (log) של עצם הגישה ושל פעולות ושאילתות המבוצעות במערכות המידע של התאגיד הבנקאי, אשר יכלול, בין היתר, את זיהוי מורשה הגישה, המקום, הזמן וכן פרטים על נשוא הגישה.

(2) על אף האמור בפסקה (1) לעיל, לגבי שאילתות של עובדי התאגיד הבנקאי יקיים התאגיד הבנקאי נתיב ביקורת על פי שיקול דעתו, תוך התבססות על הערכת הסיכונים.

(3) תאגיד בנקאי יקבע את פרק הזמן לשמירת הרישומים כאמור בפסקה (1), ובלבד שפרק הזמן לשמירת הרישומים לא יקטן מ- 60 יום לרישומי שאילתות ו-6 חודשים לרישומי פעולות.

(ג) תאגיד בנקאי יידע את לקוחותיו ואת עובדיו לגבי עצם קיומם של הליכי שמירה של פעולותיהם.

(ד) בכפוף לאמור בסעיף 4(ו), מערכות ניהול הרישומים תספקנה לגורמים המוסמכים לכך, התראות על פעילויות חיצוניות בלתי מורשות וכן על פעילויות חריגות של המשתמשים לסוגיהם.

ביקורת פנימית

7. (א) תאגיד בנקאי יכלול, במסגרת הביקורת הפנימית שלו, יחידה ארגונית לביקורת טכנולוגיית המידע שלו. האחראי על הביקורת הפנימית בתחום טכנולוגיית המידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים לביצוע הביקורת בתחום זה.

(ב) תאגיד בנקאי יעמיד לרשות הביקורת הפנימית את הכלים הדרושים לביצוע ביקורת ובקרה בסביבת מערך טכנולוגיית המידע.

(ג) בכל מקרה בו נעשה שימוש במיקור חוץ של ביקורת פנימית בתחום טכנולוגיית המידע, יש לשמור על יכולת ההערכה בידי הביקורת הפנימית של התאגיד הבנקאי.

פרק ג': <u>סיכונים</u>

הערכת סיכונים

8. (א) הנהלת תאגיד בנקאי תבצע הערכת סיכונים (Risk Assessment) של מערך טכנולוגיית המידע. על הערכת הסיכונים להתייחס למכלול הסיכונים הפוטנציאליים הקשורים בניהול מערך טכנולוגיית המידע, כגון:

- משתמשי המערכת הפנימיים והחיצוניים לתאגיד הבנקאי;
- סביבת המערכת;
- פעילות המערכת והשלכותיה על עסקי התאגיד;
- רגישות המידע;
- מיקור חוץ.

(ב) תהליך הערכת הסיכונים יהיה מתמשך, והערכת הסיכונים תתעדכן בהתאם לשינויים בגורמי הסיכון השונים.

(ג) בהתאם להערכת הסיכונים על התאגיד הבנקאי לנקוט באמצעים הנדרשים למזעור אפשרות פגיעה במערך טכנולוגיית המידע על כל חלקיו, ומזעור נזק פוטנציאלי.

פרק ד': אבטחת מידע

מנהל אבטחת מידע

9. (א) (1) מנהל אבטחת מידע יהיה כפוף לחבר הנהלה של התאגיד הבנקאי.

(1א) על אף האמור בסעיף קטן (1), המפקח על הבנקים רשאי להתיר, במקרים חריגים, למנהל אבטחת המידע בתאגיד הבנקאי לשמש מנהל אבטחת המידע גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(3א), 11(א)(3ב), ו-11(ב) לחוק הבנקאות (רישוי).

(2) מנהל אבטחת מידע לא יעסוק בתפקידים ביצועיים אשר עלולים לגרום ניגוד עניינים, ובכלל זה לא ישמש כמנהל טכנולוגיית המידע.

(3) הנהלת תאגיד בנקאי תקבע את תחומי אחריותו של מנהל אבטחת המידע ואת הנושאים שהחלטות לגביהם טעונות התייחסותו. תחומי אחריותו יכללו, בין היתר:

- אחריות כוללת ליישום מדיניות אבטחת המידע בתאגיד הבנקאי;
- פיתוח ומעקב של יישום תוכניות אבטחת המידע בתאגיד הבנקאי ובחינה של אפקטיביות מערכת אבטחת המידע;
- טיפול באירועים חריגים בתחום אבטחת המידע.

(4) הנהלת תאגיד בנקאי תעמיד לרשות מנהל אבטחת המידע את המשאבים הדרושים למילוי תפקידו.

(ב) מנהל אבטחת מידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים בתחום עיסוקו.

אבטחת מידע

10. (א) הנהלת תאגיד בנקאי תרכז את עקרונות אבטחת המידע במסמך כתוב, אשר יובא לאישור הדירקטוריון. מסמך זה יעודכן אחת לתקופה.

