הפיקוח על הבנקים אגף הביקורת

י״א בתמוז תשפ״א | 21.06.2021

תוצאות הבדיקה שערך הפיקוח על הבנקים בנושא
<u>ממשל הניהול של סיכונים טכנולוגיים במערכת הבנקאית</u>

- **סיכוני טכנולוגיה מצויים במוקד תשומת הלב של הפיקוח על הבנקים, בדומה לרגולטורים מובילים בעולם. בשנים האחרונות נוצרה הסכמה רחבה כי סיכונים אלה נמצאים במגמת עלייה.**
- **הפיקוח על הבנקים נותן מענה לדאגה מהתגברות הסיכונים הטכנולוגיים במגוון אמצעים, ובכללם תהליכי ביקורת. זאת במקביל לקידום חדשנות וטכנולוגיה במגוון תחומים של עשייה בנקאית.**
- **בתהליך הביקורת שערך הפיקוח על הבנקים בשנה האחרונה נבחנו, בין השאר, איכותם של ממשל ניהול הסיכונים הטכנולוגיים, המסגרת לניהול הסיכונים ובקרתם, וכן המשאבים המוקדשים לניהולם.**
- **בתהליכים אלה זיהה הפיקוח על הבנקים מאמץ משמעותי מצד המערכת הבנקאית בניהול הסיכון הטכנולוגי, כולל סיכון הסייבר. יחידות ארגוניות רבות פועלות בבנקים בתחום של ניהול סיכונים והבקרה עליהם. עם זאת, זוהו תחומים שבהם נדרש שיפור וחיזוק, וכל בנק קיבל דרישות ספציפיות בהתאם למצבו, לדוגמה:**
  - **להמשיך ולחזק את ההבנה הטכנולוגית של הדירקטוריון.**
  - **לוודא זיהוי והערכה מלאים של מוקדי הסיכון הטכנולוגי, לרבות אמינות ושלמות נתונים (Data Integrity Risk) והסיכון הגלום בניהול השינויים (IT Change Risk) – הטמעה של טכנולוגיות חדשות ופרויקטים טכנולוגיים אסטרטגיים שהבנקים מבצעים.**
  - **לחזק את הפיקוח והמעקב אחר פרוייקטים אסטרטגיים, הכרוכים לא רק בהטמעת טכנולוגיה חדשה, אלא גם בשינויים בתהליכים ובמבנה הארגוני. מורכבות הפרוייקטים האמורים מחייבת את ניהולם בהתאם למתודולוגיה ברורה, תוך ליווי על ידי פונקציית ניהול הסיכונים הבלתי תלויה, ביקורת זמן אמת על ידי הביקורת הפנימית, ופיקוח הדירקטוריון.**
  - **דרישות לחיזוק פונקציית ניהול הסיכונים הבלתי תלויה בתחום הסיכונים הטכנולוגיים.**

מזה מספר שנים מקדם הפיקוח על הבנקים חדשנות וטכנולוגיה במערכת הבנקאית – הטמעת שירותים דיגיטליים לרווחת הלקוחות; שיפור מתמיד ברמת המערכות לצורך המשך ייעול תהליכי העבודה בבנקים, תוך שמירה על רמה גבוהה של אבטחת המידע; קידום תשתיות מידע לצורך הגברת התחרות ועידוד להטמעת טכנולוגיה חדשה בניהול סיכונים ובבקרה פנימית.

