לקוחות יקרים,

ביום 18 בנובמבר 2024 פורסמה על ידי הפיקוח על הבנקים הוראת ניהול בנקאי תקין מס' 364 שכותרתה "ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר". ההוראה נועדה לספק מסגרת כוללת, אחידה, סדורה וגמישה לניהול הסיכונים הטכנולוגיים לאור התפתחות האיומים והסיכונים העדכניים. בהתאם לגישת הפיקוח על הבנקים העדכנית, ההוראה מאזנת בין שני היבטים: מחד, היא מאפשרת לכל תאגיד בנקאי לנהל את סיכוניו בהתאם לאסטרטגיה ותיאבון הסיכון שיבחר לעצמו; ומאידך, היא מקבעת ומחדדת את החשיבות שיש לייחס לניהול סיכונים אלה בחיי התאגיד הבנקאי. במסגרת זו, ההוראה מקבעת באופן רחב אחריות ישירה לדירקטוריון למעורבות אקטיבית בהתוויית אסטרטגית ניהול הסיכון, לרבות בחינת המשאבים המוקצים ליישומה וחובות לפיקוח אקטיבי על אופן ביצועה וניהולה. בנוסף, ההוראה קובעת דרישה קוגנטית לקיומם של בעלי תפקיד ייעודיים שונים והגדרה ברורה של היקף אחריותם. ההוראה מחליפה שלוש הוראות קיימות: נב"ת 357 בנושא ניהול טכנולוגיית המידע, נב"ת 361 בנושא ניהול הגנת הסייבר ונב"ת 363 בנושא ניהול סיכוני סייבר בשרשרת אספקה. מדובר בהסדר משמעותי החל ישירות על תאגידים בנקאיים, אך לא פחות מכך – מעניין כל גוף המעוניין לעבוד עם תאגידים בנקאיים.

ההוראה מצריכה לדעתנו, עבודת מטה נרחבת לשם יישומה ודורשת הליכי טרנספורמציה יסודיים הנוגעים לתאגיד הבנקאי בכל רמות הניהול שלו כמו גם, באופן יישום התקשרויותיו עם ספקיו ונותני השירות שלו. כן דורשת ההוראה לטעמנו, ליווי מקצועי והדוק המשלב הבנה משפטית נרחבת בעולמות הפרטיות, הסייבר, טכנולוגית המידע, מערכות ההפעלה והרגולציה הבנקאית. הדברים האמורים לעיל נכונים לתאגידים בנקאיים, אך לא פחות מכך - לכל ארגון שיהיה מעוניין לעבוד עם תאגידים בנקאיים. נשמח לסייע לכם בבחינת השלכות ההוראה על פעילות הארגון שלכם ולסייע לארגונכם לעמוד בה.

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

אגמון עם טולצ'ינסקי, משרד עורכי דין | www.agmon-law.co.il

להלן עיקרי ההוראה לדעתנו.

1. **<u>מבנה והוראות אחרות</u>**

1.1 הוראת נב"ת מס' 364 ("**ההוראה**"), מגדירה שישה תחומים מרכזיים בהם נדרש התאגיד הבנקאי לפעול: (א) ממשל תאגידי וניהול סיכונים; (ב) ניהול סיכוני טכנולוגיות מידע; (ג) ניהול סיכוני אבטחת מידע וסייבר; (ד) ניהול אירועים; (ה) המשכיות עסקית וחוסן תפעולי; ו-(ו) ניהול סיכונים מול צדדים שלישיים.

1.2 <u>הרמוניזציה עם יתר הוראות הפיקוח</u>:

(א) ההוראה מחליפה את הוראות נב"ת 357 (ניהול טכנולוגיית המידע) ("**נב"ת 357**"), נב"ת 361 (ניהול הגנת הסייבר 361) ("**נב"ת 361**") ונב"ת 363 (ניהול סיכוני סייבר בשרשרת אספקה).

(ב) לפי הפיקוח על הבנקים ("**הפיקוח**"), ההוראה תואמת את העקרונות הכלליים לניהול סיכונים לפי הוראת נב"ת מס' 310 בנושא ניהול סיכונים ("**נב"ת 310**"), והוראת נב"ת 350 בנושא ניהול הסיכון התפעולי. כן היא כתובה בהלימה עם הוראות נוספות הנוגעות בתחומים טכנולוגיים, כמו הוראת נב"ת 362 בנושא מחשוב ענן, הוראת נב"ת מס' 355 בנושא המשכיות עסקית והוראת נב"ת 359A בנושא מיקור חוץ ("**נב"ת 359A**").

(ג) לפי הפיקוח, בעתיד ההוראה תשמש בסיס להוראות הפיקוח בנושאים ייעודיים בתחום טכנולוגיית המידע, וכך למשל עתיד הפיקוח על הבנקים לפרסם התאמות להוראת נב"ת 366 בנושא דיווח על אירועי כשל טכנולוגי וסייבר.

1.3 <u>הגדרות</u>. סעיף בעל נפקות רוחבית רבה, שלרוב לא נותנים עליו את הדעת, הוא סעיף ההגדרות. במסגרת זו נעשו שינויים, והעיקריים בעניינו הם:

(א) "אירוע כשל טכנולוגי" – ההוראה מרחיבה את ההגדרה הקיימת בנב"ת 357, וכן יוצרת הבחנה בין "אירוע כשל טכנולוגי" - המתייחס לאירוע שאינו קשור לאבטחת מידע, לבין "אירוע אבטחת מידע" - המתייחס לאירוע שבו נפגעה אבטחת המידע או שהיה בו פוטנציאל לפגיעה באבטחת המידע, וכל כשל בשלמות או חוסר התאמה/זמינות של נכס מידע, אשר יחשבו כאירוע כשל טכנולוגי גם אם לא גרם לכך שפעילותו השוטפת של מערך טכנולוגיות המידע או של השירותים הניתנים על ידי התאגיד הבנקאי תיפגע. הגדרה זו משפיעה, למשל, על הסכמים עם צדדים שלישיים לדעתנו ועל המדיניות הפנימית של התאגיד בנושא דיווח וטיפול בכשל שכזה.

(ב) "מידע רגיש" - ההגדרה נותרה מרחיבה ביחס להגדרה בחוק הגנת הפרטיות, תשמ"א-1981 ("**חוק הגנת הפרטיות**") ומוסיפה לכלול מידע אודות תאגידים ו-"מידע בעל רגישות מיוחדת" (כהגדרתו בתיקון 13 לחוק הגנת הפרטיות ("**תיקון 13**")). בהקשר זה, מעניין לשים לב להגדרה הרחבה יותר בתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("**תקנות אבטחת מידע**"), ביחס לנתונים המקימים חובה לאבטח מאגרים ברמת אבטחה בינונית וגבוהה.