(ב) תאגיד בנקאי יישם אמצעי אבטחה - פיזית ולוגית, למניעה, גילוי, תיקון ותיעוד של חשיפות במערך טכנולוגיית המידע ודיווח עליהם, בהתאם להערכת הסיכונים ותוך התייחסות גם להיבטים הבאים:

(1) זיהוי ואימות (Identification & Authentication);

(2) סודיות ופרטיות (Privacy);

(3) שלמות ומהימנות של הנתונים (Integrity);

(4) מניעת הכחשה (Non Repudiation).

(ג) תאגיד בנקאי ינהל מעקב שוטף אחר ההתפתחויות הטכנולוגיות, ויתאים את רמת האבטחה ובקרת הגישה למערכותיו על פי השינויים ברמת הסיכונים הנגזרים משינויים טכנולוגיים אלו.

(ד) תאגיד בנקאי יפעל להפרדת סביבת הייצור (Production) מסביבת הפיתוח והניסוי (Test).

סקר בטיחות וניסיונות חדירה מבוקרים

11. (א) (1) אחת לתקופה, בהתאם להערכת הסיכונים, ייזום מנהל אבטחת המידע סקר בטיחות של מערך טכנולוגיית המידע של התאגיד הבנקאי (להלן: הסקר). בסקר שיבוצע תוערך האפקטיביות של אמצעי ההגנה, בהתייחס להערכת הסיכונים, ויוצעו דרכים לתיקון הליקויים שיימצאו.

(2) לגבי מערכות שהוגדרו על-ידי התאגיד הבנקאי כבעלות סיכון גבוה, לרבות מערכות בנקאות בתקשורת, יש לערוך סקר במתכונת כאמור בפיסקה (1) לעיל לפני הטמעת שינויים משמעותיים במערכות אלו, כאשר חלו שינויים משמעותיים בסביבה הטכנולוגית בה המערכות פועלות, וכן לקראת הכנסתן לשימוש של מערכות חדשות כאמור, ולפחות אחת ל-18 חודשים.

(3) תוצאות הסקר יכללו דוח מפורט על הממצאים וההמלצות, ותמצית ניהולית שתציג את עיקרי הדברים.

(ב) מנהל אבטחת מידע ייזום ניסיונות חדירה מבוקרים למערך טכנולוגיית המידע של התאגיד הבנקאי לבחינת עמידותו בפני סיכונים פנימיים וחיצוניים. פעולה זו תיעשה בתדירות ההולמת את הסיכונים הספציפיים של המערכות השונות, בהתאם להערכת הסיכונים.

(ג) (1) סקר הבטיחות וניסיונות החדירה המבוקרים, כאמור לעיל, ייערכו על ידי גורמים מקצועיים, עצמאיים, בלתי תלויים, חיצוניים לתאגיד הבנקאי, תוך מניעת ניגודי עניינים ונקיטת אמצעי הזהירות המתחייבים.

(2) הנהלת תאגיד בנקאי תשלים את דיוניה בממצאי סקר הבטיחות וניסיונות החדירה המבוקרים והשלכותיהם, ותקבל את ההחלטות המתחייבות, לרבות קביעת לוח זמנים ליישומן, תוך פרק זמן סביר לאחר מועד תחילת ביצועם.

(ד) ממצאים מהותיים שעלו בסקר הבטיחות ובנסיונות החדירה המבוקרים יובאו לידיעת הדירקטוריון או ועדה דירקטוריונית מתאימה.

בקרת גישה

12. (א) (1) תאגיד בנקאי יבצע זיהוי אישי חד-ערכי של כל גורם בעל גישה למערכת מידע (להלן: מורשה גישה) כתנאי מוקדם למתן הגישה.

(2) על אף האמור בפסקה (1) לעיל, במקרים חריגים של ספקים ועובדים בהם לא ניתן לקיים את האמור לעיל, יישם התאגיד הבנקאי אמצעים חלופיים מתאימים.

(ב) (1) תאגיד בנקאי יקבע כללים וכלים לזיהוי ולמתן הרשאות לגורמים שונים לרכיבי טכנולוגיית המידע. כללים אלו יביאו בחשבון את רמות הסיכון הנגזרות מטווח האחריות והסמכות של המשתמשים (על-פי סיווג לקבוצות), מהיישום עצמו, מרגישות המידע ומשאר רכיבי טכנולוגיית המידע.

(2) הסיווג לקבוצות משתמשים יתייחס לגורמים הפנימיים בתאגיד הבנקאי ולגורמים החיצוניים (לרבות לקוחות, ספקים וכו').

(3) תאגיד בנקאי יפעיל כלים לניהול ולבקרה של מערכת ההרשאות.

(4) אמצעי הגישה למערכות המידע יהיו בטכניקות מקובלות לעניין זה.

(ג) (1) לצורך בקרת גישה למערכות מידע שהוערכו כבעלות סיכון גבוה, ובכל מקרה של גישה מרחוק למערך טכנולוגיית המידע של התאגיד הבנקאי על ידי עובדים, ספקים ונותני שירותים, ישתמש התאגיד הבנקאי בטכנולוגיה המשלבת זיהוי ואימות של המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה.