במקביל לכך מזהה הפיקוח על הבנקים עלייה משמעותית בסיכוני הטכנולוגיה במערכת הבנקאית,[1] והוא נותן לכך מענה במגוון אפיקים ואמצעים. זאת בדומה לרגולטורים פיננסיים במדינות אחרות, אשר ממקדים תשומת לב רבה בסיכון הטכנולוגי. כך, רשות הפיקוח על הבנקים באיחוד האירופאי (EBA) פרסמה מסמך עקרונות מקיף לעניין ניהול הסיכונים הטכנולוגיים.[2] גם בארצות הברית ה-OCC (רגולטור הדומה במהותו לפיקוח על הבנקים בישראל) מצביע על ההיבטים הטכנולוגיים כמוקד סיכון משמעותי.[3]

במסגרת הצעדים שנקט הפיקוח על הבנקים במענה לכך, בוצע תהליך ביקורת רוחבי במערכת הבנקאית שתכליתו לבחון את נאותות הממשל התאגידי בניהול הסיכון, את המסגרת הכללית לניהולו ואת המשאבים המוקדשים לו. רמת משילות גבוהה בניהול הסיכון הטכנולוגיה הוא תנאי הכרחי להתמודדות נאותה וארוכת טווח עמו. התהליך האמור בוצע על ידי צוות מבקרים המשלב התמחות מתחום הטכנולוגיה והתמחות מתחום הממשל התאגידי. בתהליכים אלה זיהה הפיקוח על הבנקים, לצד מאמץ משמעותי של המערכת הבנקאית בניהול הסיכון הטכנולוגי, כולל סיכון הסייבר, גם תחומים שבהם נדרש שיפור וחיזוק, ופנה לבנקים בדרישות ספציפיות ומפורטות כדי לסגור את הפערים.

סקירה זו מפרטת את הדרישות המרכזיות שהופנו לבנקים, כאמור. הפירוט שלהלן הוא מצרפי וכולל, ואינו מייצג בנק ספציפי כלשהו.

ממשל תאגידי בניהול סיכון טכנולוגי

כמקובל בעולם, תאגידים בנקאיים נדרשים לנהל את כלל הסיכונים הגלומים בפעילותם בשלושה קווי הגנה, כשלכל קו הגנה מוקצה תפקיד ספציפי ומוגדר:[4]

- **קו הגנה ראשון** – החטיבות העסקיות של הבנק, כמו חטיבה קמעונאית, חטיבה עסקית וחטיבה לנכסי לקוחות, מפעילות טכנולוגיה לצורך ביצוע עסקיהן. החטיבה לטכנולוגיית המידע, אשר מנהלת את המערכות והתשתיות הטכנולוגיות של הבנק, אף היא מהווה קו הגנה ראשון.[5] כל החטיבות בקו הגנה ראשון אחריות באופן ישיר ומרכזי לסיכונים הנובעים מפעילותן, באמצעות כלל העובדים והמנהלים, ובאמצעות יחידות בקרה וניהל סיכונים ייעודיות.

- **קו הגנה שני** – פונקציית ניהול הסיכונים הבלתי תלויה, הנפרדת מהחטיבות העסקיות. אי התלות מתבטאת בעיקרה בהעדר כפיפות ארגונית למנהלים בקו הראשון,[6] ועיצוב נאות של יעדים ותגמול, כך שייבנו בהתאם לאופיו המיוחד של תפקיד הפונקציה ובמנותק מהתוצאות העסקיות של התחומים הספציפיים הנבחנים על ידה.[7] תפקיד הקו השני הוא לקבוע מתודולוגיה ולהנחות את הקו הראשון, לאתגר את עבודתו, וכן לתכלל את המידע הנוגע לניהול הסיכונים. היחידות בקו ההגנה השני מרוכזות

---

[1] מערכת הבנקאות לישראל, סקירה שנתית 2019 – עמוד 19, איור א-10 ; מערכת הבנקאות לישראל, סקירה שנתית 2018 – עמוד 15, איור א-15 https://www.boi.org.il/he/NewsAndPublications/RegularPublications/Pages/Skira19.aspx.
https://www.boi.org.il/he/NewsAndPublications/RegularPublications/Pages/Skira18.aspx

[2] EBA Guidelines on ICT and Security Risk Management
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf?fireglass_rsn=true

[3] OCC, Semiannual Risk Perspective, Fall 2020 (09/11/2020), p. 15
https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-fall-2020.html?fireglass_rsn=true

[4] הוראת ניהול בנקאי תקין 310 בנושא ניהול סיכונים.