(ג) "נכסי מידע" – ההגדרה כוללת תדפיסים, בשונה מהגדרת "מאגר מידע" (כפי שהיא גם בתיקון 13, השמורה "לאוסף פרטי מידע אישי המעובד באמצעי דיגיטלי"), אך בדומה לסעיף 2 בחוק הגנת הפרטיות, שיכול אף הוא להקים חשיפה לא מבוטלת לתאגידים בנקאיים. הגדרה זו משפיעה על כלל המנגנונים והבקרות בהוראות השונות.

(ד) "עובדים" – גם הוראה זו מוסיפה להתייחס לעובדים חיצוניים המנוהלים על ידי התאגיד הבנקאי, כך שנשמר פער ביחס להגדרת "בעל הרשאת גישה" המקובלת בתקנות אבטחת מידע.

(ה) "חוסן תפעולי" - יכולת התאגיד הבנקאי לספק פעולות חיוניות לאורך תקופה של שיבוש.

(ו) "מודעות מצבית" - היכולת לקלוט מידע בנוגע לאיומים, למטרות ולסביבה, לפרש אותו נכון ובזמן.

(ז) "יכולת אבטחת מידע" - כלל המשאבים, המיומנויות והבקרות הנדרשים לצורך קיום פעילות אבטחת מידע נאותה בסביבת סיכונים משתנה.

2. **<u>ממשל תאגידי</u>**. ההוראה מחייבת יישום מסגרת ממשל תאגידי מקיפה המשלבת את ניהול סיכוני טכנולוגיית המידע כחלק אינטגרלי מהפעילות העסקית של התאגיד הבנקאי, הכולל מסגרת מתאימה לניהול סיכוני טכנולוגיית המידע, ובכלל זה מסגרת לניהול סיכוני אבטחת מידע וסייבר. במסגרת זו:

2.1 <u>הדירקטוריון</u>. דירקטוריון התאגיד הבנקאי אחראי לניהול סיכוני טכנולוגיית המידע בתאגיד הבנקאי. בין היתר, עליו לוודא כי אבטחת המידע ואמצעי הבקרה האחרים המיושמים בתאגיד הבנקאי תואמים את היקף הסיכונים לנכסי המידע שלו, בצורה המאפשרת את המשך פעילותו. בין היתר, נדרש הדירקטוריון:

(א) להתוות ולאשר את אסטרטגיית טכנולוגיית המידע והתיאבון לסיכון, לאשר את מדיניות ניהול טכנולוגיית המידע והמסגרת לניהול סיכונים, ולקיים דיון לפחות אחת לשנה

באפקטיביות יישומם. במסגרת זו, על הדירקטוריון לוודא את נאותות ביסוי הבדיקות הנעשות על סביבת הבקרה, לבחון חריגות מהותיות מהמסגרת והטיפול שניתן להן.

אסטרטגיית טכנולוגיית המידע נדרשת לתת מתווה מקיף המנחה את ניהול הטכנולוגיה בתאגיד הבנקאי, לכלול יעדים ותוכניות ברמת המאקרו עבור כל תחומי טכנולוגיית המידע המשפיעים על התאגיד הבנקאי (לא רק עבור התשתיות) לאופק של 3 עד 5 שנים.

אסטרטגיה זו נדרשת להסתמך על תיאבון הסיכון של התאגיד, דבר אשר נותן משנה תוקף לצורך לנסחו בצורה ברורה שתאפשר ניסוח ברור של מדיניות ומגבלות סיכון.

(ב) להחליט לגבי אילו פרויקטי טכנולוגיית מידע מרכזיים הוא מעוניין לקבל דיווח, אילו מדדי ביצוע הוא מעוניין לקבל, ואילו תיעדופים נדרשים להיות מובאים לאישורו.

(ג) לוודא כי היקף כוח האדם ומיומנותו בכל שלושת קווי ההגנה מספיקים בכדי לתמוך בצרכי מערך טכנולוגיית המידע, בתהליכי ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והסייבר, על מנת ליישם את אסטרטגיית טכנולוגיית המידע שגיבש התאגיד הבנקאי. כמו-כן, עליו לוודא את התקציבים המוצעים לנושאים אלה.

(ד) לדון, להחליט ולאשר אחת לשנה את תוכנית העבודה השנתית והרב-שנתית בתחום טכנולוגיית המידע, ובכלל זה תוכנית העבודה לטיפול בסיכוני טכנולוגיית המידע. במסגרת זו, על הדירקטוריון לקיים פגישה שנתית עם מנהל טכנולוגיית המידע ומנהל הגנת הסייבר ואבטחת המידע לצורך הערכת אפקטיביות המסגרת. כמו-כן, במידת הצורך, נדרש הדירקטוריון לאתגר את ההנהלה בנוגע לאפקטיביות מדיניות ניהול טכנולוגיית המידע.

(ה) לקבל דיווח על אירועי סייבר משמעותיים ולדון בהשלכותיהם על התאגיד הבנקאי. כפועל יוצא, יהיה צורך בתאגידים הבנקאיים לקשור בין יכולות אבטחת המידע והסייבר של התאגיד לתפקיד הדירקטוריון לוודא כי רמת ההגנה של אבטחת המידע והסייבר תואמת את האיומים השונים ומאפשרת את ההמשכיות העסקית לה נדרש התאגיד, ולהבטיח את ציות התאגיד הבנקאי לדרישות חוקיות ורגולטוריות בתחום טכנולוגיית המידע, אבטחת המידע והגנת הסייבר.

(ו) ניתן דגש לכך שהדירקטוריון נדרש להבין את פעילות טכנולוגיית המידע בתאגיד הבנקאי ואת הסיכונים הכרוכים בה, וזאת לצורך מילוי חובותיו. בהקשר זה חשוב לדעתנו לשים לב ל: (1) סוגיות החופפות והנוספות שבין הנחיה זו לבין הנחיית הרשות להגנת

הפרטיות מס' 1/2024 בדבר תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע) ("**הנחיית הרשות**");[1] ו-(2) שלפי הפיקוח, גם המגמה שלו היא להגביר את מעורבות הדירקטוריון בתחום טכנולוגיות המידע, אבטחת המידע והסייבר.

יש לציין כי הוראה זו מרחיבה לדעתנו את תפקידי הדירקטוריון ואת דרישות הדיווח. תפקידיו הנוספים של הדירקטוריון ופירוט נוסף אודות תחומי אחריותו נמצאים בהוראה, ואולם אין ספק לטעמנו כי רמת ההבנה הנדרשת מהדירקטוריון ומהגורמים בהם הוא נעזר גדלה באופן משמעותי לאור ההוראה והנחיית הרשות.