(2) על אף האמור בפיסקה (1) לעיל, רשאי תאגיד בנקאי להשתמש בטכנולוגיה חלופית במקרים הבאים:

- במערכות בסיכון גבוה שלא באמצעות גישה מרחוק, על פי שיקול דעתו של התאגיד הבנקאי, שתתועד בכתב;
- בגישה מרחוק של ספקים ונותני שירותים, כאשר שימוש בטכנולוגיה כאמור אינו אפשרי מסיבות שאינן תלויות בתאגיד הבנקאי.

(ד) תאגיד בנקאי יקבע קריטריונים להפעלת מנגנון ניתוק התקשורת (Time-out) לאחר פרק זמן שבו לא היתה פעילות מצד מורשה הגישה. פרק הזמן ייקבע תוך התחשבות בהערכת הסיכונים.

(ה) על אף האמור בסעיפים (א) – (ג) לעיל, על לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת" יחולו הסעיפים הרלבנטיים בהוראה זו.

הצפנה

13. תאגיד בנקאי יבחן את הצורך בהצפנה של נתונים, לרבות בתווך התקשורת, במערכות שהוגדרו בהתאם להערכת הסיכונים כבעלות סיכון גבוה, ובלבד שבמקרים הבאים תתקיים הצפנה:

(א) בטל.

(א1) בטל.

(ב) גישה מרחוק למחשב התאגיד הבנקאי, בכפוף לאמור בסעיף 12(ג). האמור בסעיף זה אינו חל על חל לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת".

(ג) סיסמאות של מורשי גישה.

קישוריות התאגיד הבנקאי לאינטרנט

14. (א) תאגיד בנקאי ינקוט באמצעים לאיתור התחזות לאתר האינטרנט שלו, ויספק ללקוח כלים מתאימים לוודא את זהות האתר של התאגיד הבנקאי.

(ב) קישוריות התאגיד הבנקאי לאינטרנט תיעשה במקרים הבאים בלבד:

(1) קישוריות עובדים לאינטרנט, כמפורט בסעיפים קטנים (ג) ו- (ד);

(2) מתן שירותי בנקאות בתקשורת, כמפורט בהוראת ניהול בנקאי תקין מספר 367;

(3) שימוש אחר שאושר מראש על-ידי המפקח, כאמור בסעיף 30(א).

(ג) הנהלת תאגיד בנקאי תקבע את השימושים המותרים לעובדי התאגיד הבנקאי באמצעות קישוריות לאינטרנט, על פי הערכת סיכונים ותוך נקיטת אמצעי בקרה נאותים ובכפוף לאמור בסעיף קטן (ד).

(ד) קישוריות עובדי התאגיד הבנקאי לאינטרנט מתחנות עבודה תתאפשר בהתקיים אחד מאלה:

(1) תחנת העבודה קשורה אך ורק לאינטרנט או לרשת שקשורה אך ורק לאינטרנט (Stand Alone) ושאין עליה יישומים בנקאיים או מידע רגיש;

(2) הקישוריות לאינטרנט תיעשה באמצעות שרת נפרד של התאגיד הבנקאי, ותבוקר באופן שוטף על ידי האמצעים האמורים בסעיף קטן (ה). בתצורה זו, הקישוריות לאינטרנט תבוצע לצורכי גלישה ודואר אלקטרוני בלבד;

(ה) בהתאם לאמור בסעיף 10(ג), קישוריות של רשת התאגיד הבנקאי לאינטרנט תאובטח לפחות על-ידי אנטי וירוס, מסנני תוכן (Content-Filtering), מערכת לאיתור ניסיונות חדירה (IDS) ו- Firewall.

(ו) התאגיד הבנקאי יישם, על פי הערכת הסיכונים, אמצעים ממוכנים לבקרת אפליקציה ולסריקת חולשות המערכת.

(ז) האמור בסעיפים קטנים (ה) ו- (ו) יחול על כל אתרי התאגיד הבנקאי, לרבות האתר השיווקי.

פרק ה': גיבוי והתאוששות

דיון בהנהלה

15. (א) אחת לתקופה תקיים הנהלת תאגיד בנקאי דיון בעקרונות הגיבוי וההתאוששות ותקבל החלטות בתחום זה, תוך התייחסות מפורטת להערכת הסיכונים ולעניינים הבאים:

(1) הגדרת מצבי תקלות (לרבות אצל ספקי התאגיד הבנקאי) ואסונות (לרבות אסונות טבע, שריפות, מלחמה ושעת חירום) עבור מכלול היחידות הארגוניות, והשלכותיהם על המשך הפעילות של התאגיד הבנקאי;

(2) קביעת התהליכים העסקיים החיוניים גם במצבי תקלות ואסונות, מערכות המידע הרלבנטיות לתפעולם ואופן תפעולן של מערכות אלו במצבים כאמור;

(3) רכיבי התוכנה, החומרה והתקשורת השונים;

(4) היבטי הגיבוי וההתאוששות, לרבות התייחסות לגיבוי שוטף, משך הגיבוי, תדירות הגיבוי, מדיית הגיבוי, זמני השבתה מרביים, ותהליך החזרה לשגרת העבודה;

(5) הסתמכות על גורמי חוץ בעת קיומן של הפרעות לפעולה סדירה של מערכות המידע, וזמן ההתאוששות הנחוץ לתאגיד הבנקאי להחזרת מערכות המידע לפעולה סדירה.