[5] בהתאם לסעיף 4(א) להוראת ניהול בנקאי תקין מספר 310 בנושא ניהול סיכונים, "פונקציות תומכות, כגון ניהול טכנולוגיית המידע מהוות חלק מקו ההגנה הראשון".

[6] למעט המנהל הכללי, האחראי לפעילות תקינה הן של קו ההגנה הראשון והן של קו ההגנה השני.

[7] סעיף 17 בהוראה 301A "מדיניות תגמול בתאגיד בנקאי".

בחטיבה נפרדת לניהול או לבקרת סיכונים, וכן בחטיבות אחרות שאינן עוסקות בתפקידים עסקיים, אלא בבקרה ושמירת הסף, כגון: חשבונאי ראשי ויועץ משפטי.

- **קו הגנה שלישי** – הביקורת הפנימית, אשר בודקת ומעריכה באופן בלתי תלוי את התפקוד של הקו הראשון והשני ומעריכת את הבקרה הפנימית של התאגיד הבנקאי. הביקורת הפנימית איננה כפופה למנהל הכללי של הבנק, אלא משמשת כזרוע ארוכה של הדירקטוריון.
- לדירקטוריון תפקיד מרכזי בממשל ניהול הסיכונים, כאורגן המפקח על כלל קווי ההגנה.

<u>איור א'</u> להלן מדגים באופן כללי את הממשל בניהול הסיכון הטכנולוגי.[8]

פעילותם הסדורה והאפקטיבית של כל הקווים בממשל ניהול הסיכונים באופן מצרפי מצופה לתת מענה נאות לניהול הסיכון. לפיכך, התכלית המרכזית של סבב הביקורות הייתה לוודא תפקודם התקין של שלושת קווי ההגנה והדירקטוריון גם בניהול הסיכון הטכנולוגי.

<u>איור א' – מבנה כללי של הממשל בניהול הסיכון הטכנולוגי</u>

מקור: הפיקוח על הבנקים

יישום התפיסה של שלושה קווי הגנה לגבי ניהול סיכונים טכנולוגיים עשויה להיות מאתגרת. אף כי אין חולק שהמערכת הבנקאית מנהלת את הסיכונים הטכנולוגיים, לא תמיד נשמרת ההפרדה הברורה בין קווי ההגנה. עיקרי הדרישות בנושא זה כלפי הבנקים היו לאפיין באילו קווי הגנה פועלות יחידות בקרה וניהול סיכונים שונות – האם בקו הראשון או בקו השני. להבחנה זו נודעת חשיבות בשל תפקידם השונה של קווי ההגנה ורמת אי התלות המאפיינת אותם. קו ההגנה השני נהנה מאי תלות רבה יותר, המובטחת באמצעות

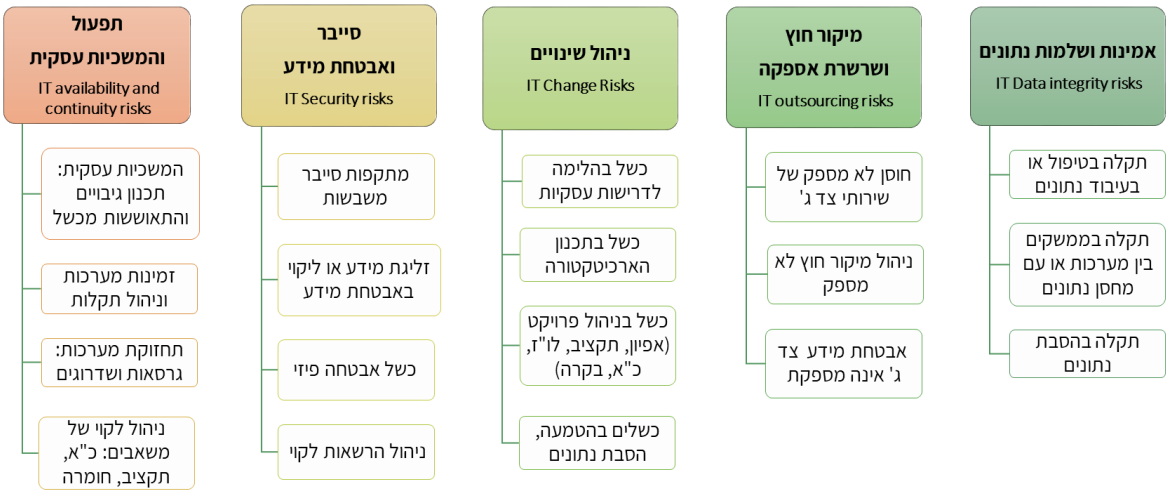
[8] המבנה הארגוני בתוך כל אחד מקווי ההגנה עשוי להשתנות מבנק לבנק, ואף חלק מהפונקציות בקו ההגנה הראשן עשוי להתבצע על ידי חברות בנות.