2.2 <u>ההנהלה הבכירה</u>. ההנהלה הבכירה של התאגיד הבנקאי אחראית ליישום ותחזוקה של סביבת פעילות מאובטחת ונאותה, המאפשרת את השגת היעדים האסטרטגיים, התאגידיים והתפעוליים של התאגיד הבנקאי, והעומדת בחוק וברגולציה הרלוונטיים. בכלל זה, תהיה ההנהלה הבכירה אחראית לביצועי מערך טכנולוגיית המידע ולתפעול השוטף שלו ותידרש:

(א) לתכנן וליישם מסגרת לניהול סיכוני טכנולוגיית המידע ולפקח עליה.

(ב) לגבש ולעדכן באופן שוטף את מדיניות ניהול טכנולוגיית מידע ואת המסגרת לניהול סיכוני טכנולוגיית המידע.

(ג) לגבש וליישם תוכנית עבודה שנתית ורב-שנתית בתחום טכנולוגיית המידע ולניהול הסיכונים הקשורים בה, ולהקצות משאבים מתאימים ליישומה.

(ד) לשמור על יכולת אבטחת מידע ועדכונה לצורך המשך פעילותו הנאותה של התאגיד הבנקאי.

(ה) לקבל דיווח על תמונת מצב עדכנית של איומי הסייבר ודרכי ההתמודדות מולם, בהתאם לתוצאות הערכת הסיכונים, וכן לקבל דיווח תקופתי על אירועי סייבר רלוונטיים (פנימיים וחיצוניים) וניתוח המשמעויות הנגזרות מהם.

(ו) לדון בהשלכות האופרטיביות, חוצות ארגון, של סיכוני סייבר ולהנחות ולבקר על ביצוע שינויים או התאמות במערך ההגנה ו/או בפעילות העסקית לפי הצורך. כמו-כן, לתעדף ולתאם בין הפונקציה האחראית על טכנולוגיית המידע לבין קווי העסקים, להתוות ולבצע מעקב אחר תיאום פעילות אבטחת המידע, לוודא קיום תהליך לקבלה, ניתוח ותגובה

[1] מזכרנו בנושא זמין כאן.

של מידע מודיעיני על איומים ופגיעויות, כגון באמצעות השתתפות בתוכניות לשיתופי פעולה בנושא.

(ז) לספק לדירקטוריון את המידע ביחס ל: (1) סיכוני טכנולוגיית המידע ואופן ההתמודדות; (2) אירועי אבטחת מידע רלוונטיים וניתוח משמעויות מהם; (3) מימוש אסטרטגיית טכנולוגיית המידע; (4) שינויים מהותיים בתחום טכנולוגיית המידע; (5) דיווח מיידי לדירקטוריון באשר לחריגה מהותית ממדיניות ניהול טכנולוגיית המידע ומהמסגרת לניהול סיכוני טכנולוגיית המידע, התפתחויות שליליות מהותיות בסיכוני טכנולוגיית המידע, שינוי מהותי בנכסי המידע או בסביבה העסקית, ובאשר לאירועי כשל טכנולוגי ואירועי אבטחת מידע שיש להם פוטנציאל להשפעה משמעותית על התאגיד הבנקאי.

(ח) לקיים דיון שנתי ב: (1) מדיניות ניהול טכנולוגיית המידע, בתוכנית העבודה, ביכולת אבטחת המידע, במדיניות אבטחת המידע והגנת הסייבר, ובתוכנית העבודה; (2) תהליך מיפוי נכסי המידע וליישום בקרות טכנולוגיות, לרבות בקרות אבטחת מידע.

(ט) למנות מנהל טכנולוגיות מידע שיהיה חבר הנהלה ויישא באחריות מפורשת למכלול הנושאים הקשורים לטכנולוגיית המידע, ולמנות מנהל הגנת סייבר ואבטחת מידע שיהיה כפוף לחבר הנהלה ואחראי לניטור ולעמידת התאגיד הבנקאי במסגרת לניהול אבטחת המידע. בהקשר זה, נזכיר כי תאגידים בנקאיים יידרשו גם לממוני הגנת פרטיות כעת גם מכוח תיקון 13.[2]

(י) לקיים דיונים תקופתיים בעמידה ביעדי תוכנית העבודה, דיונים נוספים כאשר עולים ממצא ים מהותיים מתהליך הניטור של המסגרת לניהול טכנולוגיית המידע, שינויים מהותיים במסגרת ניהול סיכוני טכנולוגיית המידע ונושאים נוספים מהותיים, כגון: התקשרויות משמעותיות.

תפקידים נוספים של ההנהלה הבכירה ופירוט נוסף אודות תחומי אחריותה נמצאים בהוראה. גם אם אין שינוי מהותי בתפקידיה ותחומיה אחריותה, ההוראה בהחלט מעלה את המעורבות ורמת הידע הנדרשת מההנהלה הבכירה ומהגורמים בהם היא נעזרת ביחס לסוגיות סייבר ואבטחת מידע ומרחיבה את הדרישות הקיימות בנב"ת 357 ובנב"ת 361. הנושאים האמורים יידרשו לקבל ביטוי גם בנהלי העבודה השונים ובנהלים העוסקים באירועי סייבר של התאגידים הבנקאיים. כל אלה יצריכו התאמות, אך לטעמנו קצרה היריעה מלהביא אותן במזכר זה.

[2] ראו סעיף 17ב1(א)(4) לתיקון 13.

2.3 <u>מנהלי קווי עסקים</u> – סעיף 27 להוראה מחזק, לדעתנו, את הקשר בין המנהלים של קווים עסקיים לתהליכים הנוגעים למערכות השונות בתאגיד הבנקאי. בהוראה מושם דגש על אחריותם של מנהלי קווי העסקים לוודא כי תוכניות הפיתוח של מערך הטכנולוגיות בתאגיד תואמות את התוכנית העסקית, לוודא קיומם של תהליכי עדכון שוטפים למערך טכנולוגיות המידע בתאגיד בדבר צרכים עסקיים חדשים או משתנים, ודוחות הנדרשים ממערכות. כמו-כן, באחריותם לוודא בדיקות נאותות של צדדים שלישיים, הלוקחים חלק בהליכים העסקיים עליהם הם מופקדים.

2.4 <u>מנהל טכנולוגיות מידע</u>. מנהל טכנולוגיות המידע אחראי, בין היתר, על:

(א) פיתוח ויישום אסטרטגיית טכנולוגיית המידע, מדיניות ניהול טכנולוגיית המידע ותוכניות עבודה שנתיות ורב-שנתיות, בשים לב להנחיות הדירקטוריון וההנהלה הבכירה.