(ב) במסגרת הדיון יוחלט על הסדרי הגיבוי השוטף (לרבות גיבוי לכוח אדם ולתיעוד) ועל השקעות במתקני גיבוי ובהסדרי גיבוי אחרים עבור מערכות מהותיות שנקבעו על פי האמור בסעיף קטן (א)(2) לעיל.

הסדרי גיבוי והתאוששות

16. (א) (1) תאגיד בנקאי יקיים תכנית מפורטת להפעלת מערך טכנולוגיית המידע שלו במקרים של תקלות ואסונות (להלן: תכנית התאוששות מאסון), כאמור בסעיף 15.

(2) תאגיד בנקאי יבחן ויעדכן את תכנית ההתאוששות מאסון על-פי השינויים שחלו בתקופה שחלפה מהעדכון הקודם (לרבות שינויים במערך החירום ובהערכת הסיכונים) לפחות אחת לשנתיים וכן בעת ביצוע שינוי מהותי.

(ב) לפחות אחת לשנתיים וכן בעת ביצוע שינוי מהותי במערך החירום, יקיים תאגיד בנקאי ניסוי של כל הסדרי הגיבוי וההתאוששות שלו.

(ג) אחסון גיבויי ציוד, תוכנה ומידע חיוניים יהיה במקום מרוחק ממקום אחסון המקור, כך שאירועים כאסון טבע, מלחמה ודומיהם לא יפגעו בו-זמנית בציוד, בתוכנה ובמידע המקוריים ובגיבוי, ולא ימנעו שימוש בהם.

(ד) תאגיד בנקאי ינקוט באמצעים שיבטיחו אפשרות שחזור מידע מעותקי גיבוי, לרבות מידע שנשמר באמצעים שחדלו לשמש אותו.

פרק ו': <u>מיקור חוץ</u>

מיקור חוץ

17. (א) תאגיד בנקאי רשאי לבצע פעילויות ניהול, עיבוד ואחסון של המידע שלו או פיתוח מערכות, לרבות שירותי יעוץ, ידע ושירותים אחרים, על-ידי גורמים מחוץ לתאגיד הבנקאי (להלן: גורמים חיצוניים).

(ב) על אף האמור בסעיף קטן (א), מיקור חוץ כמפורט להלן טעון הסכמה של המפקח, כאמור בסעיף 30(א):

(1) מיקור חוץ של מערכות הליבה (Core Systems);

(2) בטל;

(3) סעיף זה אינו חל על שירותי מיקור חוץ שמקבל תאגיד בנקאי כאמור בסעיף 11(א) לחוק הבנקאות (רישוי), התשמ"א - 1981, מתאגיד בנקאי השולט בו או מתאגיד עזר שבשליטת התאגיד הבנקאי השולט בו.

(ג) בטל.

(ד) במיקור חוץ מהותי, תאגיד בנקאי יוודא את מהימנותו ואת חוסנו הכלכלי של נותן השירותים, ויבחן מראש את התאמת כישוריו ואת יכולתו לבצע את המטלות.

הסכם התקשרות

18. (א) התקשרות לצורך מיקור חוץ תיעשה בהסכם כתוב.

(ב) במיקור חוץ מהותי, הסכם ההתקשרות יתייחס מפורשות לפחות לנושאים הבאים:

(1) הגדרת תחומי אחריות של כל אחד מהצדדים להסכם, לרבות קבלני משנה;

(2) הסכם רמת השירות (SLA);

(3) חובת הסודיות, אבטחת מידע ומצבי חירום;

(4) הסדרים להפסקת ההסכם וליישוב מחלוקות. בהקשר זה יתייחס ההסכם גם להסדרים שיאפשרו לתאגיד הבנקאי לתפעל ולתחזק את פעילות מיקור החוץ במקרים בהם הגורם החיצוני חדל מלספק את השירות (כגון על-ידי החזקת תוכניות מקור אצל נאמן);

(5) פעילות הגורם החיצוני עבור התאגיד הבנקאי יהיו ניתנות לביקורת מטעמו.

(ג) אין בהוראת סעיף זה בכדי לגרוע מאחריותו של התאגיד הבנקאי לכל פעולה שנעשית מטעמו על ידי גורמים חיצוניים.

פרק ז': <u>שירותי בנקאות בתקשורת</u>

בטל.

פרק ח': שונות

בנק חוץ

29. ההוראה תחול כלשונה על בנק חוץ, למעט השינויים המפורטים להלן:

(א) בכל מקום בהוראה, הביטוי "מערך טכנולוגיית מידע" יוחלף בביטוי "מערך טכנולוגיית המידע המקומי, לרבות הממשקים של מערך זה עם מערך הבנק בחו"ל".

(ב) סעיף 3 יחול על ההנהלה במקום על הדירקטוריון.