כפיפות ארגונית למנהלים עצמאיים ובלתי תלויים בחטיבות העסקיות,[9] וממנגנון תגמול שונה.[10] יחידה או גוף הנמצאים בכפיפות למנהל חטיבה בקו ההגנה הראשון אינה נהנית מאי התלות המספקת לצורך ביצוע תפקידי הקו השני. דרישת הפיקוח נועדה לחזק את אי התלות של יחידות בקו ההגנה השני, באמצעות מניעת כפיפותן הארגונית לחטיבות העסקיות.

הסיכון הטכנולוגי ורכיביו

תנאי מוקדם לניהול נאות של הסיכונים בכלל, וסיכון טכנולוגי בפרט, הוא זיהוי נכון של כל רכיבי הסיכון וכל מוקדי הסיכון המהותיים. משכך, נדרשים הבנקים לבחון את שלמות הרכיבים של הסיכון הטכנולוגי, ולשם כך להתעדכן בהתפתחויות המרכזיות בנושא. איור ב׳ מדגים את רכיבי הסיכון לפי המתודולוגיה של רשות הפיקוח באיחוד האירופי.

איור ב׳ - דוגמה לסיווג הרכיבים בסיכון הטכנולוגי על פי מתודולוגיה של רשות הפיקוח של האיחוד האירופי (EBA)[11]



מקור: עיבוד הפיקוח על הבנקים על בסיס המתודולוגיה של EBA.

הפיקוח על הבנקים נוכח במשאבים המושקעים לניהול רכיבי סיכון מסויימים, במיוחד סייבר ואבטחת מידע, אך בד בבד זיהה שקיימים רכיבים שדורשים הגברת מאמצים מצד התאגידים הבנקאיים. הנחה את המערכת הבנקאית לוודא זיהוי מלא של מוקדי הסיכון הטכנולוגי, כולל אמינות ושלמות הנתונים (Data Integrity) והסיכון הגלום בניהול השינויים – הטמעה של טכנולוגיות חדשות ופרויקטים טכנולוגיים אסטרטגיים שהבנקים מבצעים. מוקדים אלה זוהו גם על ידי הרגולטור האמריקאי (OCC):

---

[9] סעיף 11(ה) להוראת ניהול בנקאי תקין מספר 310, בנושא ניהול סיכונים: "פונקציית ניהול הסיכונים תהיה עצמאית דיה מקווי העסקים השונים שאת פעילויותיהן וחשיפותיהן היא בוחנת". הוראה דומה קיימת גם בהנחיות של OCC (גוף המקביל לפיקוח על הבנקים בארה"ב) בנוגע לממשל תאגידי בבנקים גדולים: " No front line unit executive oversees any independent risk management unit." (CFR Title 12, Chapter I, Part 30, Appendix D, para. E-7(d))
https://www.ecfr.gov/cgi-bin/text-idx?SID=3dcf3d2f0795de4938cb22e109ea4a0b&mc=true&node=ap12.1.30_16.d&rgn=div9

[10] הוראה 301A בנושא "מדיניות תגמול בתאגיד בנקאי".