(ב) ניהול תקציב טכנולוגיית המידע וביצועי המשאבים.

(ג) ניהול ביצועי המשאבים בתחום טכנולוגיית המידע.

(ד) ניהול רכישות והשקעות בתחום טכנולוגיית המידע.

(ה) ניהול הפיתוח המקצועי והדרכות מתאימות.

(ו) יישום ארכיטקטורת טכנולוגיית המידע התואמת את היעדים האסטרטגיים.

(ז) תמיכה בפעילות קווי העסקים, בין היתר בהיבטים של אבטחת מידע, חוסן תפעולי, ודיווח על סיכוני טכנולוגיית המידע.

(ח) קיום תהליכים ובקרות נאותים כדי לוודא שכל סיכוני טכנולוגיית המידע מזוהים, מנותחים, נמדדים, מנוטרים, מנוהלים, מדווחים ונשמרים בתוך מגבלות התיאבון לסיכון של התאגיד הבנקאי.

(ט) תכלול ובקרה של אירועי כשל טכנולוגי בתאגיד הבנקאי.

(י) קיום פגישה עם הדירקטוריון, לפחות אחת לשנה, לצורך הערכת אפקטיביות המסגרת לניהול טכנולוגיות המידע בתאגיד הבנקאי.

2.5 <u>מנהל הגנת הסייבר ואבטחת המידע</u>. תפקיד זה מהווה פונקציה מרכזית בניהול סיכוני אבטחת המידע והסייבר, תפקיד אשר הורחב במסגרת הוראה זו מהאמור בנב"ת 361. מנהל הגנת הסייבר ואבטחת המידע אחראי, בין היתר, על:

(א) תכלול היבטי ניהול אבטחת מידע והגנת הסייבר בתאגיד הבנקאי וייעוץ להנהלה בנושא, לרבות סיוע להנהלה בגיבוש ויישום מדיניות אבטחת מידע והגנת הסייבר.

(ב) גיבוש מתודולוגיה תאגידית לניהול סיכוני אבטחת מידע.

(ג) פיתוח, מעקב אחר יישום, וניטור של תוכנית מקיפה ופרטנית להתמודדות התאגיד הבנקאי עם סיכוני אבטחת המידע והגנת הסייבר.

(ד) הגדרת עקרונות ונהלי עבודה למימוש בקרות אבטחת המידע והגנת הסייבר.

(ה) ייזום, קידום והטמעת תהליכים להגברת מודעות המשתמשים.

(ו) קביעת מסגרת הדיווחים שיקבל מגורמים שונים בתאגיד הבנקאי.

(ז) ייזום בדיקות להערכת אפקטיביות בקרות אבטחת המידע.

(ח) בדיקת נאותות אצל צדדים שלישיים. בהקשר זה הסעיף אינו מתייחס לרמה שבה תבוצע בדיקת הנאותות והיא יכולה להתבצע בהתאמה להשפעות האפשריות של אירוע אבטחת מידע על נכסי המידע שאליהם יש לו גישה.

(ט) התעדכנות בסיכוני אבטחת המידע ביוזמות עסקיות חדשות וקביעת דרכים להפחתתם, באמצעות דו-שיח עם הנהלות קווי העסקים, ובאמצעים אחרים.

(י) התעדכנות בתהליכי זרימת המידע, הסיכונים למידע בתהליכים אלו, ואמצעי אבטחת המידע והגנת הסייבר הנדרשים, באמצעות דו-שיח עם הנהלות קווי העסקים.

(יא) תכלול ובקרה של ניהול אירועי אבטחת מידע בתאגיד הבנקאי, לרבות דיווח על אירועי אבטחת מידע מהותיים לדירקטוריון, להנהלה ולרשויות הרלוונטיות.[3]

(יב) ניתוח אירועי אבטחת מידע משמעותיים בישראל ובעולם, הפקת לקחים ויישום המסקנות הרלוונטיות לתאגיד הבנקאי.

לצורך הובלה ותיאום של תהליכים הנוגעים לניהול אבטחת המידע והגנת הסייבר, יידרשו למנהל הגנת הסייבר ואבטחת המידע ממשקים פנימיים וחיצוניים חזקים מבעבר. אין זה מפתיע כי מינויו והחלפתו יוסיפו לדרוש דיווח לפיקוח על הבנקים.

הגורמים האמורים לעיל ידרשו להערכתנו לליווי משפטי מעשי צמוד ובהקשר זה, בולט בעיננו היעדר ההתייחסות לתפקיד ממונה הגנת הפרטיות (הנדרש לפי תיקון 13 לתאגידים בנקאיים) וממשקי העבודה ביניהם. כן ניכר שיידרש מודיעין סייבר משמעותי לצורך קיום דיונים ביחס לאירועים הקורים בעולם ושיתוף פעולה עם מערך הסייבר הלאומי כדי לקבל גישה למודיעין איכותי ומבוקר.

2.6 <u>ביקורת פנימית</u>.

[3] עמדת הפיקוח מבחינה בין "תכלול ניהול אירוע" לבין "ניהול אירוע". הגורם המתכלל את האירוע אינו בהכרח הגורם המנהל אותו בפועל. התאגיד הבנקאי רשאי לקבוע את זהות הגורם האחראי לניהול האירוע בהתאם למאפייניו, ואולם תכלול האירוע נותר באחריותו הבלעדית של מנהל הגנת הסייבר ואבטחת המידע.

(א) הביקורת הפנימית היא כלי בקרה חשוב במערכת הבנקאית. אין בכך חדש, אך במסגרת ההוראה נדרש לקיים בעת יחידה ארגונית לביקורת טכנולוגיות המידע בתאגיד הבנקאי. כאשר אין לביקורת הפנימית את הידע והמומחיות המתאימים או כאשר הנושא הנבדק מנוהל אצל צד שלישי, יכול הדירקטוריון לבחור להסתמך על חוות דעת מומחים או על אמצעים אחרים לפי שיקול דעתו.

(ב) הביקורת הפנימית תמפה את כלל הפעילות של מערך טכנולוגיית המידע, הממשל התאגידי, הפונקציות והתהליכים בתחום טכנולוגיית המידע לרבות אלו שבתחום אבטחת המידע. גם כאן, מיפוי ההליכים העסקיים, זרימת המידע בהם והטכנולוגיות הלוקחות חלק בהליכי עיבוד המידע השונים מקבלת משנה תוקף בדומה למפורט להלן.