(ג) לסעיף קטן 11(א)(3) יתווסף המשפט:

"עותק מהתמצית הניהולית יועבר לידיעת הממונה על אבטחת המידע בבנק האם".

(ד) לסעיף 16 להוראה יתווסף הסעיף הבא:

"(ה) בנק חוץ ישמור בכל עת, במערכות המידע המקומיות בסניפיו בישראל, נתונים מלאים המכילים את כל הפרטים האישיים והמנהליים לגבי בעלי החשבונות, מיופי הכח וזכויות החתימה, וכן את כל היתרות העדכניות של החשבונות המנוהלים בסניפיו בישראל".

(ה) הסעיפים המפורטים להלן יכולים להתבצע על ידי בנק האם, ולא ישירות על ידי בנק החוץ, ובלבד שבנק החוץ יבצע במידת הצורך את ההתאמות הנדרשות כדי לעמוד בסעיפי ההוראה הבאים כלשונם: 5, 6(א), 6(ב), 7, 8(א), 10(א), 10(ב), 12, 13, 14, 16(ד), ובכדי לעמוד בהוראת ניהול בנקאי תקין מספר 367.

(ו) במקרים חריגים, בנק חוץ הסבור כי סעיפים מסוימים בהוראה זו אינם ישימים לגביו, רשאי לפנות למפקח על מנת לתאם תחולתם ו/או דרך יישומם לגביו, כמפורט בסעיף 30(א).

פעולות הטעונות הסכמה ופעולות הטעונות דיווח

30. (א) תאגיד בנקאי המעוניין לבצע את אחת מהפעולות הבאות יודיע מראש למפקח. לא הודיע המפקח לתאגיד הבנקאי, תוך 90 יום, על אי אישור הפעילות, יוכל התאגיד הבנקאי לראות זאת כאישור:

(1) בטל;

(1א) מינוי מנהל טכנולוגיית המידע כמפורט בסעיף 4(א1) ו/או מינוי מנהל אבטחת מידע כמפורט בסעיף 9(א)(1א).

(1ב) בטל.

(2) קישוריות התאגיד הבנקאי לאינטרנט על-פי סעיף 14(ב)(3);

(3) מיקור חוץ כמפורט בסעיף 17(ב);

(4) בטל;

(5) התאמת תחולת סעיפי ההוראה עבור בנק חוץ, כמפורט בסעיף 29(ו).

(ב) תאגיד הבנקאי ידווח למפקח על הבנקים על הנושאים והאירועים הבאים:

(1) אירועים חריגים, לרבות ניסיונות מהותיים של חדירה ותקיפה, חדירות בפועל למערכות מחשב, קריסה של מערכות מרכזיות, הפעלת תכנית החירום של התאגיד הבנקאי וכיוצא באלה;

(2) הפסקה של שירותים מהותיים ללקוחות כתוצאה מהשבתה לא מתוכננת של פעילות מערכות ממוכנות לפרק זמן של יותר מיום עסקים אחד;

(3) הקמת תאגיד עזר שעיסוקו בתחום טכנולוגיית המידע;

(4) החלטה על שינויים מהותיים צפויים במדיניות ניהול טכנולוגיית המידע, הסבה מהותית של מערכות המחשוב ומחשוב מחדש של מערכות מרכזיות ודומיהם;

(5) בטל;

(6) בטל.

(ג) הודעות ודיווחים לפי סעיפים (א) ו-(ב) לעיל יש לשלוח ליחידה למידע ודיווח בפיקוח על הבנקים בבנק ישראל.

(ד) דיווחים לפי סעיפים (ב)(1) ו-(ב)(2) לעיל יש לשלוח בתוך יום עסקים אחד מקרות האירוע נשוא הדיווח. הודעות לפי סעיפים (ב)(3) עד (ב)(6) יש לשלוח 30 יום מראש.

(ה) על אף האמור בסעיפים (ב), (ג) ו – (ד) לעיל, לעניין דיווח על אירוע או חשד לאירוע של תרמית בשירותי בנקאות בתקשורת וכן לגבי אירוע משמעותי הקשור לבנקאות בתקשורת לרבות ניסיונות מהותיים של חדירה וחדירות בפועל, הפסקת שירות של מערכות והונאות במערכות בנקאות בתקשורת, יחולו הוראות הדיווח המפורטות בהוראת ניהול בנקאי תקין מספר 367 בנושא "בנקאות בתקשורת".

* * *

<u>עדכונים</u>

חוזר 06 מס'	**גרסה**	**פרטים**	**תאריך**
830		חוזר מקורי	31/12/79
-----	1	שיבוץ בהוראות ניהול בנקאי תקין	8/91
-----	2	גרסה מחודשת של קובץ ניהול בנקאי תקין	12/95
1890	3	עדכון	27/8/97
2118	4	החלפת הוראה 357 + הוראה 412	14/9/03
2292	5	עדכון	30/1/11
2334	6	עדכון	29/4/12
2507	7	עדכון	21/7/16
2579	8	עדכון	13/11/18