[11] EBA Guidelines on ICT and security risk management.
https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

> While banks overall have adequate cybersecurity systems, examiners continue to identify concerns in banks related to bank information technology (IT) systems, change management and information security.[12]

נוכח מהותיות הסיכון הטכנולוגי והתגברותו, ה-OCC נותנת גם הנחיות ספציפיות ומפורטות גם לבנקים גדולים בהם התגלו חולשות בניהול הסיכון הטכנולוגי וסיכון הנתונים (Data).[13]

הדירקטוריון

לדירקטוריון וועדותיו תפקיד קריטי בפיקוח על פעילות כל שלושת קווי ההגנה, ועל הדירקטוריון למלא תפקיד זה גם בתחום הטכנולוגי. לאור מרכזיות הסיכון, פרסם הפיקוח על הבנקים הוראה כי תמהיל הכישורים של הדירקטוריון חייב להיות מותאם לאסטרטגיה של הבנק, ומכל מקום חייב לכלול לפחות דירקטור אחד בעל מומחיות טכנולוגית[14].

המערכת הבנקאית עומדת בדרישת המינימום על פי ההוראה, ובמקרים מסויימים אף מחזקת את הדירקטוריון בדירקטורים נוספים בעלי מומחיות טכנולוגית. כך באחד מהבנקים הגדולים מכהנים ארבע דירקטורים בעלי מומחיות טכנולוגית. בעקבות הביקורת, נדרשו חלק מהבנקים לבחון את האפשרות להגדיל את מספר הדירקטורים בעלי רקע טכנולוגי,[15] וזאת על רקע המסקנה כי האתגרים הטכנולוגיים מחייבים חיזוק נוסף של תמהיל הכישורים המצרפי של חלק מהדירקטוריונים. חלק מהבנקים אף פעלו מאז כדי לחזק את הדירקטוריונים, כאמור.[16]

הדרישה לחיזוק הדירקטוריונים בדירקטורים בעלי כישורים טכנולוגיים נועדה לחזק לא רק את מליאת הדירקטוריון, אלא גם את ועדותיו – הוועדה לענייני טכנולוגיית המידע וחדשנות טכנולוגית, אשר הוקמה על פי הוראת הפיקוח על הבנקים;[17] וכן ועדת הביקורת והוועדה לניהול סיכונים, אשר נדרשות לשלב גם דירקטורים בעלי מומחיות טכנולוגית.

במקביל לדרישה לחזק את הרכב הדירקטוריון כאמור, הדגיש הפיקוח על הבנקים כי האחריות לניהול הסיכון הטכנולוגי מוטלת על כלל הדירקטורים. גם דירקטורים שהרקע המקצועי שלהם אינו מתחומי הטכנולוגיה מחויבים בהבנת הסיכון האמור, בין השאר, באמצעות השלמת פערי הידע הנדרש לשם פיקוח אפקטיבי על ההנהלה, העסקת יועצים עצמאיים ובלתי תלויים בקווי ההגנה הראשון והשני, בעלי מומחיות ספציפית לפי העניין, ובאמצעות כלים נוספים שעומדים לרשותם. משכך, חשיבות רבה נודעת לביצוע תהליכים אפקטיביים של הערכה עצמית מקיפה על ידי הדירקטוריון, אשר בין השאר אמורה להצביע על חסרים בידע מקצועי, וכפועל יוצא מכך, על צורך בהשלמתם באמצעים שונים.

---

[12] OCC, Semiannual Risk Perspective, Fall 2020 (09/11/2020), p. 15
https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-fall-2020.html?fireglass_rsn=true

[13] למשל, פרק 5 (Article V: Data Governance Program, pp. 8-13) ופרק 10 (Article X: Staffing and Technology Resource Assessment), הרלוונטיות במיוחד לממשל של סיכוני הטכנולוגיה –Data, במסמך אכיפה מספר 2020-056.
https://www.occ.gov/static/enforcement-actions/ea2020-056.pdf?fireglass_rsn=true
מסמכי אכיפה מופרטים מסוג זה מאפשרים במידה מסויימת מבט על הציפיות הספציפיות של הרגולטורים בארה״ב.