3. **<u>מסגרת ניהול סיכונים</u>**. תאגיד בנקאי יקבע מסגרת לניהול סיכוני טכנולוגיית המידע המשולבת במלואה בתהליכים הכוללים לניהול סיכונים בתאגיד הבנקאי. מסגרת זו תכלול, בין היתר, זיהוי והערכת סיכונים על בסיס מתמשך תוך התחשבות בשינויים בסביבה העסקית והטכנולוגית, מיפוי וסיווג של כל נכסי המידע לפי רמת קריטיות ורגישות עם עדכון שנתי לפחות, קביעת אמצעים למזעור הסיכון ובקרות מותאמות לרמת הסיכון, ניטור שוטף של אפקטיביות הבקרות והאמצעים שיושמו, ודיווח תקופתי להנהלה ולדירקטוריון על מצב הסיכונים והבקרות.

3.1 תאגיד בנקאי ינהל את סיכוני טכנולוגיית המידע בשלושת קווי ההגנה הנדרשים לפי נב"ת 310, תוך הטמעה ויישום, בין היתר, של המסמכים והתהליכים הבאים:

(א) אסטרטגיית טכנולוגיית המידע, ובכלל זה תיאבון לסיכון עבור סיכוני טכנולוגיית המידע.

(ב) מדיניות ניהול סיכוני טכנולוגיית המידע הנגזרת מהאסטרטגיה.

(ג) זיהוי והערכה של סיכוני טכנולוגיית המידע אליהם חשוף התאגיד הבנקאי.

(ד) הגדרת אמצעים למזעור הסיכון, לרבות בקרות.

(ה) ניטור האפקטיביות של האמצעים למזעור הסיכון, ניטור של אירועי כשל טכנולוגי ואירועי אבטחת מידע (פרק י"א להוראה), ובן נקיטת צעדים לתיקונם של האמצעים, לרבות יישום בקרות מתאימות במידת הצורך.

(ו) דיווח להנהלה הבכירה ולדירקטוריון בנוגע לסיכוני טכנולוגיית המידע והבקרות המיושמות.

(ז) זיהוי והערכה של סיכוני טכנולוגיית המידע שנוצרו כתוצאה משינויים.

3.2 <u>זיהוי של פעילויות, תהליכים ונכסי מידע וסיווגם</u>:

(א) התאגיד הבנקאי יקבע מתודולוגיה, רחבה יותר לדעתנו מהאמור בנב"ת 357, לזיהוי וסיווג הקובעת עקרונות, בין היתר, באשר למה נחשב נכס מידע, פעילות עסקית ותהליך תומך, רמת פירוט המיפוי הנדרשת, ועקרונות לדירוג קריטיות ורגישות, ויתעד אותה.

(ב) לכל נכס מידע ייקבע בעל נכס שיהיה אחראי להפעלתו ומתן דיווחים לגביו. במקרה בו נכס מסוים משרת מספר תהליכים עסקיים להם רמת קריטיות שונה, הנכס יופעל לפי רמת הקריטיות המחמירה.

(ג) תהליך זיהוי הנכסים צריך להיעשות אחת לשנה, וכן בכל אחד מהמקרים הבאים: (1) כאשר נעשים שינויים מהותיים בנכסי מידע, בפעילויות עסקיות ובתהליכים תומכים; (2) כאשר נעשים שינויים בסביבה העסקית שבה התאגיד הבנקאי פועל. לפיכך, נדרש שהמתודולוגיה תכלול הליך לזיהוי המקרים בהם נדרש שינוי בסיווג של נכסי המידע, של הפעילויות העסקיות או של התהליכים התומכים.

(ד) המיפוי יכול לאפשר (אך לא מחליף) את הדרישה בדבר ניהול ועדכון מסמך הגדרות המאגר לפי תקנות אבטחת מידע.[4]

3.3 <u>הערכת והפחתת סיכון</u>. בהמשך למיפוי, תאגיד בנקאי יבצע הערכת סיכונים על בסיס מתמשך, במסגרתה יזהה ויעריך את סיכוני טכנולוגיית המידע המשפיעים על הפעילויות העסקיות, התהליכים התומכים, ונכסי המידע שזוהו, בהתאם לרמת הקריטיות והרגישות שלהם. הגדרת הבקרות ויישומן לצורך הגנה על נכסי המידע תיעשה לפי רמת סיווג הקריטיות והרגישות, כמפורט בפרק ח' להוראה.

4. **<u>ניהול סיכוני טכנולוגיית המידע</u>**

4.1 <u>מדיניות ניהול טכנולוגיית המידע</u>. ניהול אפקטיבי של טכנולוגיית המידע הוא חלק מהותי מניהול סיכוני טכנולוגיית המידע. העקרונות והפרקטיקות המרכיבים את תהליכי התכנון, היישום והתפעול המפורטים בהוראה צריכים לבוא לידי ביטוי במדיניות טכנולוגיית המידע (עליה אמון בראש ובראשונה מנהל מערכות המידע), כדי לקיים סביבה טכנולוגית אפקטיבית. על מערכות המידע של התאגיד הבנקאי לענות על המאפיינים הבאים תוך יישום בקרות מתאימות:

(א) לספק מידע מדויק, עקבי, שלם, רלוונטי ובזמן אמת.

(ב) להיות אמינות כך שניתן יהיה להסתמך עליהן לצורך תיעוד ואיסוף מידע.

(ג) לספק מידע על מגמות ואינדיקטורים לסיכוני מפתח (Key Risk Indicators).

[4] בהקשר זה יש לזכור את חובות הדיווח לרשות לפי תיקון 13.

(ד) לתמוך באסטרטגיה העסקית של התאגיד הבנקאי.

(ה) לשמור על הסודיות, השלמות והזמינות של הנתונים.

(ו) לאפשר אוטומציה של תהליכים ידניים על מנת להפחית ככל הניתן את הפעילויות המוטות עבודה ידנית.