<u>עדכונים הוראה 412 (בנקאות בתקשורת)</u>

חוזר 06 מס'	**גרסה**	**פרטים**	**תאריך**
103/16		חוזר מקורי	25/9/88
-----	1	שיבוץ בהוראות ניהול בנקאי תקין	8/91
-----	2	גרסה מחודשת של קובץ ניהול בנקאי תקין	12/95
1814	3	עדכון	17/4/96

1822	4	עדכון	30/6/96
1889	5	עדכון	27/8/97
2118		ביטול ההוראה	14/9/03

מחשוב ענן

פרק א': רקע

מבוא

1. בשנים האחרונות מתפתחת מגמה של מעבר הולך וגובר לתצורות שונות של מחשוב ענן (Cloud Computing). טכנולוגיות אלו מאפשרות ניצול יעיל ונוח של משאבי מחשוב תוך אפשרות לשיתוף משאבים ולשימוש בהם לפי הצורך; זאת, בד בבד עם חיסכון בעלויות ציוד, שטחי ה- Data Center, חשמל וכד', התורמים למחשוב ידידותי יותר לסביבה (Green Computing).

2. בצד היתרונות הגלומים בשימוש בטכנולוגיות ענן, שימוש בטכנולוגיות אלו עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מהותיים הקשורים לאבטחת מידע וסייבר, המשכיות עסקית, שליטה ובקרה על נכסי ה- IT, וכד'. סיכונים אלו נגזרים, בין היתר, מתלות בספקים או טכנולוגיות ספציפיים; כלי ניהול, אבטחה, שליטה ובקרה שטרם הבשילו; קשיים בהגנה על המידע וביישום בקרות נאותות; העצמת הנזק הפוטנציאלי במקרה של כשל, במיוחד כאשר נוצרות נקודות כשל יחידות (Single Points of Failure); רגישות הרכיבים הייעודיים של הטכנולוגיה; קושי בהפרדת תפקידים ועוד. נציין כי סיכונים אלו בחלקם אמנם מוכרים, אך נוכח המאפיינים הספציפיים של טכנולוגיות אלו והעובדה שמדובר בטכנולוגיות מתפתחות וכלי אבטחת מידע שאינם בהכרח בשלים, גלומים בהן סיכונים ייחודיים.

3. בוטל.

תחולה

4. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א-1981 (להלן בהוראה זו – "תאגיד בנקאי"):

   1) תאגיד בנקאי;
   2) תאגיד בנקאי כאמור בסעיפים 11(א) (3א) ו-(3ב);
   3) תאגיד בנקאי כאמור בסעיף 11 (ב);
   4) סולק כהגדרתו בסעיף 36ט.

(ב) המפקח רשאי לקבוע הוראות מסוימות שונות מאלו המפורטות להלן שיחולו על תאגיד בנקאי מסוים או לפטור במקרים חריגים תאגיד בנקאי מסוים מהוראה מסוימת.

פרק ב': כללי

5. תאגיד בנקאי לא יעשה שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ו/או מערכות ליבה.

6. תאגיד בנקאי לא יאחסן, יעביר או יעבד מידע, שמוגדר על ידו כ"רגיש" (כגון: נתוני לקוחות, מידע עסקי חסוי וכד'), בענן מחוץ לגבולות מדינת ישראל, אלא אם כן, וידא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

7. מחשוב ענן מהווה מקרה פרטי של מיקור חוץ כהגדרתו בפרק ו' להוראת ניהול בנקאי תקין מס' 357. לפיכך, יש לפעול גם בהתאם להוראה כאמור, בנוסף להוראות ניהול בנקאי תקין מס' 361, 363, 367, 359A.

8. אין בהוראה זו כדי לגרוע מהחובות החלות על התאגיד הבנקאי לפי כל החוקים והתקנות הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, ובכלל זאת, חוק הגנת הפרטיות ותקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001, וכן, הנחיית רשם מאגרי מידע מס' 2/2011 – "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי".

9. התאגיד הבנקאי ייבחן את הצורך בהסתייעות, לפי העניין, ביועצים חיצוניים מומחים בהפחתת הסיכונים הגלומים בשימוש בטכנולוגיות ענן.

פרק ג': ממשל תאגידי

דירקטוריון

10. על תאגיד בנקאי אשר בוחן שימוש בטכנולוגיות מחשוב הענן להביא את הנושא לדיון מקדמי בדירקטוריון, לפני הפעלת טכנולוגיות מחשוב ענן. בדיון זה יוצגו הסיכונים הגלומים בטכנולוגיות מחשוב ענן והבקרות המיושמות או המתוכננות להפחתתם. על הדירקטוריון:

(א) לדון בסיכונים אלו, להחליט האם לתת אישור מקדמי למהלך ולהנחות את הנהלת התאגיד הבנקאי בדבר הפעולות שעליה לנקוט – בין היתר ע"פ המפורט בהוראה זו.

(ב) להנחות את ההנהלה לגבש ולאשר מסמך מדיניות לשימוש בטכנולוגיות מחשוב ענן.

11. בהמשך לאמור בסעיף 10 לעיל, הדירקטוריון ידון ויאשר מדיניות לשימוש בטכנולוגיות מחשוב ענן.