[14] סעיף 25(ד) בהוראת ניהול בנקאי תקין 301 בנושא דירקטוריון.

[15] חרף הקשיים האובייקטיביים בגיוס דירקטורים כאמור.

[16] לרבות באמצעות בקשות מתאימות מהועדה למינוי דירקטורים בתאגידים בנקאיים הפועלת מכוח סעיף 36א לחוק הבנקאות (רישוי), תשמ״א-1981.

[17] סעיף 39א בהוראת ניהול בנקאי תקין 301 בנושא דירקטוריון.

קיימת חשיבות רבה לכך שתהליך הערכה עצמית של הדירקטוריון,[18] שמהווה מנגנון שיפור וחיזוק, ייעשה תוך שימוש בכלים מתודולוגיים מגוונים. כמו כל מהלך מהותי בדירקטוריון, על תהליך הערכה עצמית להסתיים בקבלת החלטות אופרטיביות, ובמעקב אחר יישומן. כך, אם בתהליך הערכה עצמית זוהה פער בידע או במידע לצורך פיקוח אפקטיבי על ניהול הסיכון הטכנולוגי, נדרש לקבל החלטות אופרטיביות על צעדים לסגירת פער זה.

בחלק מהבנקים ממצאי הסקירה הצביעו על הצורך בהמשך השיפור בתוכניות להכשרה מקצועית מתמשכת לדירקטורים,[19] ותיקים וחדשים. בחלק מהמקרים הפיקוח על הבנקים הצביע על הצורך בהרחבת הכשרות המתמודדות עם האתגרים הטכנולוגיים של הדירקטוריונים, הן בהיבט של תוכן והן בהיבט שלשעות ההדרכה המוקדשות לסיכונים הטכנולוגיים, זאת נוכח עוצמת הסיכונים שאינה שנויה במחלוקת.

קו ההגנה הראשון – יחידות ארגוניות הנותנות שירותים טכנולוגיים

בממשל ניהול הסיכונים, האחריות המרכזית לניהול הסיכונים מוטלת על קו ההגנה הראשון – במקרה של סיכון טכנולוגי, על היחידות הארגוניות העוסקות במישרין בטכנולוגיית המידע, נתונים (Data), חדשנות, וכיוצא באלה.[20] ביחידות אלה נדרשו הבנקים להשלים את הזיהוי של הגופים העוסקים בבקרה ובניהול סיכונים, ולוודא כי הוקצו להם משאבים מתאימים לביצוע תפקידם, וכי יעדיהם ותגמולם עוצבו בהתחשב במהות תפקידם הבקרתי. הדרישה משקפת את התפיסה של הפיקוח על הבנקים, כי יחידות בקרה בקו ההגנה הראשון מהוות גורם מרכזי בניהול סיכונים ובבקרה הפנימית בתאגיד בנקאי.

חשיבות עליונה נודעת גם לקיום בקרה נאותה על פרוייקטים מהותיים, לרבות בהיבטי תקציב ולוחות זמנים, תוך הפקת לקחים מחריגות במידת הצורך. הקו הראשון מחויב למסור דיווחים ברורים ומלאים אודות פרוייקטים אסטרטגיים, בהתאם למתודולוגיה של ניהול הפרויקט, כדי לאפשר לחברי ולדירקטוריון פיקוח נאות על ניהולם.

קו ההגנה השני – פונקציית ניהול הסיכונים הבלתי תלויה

הפיקוח מצא כי קיימים עדיין מספר היבטים שבהם נדרשת העמקת הפעילות של פונקציית ניהול הסיכונים הבלתי תלויה.