4.2 ארכיטקטורה. לאור היעדים האסטרטגיים והעסקיים, צריכה להיקבע תוכנית ארכיטקטורת טכנולוגיות מידע מקיפה, אשר תסייע לתאגיד הבנקאי בעיצוב התפיסה, הבקרה והתחזוקה השוטפת של טכנולוגיית המידע. הארכיטקטורה הטכנולוגית תעוצב באופן המשרת את יעדי התאגיד, תוך שמירה על גמישות מרבית המאפשרת התאמה מהירה ויעילה לשינויים טכנולוגיים והטמעת חידושים. התוכנית נדרשת לפרט את התכנון הכולל של מערך טכנולוגיות המידע, ותכלול תרשימי זרימה של הפעילות, תהליכי עיבוד נתונים, ממשקים למערך טכנולוגיית המידע, אבטחת מידע וזמינות הנכסים. רמת הפירוט תיקבע בהתאם לרמת הקריטיות והרגישות של נכסי המידע (עליה דנו למעלה). התשתית תתבסס על עקרונות של הפרדה נאותה בין סביבות הפיתוח, הבדיקות והייצור, ותכלול מנגנוני אבטחת מידע מתקדמים ופתרונות להמשכיות עסקית, תוך הטמעת כלים אפקטיביים לניטור ובקרה שוטפים על פעילות המערכות. המערך הטכנולוגי יתוכנן כך שיתמוך בשילוב חלק של טכנולוגיות חדשניות. הארכיטקטורה צריכה לתמוך בביצוע תפיסת תחזוקה של התאגיד הבנקאי (מפורטת להלן) ובשמירה על עדכניות רשימת נכסי המידע, הפעילות העסקית וההליכים התומכים. כל זאת, תוך תיעוד מפורט ומעודכן של כלל הרכיבים, התהליכים והממשקים, באופן המאפשר תחזוקה יעילה ושימור הידע הארגוני לאורך זמן כאמור.

4.3 תשתית טכנולוגית. תאגיד בנקאי נדרש לפתח, לתעד וליישם (לפי הקריטיות והרגישות של נכסי המידע), מדיניות ונהלים מתאימים להטמעת בקרות תשתית שתגנה על המתקנים, הטכנולוגיה, והנתונים. הבקרות נדרשות להיות מיושמות אצל התאגיד או אצל צדדים שלישיים רלוונטיים. במדיניות ובנהלים יש להסדיר, בין היתר:

(א) תהליכי זיהוי, איתור וניטור של רכיבי תשתית.

(ב) הקצאה נאותה של משאבים לתחום התשתית הטכנולוגית.

(ג) תהליכי ניהול קונפיגורציה של רשתות וניהול שינויים.

(ד) תהליכי אבטחה וניטור לניתוח תעבורת נתונים וזיהוי פעילויות חריגות.

(ה) תהליכי פיתוח מערכת (תוך התייחסות ל-Scalability, Portability,Interoperability), בקרות תוכנה נאותות (לרבות ביחס לקוד פתוח), בקרות המטפלות בסיכונים הייחודיים למחשב מרכזי, הליכי גיבוי והתאוששות, וכיוצא באלה.

(א) בקרות גישה פיזית ובקרות סביבתיות.

4.4 ניהול ותפעול.

(א) ההוראה כוללת הנחיות רבות ביחס לבקרות תפעוליות, ניהול תהליכים טכנולוגיים תפעוליים (דוגמת תחזוקה, ניהול תצורה, קיבולת, עדכונים, שדרוגים, טלאים, נתיבים מבוססי לוג, גיבויים, סיום חיים והשמדה). ההוראה מביאה באופן אחוד הנחיות לגבי תהליכי ניטור, הערכה ודיווח של מערכות טכנולוגיות (סקירות תקופתיות של Activity Log), תכנון והשקעה בטכנולוגיית המידע, ניהול פרויקטים וניהול שינויים במערכות, וכן הנחיות לגבי רכישה, פיתוח ויישום מערכות וממשקים ומערכות legacy. הוראות אלה מוסיפות על נב"ת 359A.

(ב) ההוראה מגדירה דרישות מפורטות לתהליכי עבודה מרכזיים, לרבות תהליכי גיבוי ושחזור, ניהול שינויים, תהליכי תיעוד ומעקב. כמו-כן, דרישות תחזוקה מרמת הסיוע הטכני (Help Desk), תמיכה תפעולית, פתיחת מטלת תמיכה, הטיפול והסגירה שלה. מבחינת ניטור, ישנן דרישות מפורטות ביחס לשימוש באינדיקטורים מרכזיים לביצועים (KPI) שיאפשרו לקבוע עד כמה התהליך המיושם מסייע בהשגת המטרות, דוחות על זמינות מערכות, זמני תגובה של מערכות, וזמני עיבוד וכו'.

ניהול הסיכונים הטכנולוגיים, ומסמכי המסגרת הקשורים אליו, נדרשים להיות מנוסחים באופן קוהרנטי ולתאום את תהליכי הרכש והתחזוקה הפנימיים ואת ההסכמים עם הצדדים השלישיים הלוקחים חלק בניהול סיכון זה ובאספקת הטכנולוגיות שיש לנהלן באופן מדוד לשם ניהול הסיכון. יש להדגיש כי בכל הנוגע לניהול סיכוני טכנולוגיית המידע חלה הרחבה של ממש מהדרישות המוכרות בנב"ת 357 ובנב"ת 359A.

5. **אבטחת מידע והגנת סייבר**

5.1 תאגיד בנקאי נדרש להעריך באופן שוטף את נאותות יכולותיו בתחום זה תוך התאמה מתמדת להיקף נכסי המידע שברשותו ולרמת הסיכונים הנשקפת להם. המערך יכלול מגוון יכולות מתקדמות, ובהן: זיהוי והערכת איומים בזמן אמת, מנגנוני הגנה מותאמים לאיומים המתפתחים, יכולות תגובה מהירה לאירועים, מערכות להתאוששות והמשכיות עסקית, וכן מערכות ניטור ובקרה מתקדמות. לצורך הפעלת המערך באופן מיטבי, יעסיק התאגיד צוותים מיומנים ומוכשרים ויקיים תהליכי למידה והפקת לקחים שוטפים. התאגיד נדרש לקיים (ולהראות באופן טבעי) שהוא מקיים תהליך מתמשך של מיפוי וחקר סביבה, הכולל חיזוי

והערכת איומים, ניטור מגמות מתפתחות, שיתוף מידע מודיעיני עם גורמים רלוונטיים, והערכת אפקטיביות הבקרות המיושמות. על בסיס תהליכים אלה, יבצע התאגיד עדכון והתאמה שוטפים של מערך ההגנה, השקעה מתמשכת במשאבים הנדרשים (לרבות תקציב וכוח אדם), ויישם בקרות מתאימות למניעה, זיהוי ותגובה. ההוראה כוללת הנחיות ביחס ליכולות שנדרש התאגיד הבנקאי לשמר, המסגרת שיש לקיים לאבטחת המידע והגנת הסייבר, בקרות האבטחה שיש ליישם וטכנולוגיות או שיטות שיש לשקול.

5.2 על פי ההוראה, תאגיד נדרש לקיים מסגרת מקיפה לניהול אבטחת מידע והגנת סייבר המשולבת במערך ניהול הסיכונים הכולל.