12. כאמור בסעיף 13 (א) להלן, על הדירקטוריון לאשר יישום של כל מחשוב ענן מהותי.

13. על דירקטוריון התאגיד הבנקאי לוודא שהשימוש בטכנולוגיות מחשוב ענן יהיה ע"פ המדיניות שנקבעה כאמור.

הנהלה בכירה

13. (א) על ההנהלה הבכירה לגבש מדיניות לשימוש בטכנולוגיות מחשוב ענן אשר תקבע בין היתר את סוגי היישומים בטכנולוגיית מחשוב ענן בהם נדרש אישור של הדירקטוריון (להלן: "מחשוב ענן מהותי" - דוגמאות למחשוב ענן מהותי בנספח א') וסוגי היישומים בהם נדרש אישור הנהלה.

(ב) מסמך המדיניות יתייחס לסמכויות, אחריות ופעולות גופי ניהול שירותי ענן, גופי הבקרה והבקרות; סוגי השירותים והיקפם; תהליכי אישור ודרגי אישור; אחריות הגורמים השונים בתאגיד הבנקאי לטיפול בהיבטים משפטיים, תחזוקה, ניטור, הגנת הסייבר ואבטחת מידע וכד'. המדיניות תיתן מענה, בין היתר, גם לנדרש בהוראה זו.

פרק ד': יישומי מחשוב ענן המחייבים קבלת היתר - בוטל

פרק ה': ניהול סיכונים

17. (א) לפני יישום מחשוב ענן נדרש התאגיד הבנקאי לבצע תהליכי מיפוי והערכת סיכונים נאותים, במעורבות כלל הגורמים הרלוונטיים בתאגיד הבנקאי, ובהתייחס לכלל ההיבטים הרלוונטיים, כמפורט בסעיף 19 להלן.

18. במחשוב ענן מהותי, לפני התקשרות עם ספק שירותי הענן, על התאגיד הבנקאי לבצע בדיקת Due Diligence לרבות בנוגע לחוסנו הכלכלי, יכולתו המקצועית וניסיונו לספק שירותים דומים. ראוי לבצע מעת לעת בדיקה כאמור, גם במהלך תקופת ההתקשרות.

19. תאגיד בנקאי יבצע מיפוי והערכת סיכונים לכל יישום של מחשוב ענן מהותי. הערכת הסיכונים תעשה קודם להתקשרות עם הספק ותעודכן באופן שוטף במהלך תקופת ההתקשרות בין היתר, בהתאם לשינויים כגון: טכנולוגיים, משפטיים, רגולטוריים, עסקיים וארגוניים אצלו ואצל ספק שירותי הענן. על התאגיד הבנקאי לוודא קיום בקרות מפצות מתאימות. על אף שמחשוב ענן מהווה מקרה פרטי של מיקור חוץ, הערכת הסיכונים צריכה לכלול גם סיכונים ייחודיים (טכנולוגיים ואחרים) הקשורים לשימוש במחשוב ענן. דוגמאות של היבטים שיש לקחת בחשבון מובאות בנספח ב'.

20. על התאגיד הבנקאי לוודא שביכולתו לבצע ניטור אירועי סייבר ואבטחת מידע הקשורים ליישום מחשוב ענן מהותי ולשימושו במערכות מחשוב ענן. אם ניטור זה מבוצע באמצעות כלים המסופקים ע"י הספק, יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של התאגיד הבנקאי.

21. במחשוב ענן מהותי, על התאגיד הבנקאי לוודא כי עבור כלל ערוצי הגישה מ/אל ספק מחשוב הענן, קיימים אמצעים להגנת הסייבר ואבטחת המידע, שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפת התאגיד הבנקאי.

22. על המידע של התאגיד הבנקאי להיות מוצפן בעת העברתו בתקשורת וכן כאשר הוא מאוחסן במערכת שאינה לשימושו הבלעדי (Multi-tenancy). במקרים בהם יש קושי לתאגיד הבנקאי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידו כרגישים ושיש בחשיפתם כדי לפגוע בתאגיד הבנקאי ובלקוחותיו. יש לבחון יישום המאפשר, ככל שניתן, לאחסן את מפתחות ההצפנה אצל התאגיד הבנקאי.

פרק ו': הסכם התקשרות עם ספק שירותי הענן

23. מבלי לגרוע מהחובות החלות על התאגיד הבנקאי לפי סעיף 18 להוראת ניהול בנקאי תקין מס' 357 והוראת ניהול בנקאי מס' 363, במחשוב ענן מהותי, הסכם ההתקשרות עם הספק יכלול, בין היתר:

(א) קיום אפשרות חד-צדדית של התאגיד הבנקאי להפסיק את השימוש בשירותי הספק או לעבור לספק אחר תוך העברת נתוניו הרלבנטיים ממערכות הספק תוך זמן קצר, מחיקתם במערכות הספק והתחייבות הספק שלא ניתן לאחזר נתונים אלו במערכותיו.

(ב) התייחסות לקבלת מידע הנוגע למבדקים וביקורות על הספק שירותי הענן.