כך נדרשו הבנקים להקפיד על הערכה עצמאית, וכן על הצגה ברורה של כל רכיבי הסיכונים הטכנולוגיים (איור ב׳ לעיל) במסמכי הסיכונים ומסמכי הערכת הנאותות של הלימות ההון,[21] כדי לשקף תמונה ברורה להנהלה ולדירקטוריון. מסמכי הסיכונים צריכים להצביע על סוגיות הראויות לדיון בהנהלה ובדירקטוריון, וזאת בזיהוי סיכונים אפשריים במבט צופה פני עתיד.

מורכבות הפרוייקטים האסטרטגיים, הכרוכים לא רק בהטמעת טכנולוגיה חדשה, אלא גם בשינויים בתהליכים ובמבנה הארגוני, מחייבת את ניהולם בהתאם למתודולוגיה ברורה, תוך ליווי על ידי פונקציית ניהול הסיכונים הבלתי תלויה. עליה לוודא כי כל הסיכונים המהותיים של הפרויקט זוהו כנדרש על ידי קו ההגנה הראשון, ובמידת הצורך, להצביע על סיכונים שלא זוהו או לא הוערכו כנדרש.

קו הגנה שלישי – הביקורת הפנימית

---

[18] סעיף 59 בהוראת ניהול בנקאי תקין 301 בנושא דירקטוריון.
[19] סעיף 58 בהוראת ניהול בנקאי תקין 301 בנושא דירקטוריון.
[20] בהתאם להוראה 310 בנושא ניהול סיכונים.
[21] בהתאם להוראה 310 והוראה 211 בנושא הערכת נאותות הלימות ההון, בהתאמה.

גופי הביקורת הפנימית במערכת הבנקאית מבצעים את תפקידם כקו הגנה שלישי, לרבות בניהול הסיכון הטכנולוגי. הנחיות הפיקוח על הבנקים בתחום הביקורת הפנימית מוקדו בחיזוק עבודת הביקורת הפנימית בפרויקטים טכנולוגיים אסטרטגיים – המהווים מוקד סיכון טכנולוגי.

בחלק מהבנקים הביקורת הפנימית הגדירה בעבר את תפקידה בפרויקטים אסטרטגיים במונח "ליווי הפרויקט", דבר שטשטש את ההבחנה בין משימת ביקורת (Objective Assurance) לבין משימת ייעוץ (Consulting), וכן מטשטש את חלוקת התפקידים בין פונקציית הביקורת הפנימית (קו הגנה שלישי) בממשל ניהול הסיכונים, לבין פונקציית ניהול הסיכונים הבלתי תלויה (קו ההגנה השני).

במענה לכך, הבהיר הפיקוח לבנקים שהתפקיד המרכזי של הביקורת הפנימית בתאגיד בנקאי הוא ביקורת והערכה בלתי תלויה (Objective Assurance), ויש לבצעו גם בזמן אמת, קרי במהלך התנהלותו של הפרויקט האסטרטגי. ביקורת פנימית כאמור צריכה לעסוק בהיבטים השונים של ניהול הפרויקט, בהתאם להערכת הסיכונים בו.[22] תוצרי הביקורת הנעשית במקביל לביצוע הפרויקט מובאים להנהלה ולוועדת הביקורת לצורך מעקב אחר תיקון ליקויים. על פי רוב, המלצות הביקורת הפנימית מביאות לתיקון ליקויים בזמן אמת.

[22] היבטים אלה יכולים לכלול את תכנון הפרויקט, כולל התאמה למטרותיו עסקיות; אופן ניהול הפרויקט; הערכת סיכונים ואמצעי הבקרה (לדוגמה בדיקה האם הבקרות מספקות והאם נותנות מענה הולם לסיכונים); ניהול שינויים תהליכיים או מבניים בתאגיד בנקאי; ציות; מוכנות להטמעת הפרויקט, ועוד. כמקובל, ממצאי והערות ביקורת כאמור יוגשו בכתב להנהלה ולוועדת הביקורת.