(א) עקרונותיה המרכזיים כוללים, בין היתר – הגנה לעומק (Defense in Depth); הרשאות מינימליות ועקרון הצורך לדעת; זיהוי אירועי אבטחה בזמן אמת; שילוב עקרונות אבטחה כבר בשלב התכנון (Secure by Design); צמצום איסוף המידע ועיבודו למינימום ההכרחי, כבר משלב התכנון המוקדם ולאורך כל מחזור החיים של איסוף המידע והשימוש בו (Privacy by Design). תפיסת ההגנה צריכה להיות פרואקטיבית (גם בהיבטים של רכש והטמעת יכולות הסטה, עיכוב והטעיה של תוקפים) ולשמר עקרונות מסורתיים כגון ניהול הרשאות, Zero Trust, Need To Know ו-Least Privileged.

(ב) המסגרת לניהול אבטחת המידע והגנת הסייבר צריכה להיות מסונכרנת למסגרות אחרות, דוגמת מסגרת לניהול הסיכונים, מסגרת לניהול מיקור חוץ והנחיות משפטיות. המסגרת תכלול מנגנוני בקרה ופיקוח מתקדמים הכוללים ניטור רציף של פעילות משתמשים ומערכות, בקרות גישה מתקדמות, מערכות הצפנה ואבטחת מידע, בקרות על העברת מידע (ומניעת דלף DLP), זיהוי אנומליות וניהול ובקרת שינויים.

(ג) אבטחת המידע והגנת הסייבר צריכה להתייחס לנכסים לאורך כל חייהם. מהתכנון (באמור לעיל), עיצוב, רכישה, יישום, הוצאה משימוש והשמדה. התאגיד הבנקאי נדרש למפות את בקרות אבטחת המידע המיושמות לרוחב הארגון, ולקבוע תוכנית בדיקות שתתקף את אפקטיביות אותן בקרות ואת הפעלתן. התכנית צריכה להביא בחשבון את רגישות הנכסים שאותן בקרות נועדו לאבטח, אך כל בקרת אבטחת מידע תיבדק לפחות אחת לשלוש שנים. ההוראה מציגה דוגמאות לבקרות וכלים שניתן לעשות בהם שימוש לבדיקת בקרות אבטחת המידע, או לחייב צדדים שלישיים לעשות בהם שימוש ולהציג את ממצאיהם לתאגיד הבנקאי.

5.3 <u>יכולות אבטחת מידע</u>. התאגיד הבנקאי נדרש לפתח ולתחזק יכולות אבטחת מידע שצריכות לכלול, בין היתר: (א) יכולת ניהול פגיעויות ואיומי אבטחת מידע; (ב) מודעות מצבית, שיתוף

מידע ומודיעין; (ג) תפעול וניהול מערך אבטחת המידע; (ד) פיתוח ותכנון ארכיטקטורה מאובטחים; (ה) בדיקות אבטחה (Security Testing) לרבות בדיקות חדירה; (ו) מערך הדיווחים בתחום סיכוני אבטחת המידע ויכולת הניתוח של סיכונים אלו; (ז) זיהוי ותגובה לאירועים, לרבות דיווח ותקשורת עם גורמים רלוונטיים לגבי אותם אירועים; (ח) תחקיר, שימור ראיות וניתוח מעמיק של אירועי אבטחת מידע; (ט) הערכת אפקטיביות בקרות אבטחת מידע(Information Security Assurance); ו-(י) יכולות התאוששות הכוללות מערכות גיבוי מתקדמות, תוכניות המשכיות עסקית, יכולות שחזור מהיר ומנגנוני התאוששות אוטומטיים. ההוראה מדייקת הנחיות עבר בהקשר, אך מחדדת את הצורך ביכולות תחקור ושימור ראיות, בדיקת אפקטיביות היכולות השונות ואת הצורך לממשק לעולמות המודיעין ולקיים יכולות, הן בתאגיד הבנקאי והן אצל צדדים שלישיים, אשר נותנות מענה למודיעין זה.

5.4 מדיניות אבטחת המידע. מדיניות אבטחת המידע והגנת הסייבר של תאגידים בנקאיים מקבלת בהוראה הסתכלות מעמיקה וסדורה, ובמסגרת ההוראה ישנם כ-20 נושאים להם נדרשת המדיניות של התאגיד להתייחס ברמות עומק שונות, בין היתר, יש לכלול בה התייחסות מעמיקה למחויבות וציפיות הדירקטוריון וההנהלה הבכירה, להציב בה יעדים, לוודא את התאמתה לסביבה החוקית והרגולטורית. כן יש לפרט במסגרתה את המתודולוגיות להערכת סיכונים ואת אופן הקצאת המשאבים הנדרשים ליישומה.

ההוראה כוללת הוראות מפורשות ביחס לניהול הזהויות וגישה לוגית ופיזית של בעלי הרשאה לנכסי המידע, תוך פירוט אמצעים טכנולוגיים שיש לשקול אותם (לרבות ביחס לניהול מפתחות והצפנתם), וההחרגה המתבקשת ללקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בנב"ת 367 (ומקבילתה בעמדת הרשות לפיה גישה של אדם למידע אודותיו מהווה מימוש זכות עיון ולא הרשאת גישה). בנוסף, המדיניות תכלול התייחסות מפורטת לבקרות אבטחת מידע במחזור החיים של המערכות, מנגנוני ניטור וניהול אירועי אבטחת מידע, דרישות אבטחת מידע בהתקשרויות עם צדדים שלישיים, וכן תוכניות הדרכה ומודעות עובדים.

5.5 ניהול סיכונים בהתקשרויות עם ספקים. ניהול סיכונים בהתקשרויות עם ספקים מהווה נדבך מרכזי במערך ניהול הסיכונים התאגידי. על התאגיד הבנקאי לגבש ולהטמיע מסגרת מקיפה לניהול סיכונים בהתקשרויות עם ספקים, אשר תכלול מנגנונים להערכה וסיווג של ספקים על בסיס רמת הקריטיות והרגישות של נכסי המידע אליהם ניתנת להם גישה. במסגרת זו,

נדרש התאגיד הבנקאי לבצע הערכת סיכונים מקיפה טרם ההתקשרות ולבחון את יכולות אבטחת המידע של הספק והתאמתן לדרישותיו. ההסכמים עם הספקים יכללו הוראות מחייבות בנושאי אבטחת מידע והגנת סייבר, לרבות הגדרת רמת שירות (SLA) לטיפול באירועי אבטחה, דרישות להקשחת מערכות, העברת קבצי Log וכן הסדרים למחיקת נתונים בסיום ההתקשרות. התאגיד הבנקאי יקיים מערך בקרה ופיקוח שוטף על פעילות הספקים, הכולל ביצוע סקרי אבטחה ומבדקי חדירה תקופתיים, ניטור פעילות בזמן אמת, בדיקת מהימנות עובדים ופיקוח על ספקי משנה. בהתייחס לגישה מרחוק, יוטמעו אמצעי זיהוי חזקים, מנגנוני ניתוק אוטומטי ובקרות גישה מיוחדות לסביבת הייצור, תוך הקלטה וניטור של פעילות תחזוקה מרחוק. כחלק מהיערכות להמשכיות עסקית, יידרשו הספקים להציג תוכנית המשכיות עסקית מתואמת, להשתתף בתרגילי חירום ולעמוד בזמני התאוששות מוגדרים, באופן שיבטיח את רציפות השירותים החיוניים לפעילות התאגיד הבנקאי.