(ג) מתן אפשרות לתאגיד הבנקאי על בסיס הערכת הסיכונים, לבצע ביקורות אצל ספק שירות הענן.

(ד) מתן אפשרות לפיקוח על הבנקים לבצע ביקורות אצל ספק שירות הענן ביישום מחשוב ענן מהותי.

24. בכל שינוי בבעלות על ספק שירותי הענן, על התאגיד הבנקאי לבחון מחדש את ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם ע"י הבעלים החדשים.

פרק ז': מכתב ההיתר - בוטל

פרק ח': דיווח לפיקוח

27. אחת לשנה (בסיום שנה קלנדרית), על תאגיד בנקאי להעביר בכתב לידי הפיקוח על הבנקים :

(א) רשימה מעודכנת של יישומי מחשוב הענן, לרבות תיאור היישום, מועד היישום, הגורם המאשר ושם ספק שירותי הענן. במחשוב "ענן מהותי" יש לציין את מיקום שרתי הענן.

(ב) דיווח על יישומי מחשוב ענן עתידיים.

עדכונים

חוזר מס'	**גרסה**	**פרטים**	**תאריך**
2536	1	מכתב מפקח מקורי	05/07/2017
2579	2	עדכון	13/11/2018

נספח א' – דוגמאות למחשוב ענן מהותי

- יישום מחשוב הענן כולל מידע המוגדר על ידי התאגיד הבנקאי כמידע רגיש.
- המידע אינו מוגדר ע"י התאגיד הבנקאי כמידע רגיש, אך כתוצאה מחשיפתו, ניתן להסיק פרטים שיאפשרו לתקוף או לפגוע בתאגיד הבנקאי ו/או בלקוחותיו.
- שיבוש או הפסקת הפעילות של יישום מחשוב הענן, עלולים לפגוע באופן משמעותי בהתנהלות התאגיד הבנקאי ו/או ביכולתו לתת שירות ומענה ללקוחותיו.
- יישום מחשוב הענן מספק אמצעי הגנת הסייבר ואבטחת מידע כרובד הגנה יחיד, ושלא קיימים אמצעים דומים מסוגיהם גם בחצרי התאגיד הבנקאי.

נספח ב' – הערכת סיכונים - דוגמאות של היבטי מחשוב ענן

- ממשל תאגידי, מדיניות ונהלים, ביקורת פנימית וחיצונית – האם מסמכי המדיניות מתייחסים כראוי לשימוש במחשוב ענן?
- סיכון רגולטורי - קושי בעמידה בחוקים, תקנות ורגולציות של מדינת ישראל ושל המדינה שבה פועלת או מאוחסנת המערכת ו/או הנתונים. יש חשיבות, בין היתר, להתייחס לסוגיות כגון חובת הספק למסור מידע לגורמי חוק ואכיפה גם ללא ידיעת התאגיד הבנקאי. יש היבטים חוקיים רבים הקשורים לאי-אחידות ההגדרות והדרישות במדינות שונות.
- סיכון סיסטמי הנגזר מספק שירותי הענן הנותן שירותים למספר תאגידים בנקאיים.
- מחזור חיי הנתונים, לרבות מיקום, ריבוי העתקים וחשיפת נתונים.
- ניידות נתונים, רכיבים ומערכות - למשל, האם השימוש ברכיבי ענן של ספק מסוים מגביל את התאגיד הבנקאי ועלול למנוע ממנו את האפשרות לעבור לספק אחר או להעביר את המידע ו/או המערכות חזרה לחצרי הבנק.
- סיכוני סייבר ואבטחת מידע, לרבות דלף מידע, שינויים בתפיסה המסורתית, השימוש בכלי אבטחה ייעודיים, אופן ניהול מפתחות ההצפנה.
- הרשאות גישה, תוך הפעלת כלים המתאימים לסביבת מחשוב ענן.
- ניהול שינויים וניהול נכסי טכנולוגית המידע - למשל, האם לתאגיד הבנקאי יש שליטה על שינויים במערכות והאם תהליכי השינויים תואמים את מדיניות ונהלי התאגיד הבנקאי.
- סיכונים הקשורים להמשכיות עסקית ו- BCP/DRP, לרבות שינויים בתצורת רשת התאגיד הבנקאי, ומיקומם הגאוגרפי של שרתי הענן ובכללם שרתי הגיבוי.
- סיכונים הקשורים לסביבות העבודה וכלי הניהול העלולים להוסיף רמת תחכום ומורכבות למערכות.
- סיכונים משפטיים וביניהם היבטי סודיות, שמירת נתונים, הבעלות על המידע ורישוי תוכנות.
- טיפול באירועים חריגים, לרבות הסדרי הדיווח והטיפול, והסדרת תחומי האחריות.
- סיכונים הנוגעים למעטפת התקיפה כגון: שילוב מכשירים ניידים (טלפונים ניידים, טאבלטים וכל אמצעי נייד אחר) ביישום מחשוב הענן.
- סיכונים הכרוכים בשרשרת אספקה של יישום מחשוב ענן, ע"פ האמור בהוראת ניהול בנקאי תקין מס' 363.