גם בנושאי אבטחת המידע והתקשרות עם ספקים קיימת הרחבה של הדרישות הקיימות בנב"ת 357, נב"ת 361, נב"ת 362 ובנב"ת 359A. לאור כך, קיים צורך בליווי שיבטיח ניהול קוהרנטי של אבטחת המידע והסייבר לפי מסמכי מדיניות סדורים שיבואו לידי ביטוי גם בהתקשרויות התאגיד מול צדדים שלישיים המשפיעים על אבטחת המידע והגנת הסייבר שלו.

6. **<u>ניהול אירועים</u>**

6.1 באופן טבעי, ישנו צורך לנטר כשלים טכנולוגיים ואירועי אבטחת מידע, שההבדל ביניהם בזמן אמת לא תמיד חד.

6.2 לצורך כך, מחדדת ההוראה ומרחיבה את הדרישות הקיימות כיום בנב"ת 361 ובנב"ת 366, את מסגרת המדיניות והנהלים שהתאגיד הבנקאי צריך לקיים לשם זיהוי בעיות מתהוות, על מנת למנוע מהן באופן פרואקטיבי מלהתפתח לאירועי כשל טכנולוגי או לאירועי אבטחת מידע. המסגרת צריכה לקבוע את אופן הזיהוי, הגדרת תפקידים וסמכויות, הניתוח, והפתרון של הגורם השורשי (Root Cause) לאירוע או למספר אירועים לרבות תהליכי תגובה מוגדרים, תיעודם ודיווחם להנהלה ולדירקטוריון (לפי פירוט המובא בהוראה).

6.3 התאגיד הבנקאי נדרש לקבוע נוהלי דיווח, אסקלציה, ניהול, תגובה וסיום של אירוע אבטחת מידע. אין בכך חדש, אך ההוראה כן מביאה דרישות ביחס להקמת חדר מצב ותיעוד ביומן אירועים בסמוך להחלטות או התרחשויות, דרישה לקיום מאגר של פעילויות תגובה (Playbooks), סולם של רמות כוננות ופעילויות נדרשות (בדומה למקובל למשל במערכת הבריאות ותוכנית סדורה להתאוששות מאסון והבטחת המשכיות עסקית.

6.4 כן נדרש התאגיד הבנקאי לקיים תוכנית לסקירה ולתרגול תוכניות התגובה של התאגיד לאירוע אבטחת מידע ולאירוע כשל טכנולוגי, אשר תבוצע בתדירות שלא תפחת מאחת לשנה לכל אחד מסוגי האירועים. התוכנית והתרגולים צריכים להתייחס לגורמים חיצוניים ופנימיים.

6.5 תאגיד בנקאי חייב לקיים מערך ניטור ובקרה, שיהיה מאויש באופן רציף 365X7X24 ויקבל דיווחים בזמן אמת מהמערכות השונות, לרבות מערכות תפעוליות ועסקיות, ומערכות אבטחת מידע והגנת הסייבר שונות. הנחיה זו אינה חדשה בעיקרה, אך במסגרת ההוראה מובאות בקרות ניטור לדוגמא שהתאגיד הבנקאי יכול לשקול ליישמן, וכמובן אנו ממליצים לשקול את יישומן ולתעד זאת.

7. **<u>תחילה והוראות מעבר</u>**

7.1 מועד תחילת ההוראה הוא 18 חודשים מיום פרסומה.

7.2 לעניין חוזים שנכרתו לפני מועד פרסום ההוראה - במועד החידוש הקרוב של החוזה ולא יאוחר מ-3.5 שנים ממועד התחילה (כלומר, תקופה כוללת של עד 5 שנים מיום פרסום ההוראה), נדרש התאגיד הבנקאי להתאים את החוזים להוראה ככל שהדבר נדרש.

7.3 תאגיד בנקאי רשאי לפעול על פי ההוראה במועד מוקדם יותר, ובלבד שיודיע למפקח על הבנקים 30 יום קודם למועד כאמור. נבהיר כי יישום מוקדם כאמור מחייב היערכות מתאימה והצגת תוכנית יישום מפורטת לפיקוח, הכוללת אבני דרך ברורות ליישום הדרגתי של הדרישות השונות הכלולות בהוראה.

לקריאת נוסח ההוראה המלא יש ללחוץ **באן**.

לסיכום – הוראת נוהל בנקאי תקין 364, מצריכה לדעתנו עבודת מטה נרחבת לשם יישומה ודורשת הליכי טרנספורמציה יסודיים הנוגעים לתאגיד הבנקאי בכל רמות הניהול שלו כמו גם, באופן יישום התקשרויותיו עם ספקיו ונותני השירות שלו. כן דורשת ההוראה לטעמנו, ליווי מקצועי והדוק המשלב הבנה נרחבת בתחומי טכנולוגית המידע והיבטים המשפטיים בתחום הפרטיות והסייבר, ופרויקטי מערכות מידע. הדברים האמורים נכונים גם לתאגידים בנקאיים וגם לגופים המעוניינים לעבוד עם תאגידים בנקאיים. גופים אלה ידרשו להתאים עצמם לדברי ההוראה על מנת לאפשר לתאגידים הבנקאים לעשות שימוש במוצריהם או שירותיהם. נשמח לסייע לכם בבחינת השלכות ההוראה על פעילות הארגון שלכם.

נציין כי המידע האמור לעיל הוא מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי, ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים שנסקרו לעיל.

עו"ד סער רוסמן, שותף
מחלקת הייטק, טכנולוגיה והון סיכון
ראש תחום סייבר ופרטיות
Saar@agmon-law.co.il

עו"ד אילן ספיר, שותף
מחלקת הייטק, טכנולוגיה והון סיכון
Ilans@agmon-law.co.il

עו"ד מתן אברמוביץ
מחלקת הייטק, טכנולוגיה והון סיכון
Matana@agmon-law.co.il

עו"ד אלעד יונתן ביטון
מחלקת הייטק, טכנולוגיה והון סיכון
Eladb@agmon-law.co.il