

הפיקוח על הבנקים אגף הביקורת

3 באוקטובר 2021

כ"ז בתשרי תשפ"ב

2.67.2675

סקירת פעילות בנושא היערכות המערכת הבנקאית למניעה, גילוי וטיפול במעילות

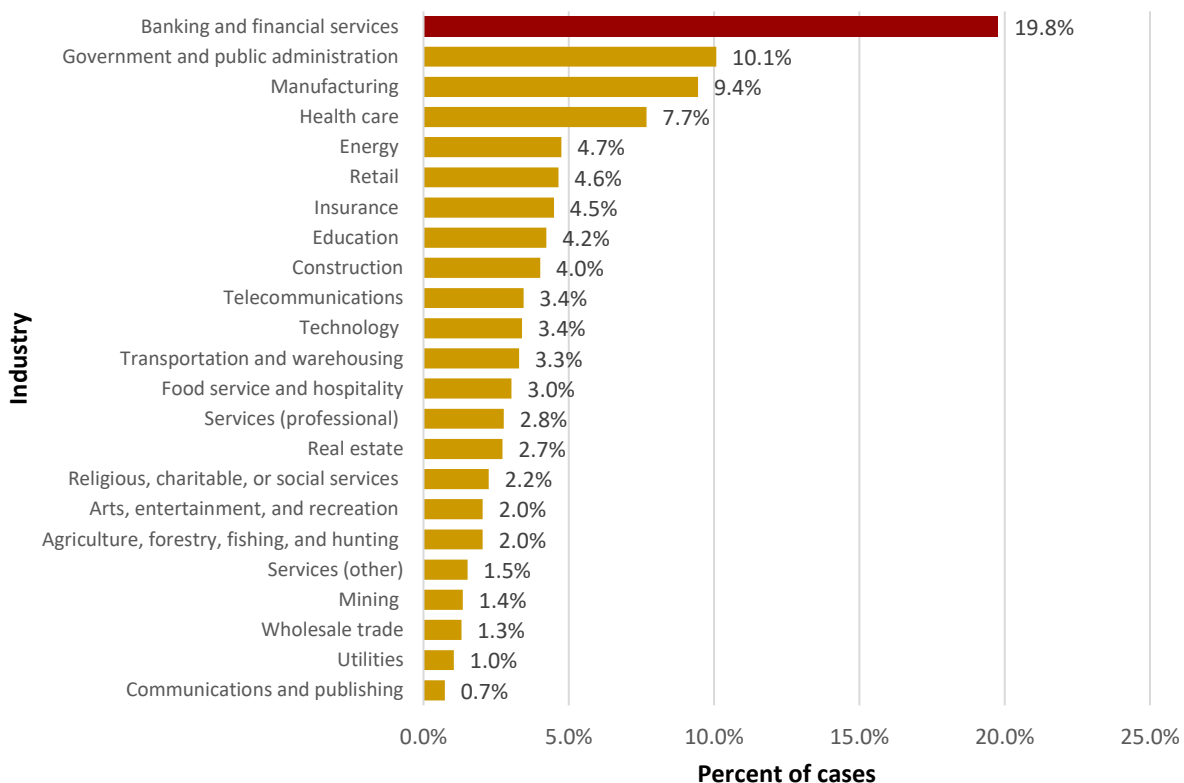
- הפיקוח על הבנקים השלים באחרונה תהליך ביקורת מערכתי בנושא בקרה פנימית בסיכון מעילות, במטרה לחזק ולשפר את היערכות הבנקים למניעת התממשות סיכון זה או צמצום נזקיו.
- הסטטיסטיקה הבינלאומית מעלה כי כל ארגון נתון לסיכון של ביצוע מעילה בידי עובדיו, מנהליו או הצדדים אחרים הקשורים אליו, והגופים הבנקאיים והפיננסיים חשופים למעילות אף ביתר שאת. למרות שלאורך קרוב לשני העשורים האחרונים לא התרחשו בבנקים בישראל מעילות משמעותיות, גופים פיננסיים במדינות אחרות חוו בשנים האחרונות אירועי מעילה משמעותיים, והסיכון לאירוע מעילה משמעותית מטבע הדברים קיים תמיד.
- תהליך הביקורת שביצע הפיקוח נועד לבחון את היערכות הבנקים להתמודדות עם סיכון זה, באמצעות בחינת הממשל התאגידי בניהול הסיכון, ההסדרים והתהליכים הקיימים בבנק והמשלבים פונקציות וגופים שונים, בקרות רוחב ארגוניות ואת סביבת הבקרה.
- הבדיקה העלתה כי המערכת הבנקאית בישראל שואפת להטמיע תרבות ארגונית של אפס סבלנות למעילות ומשקיעה משאבים רבים במניעה ובגילוי המוקדם של מעילות, ובטיפול בתוצאות של אותן מעילות שהתרחשו בפועל למרות הכל. עם זאת, במסגרת תהליכי ביקורת אלו זוהו תחומים שבהם נדרשו התאגידיים הבנקאיים להמשיך בתהליכי החיזוק של ניהול הסיכונים והבקרה הפנימית.
- ניהול הסיכון בבנקים מנוהל בפועל בהתאם לתפיסת שלושה קווי ההגנה. הבדיקה העלתה שככלל הביקורת הפנימית פעילה ומעלה ערך משמעותי בניהול הסיכון. אולם נמצאו גם תחומים שבהם נדרש חיזוק הממשל על מנת שיהיה מקיף ואקטיבי יותר. כך למשל, נמצא כי המידע שמובא בפני ההנהלה והדירקטוריון בנושא זה אינו תמיד שלם, ואינו מוכלל ומנותח די הצורך, באופן שמקשה בזיהוי מוקדי הסיכון או כשלים אפשריים בבקרה פנימית. בנוסף, בקרות הרוחב ארגוניות, כמו מנגנון חשיפת אי סדרים, לא פועלות באופן אפקטיבי בחלק מהבנקים. קיימות גישות לא אחידות לטיפול בחריגות עובדים ושיעור התלונות המתגלות באמצעות טיפ שהתקבל מעובד או באופן אנונימי נמוך בהשוואה בינלאומית. מנגנוני הרוטציה וההיעדרות הרציפה מתקיימים, ואולם לא ניתן דגש מספק לבקרות במסגרת תהליכים אלה, אשר עשויות להגביר את הסיכוי לגילוי מעילה באמצעותם.
- בעקבות התהליך שבוצע, הפיקוח הבהיר לבנקים כי עליהם ליישם תכנית פעולה אקטיבית ויזומה, כדי להעביר מסרים ארגוניים, להדריך את המנהלים והעובדים ולהכשיר את עובדי ניהול הסיכונים והבקרה, ובנוסף לאמץ סטנדרטים מיטביים המקובלים ברמה בינלאומית בהקשר זה, הפיקוח על הבנקים הבהיר שבכוונתו לחייב את היישום של מסגרת COSO העדכנית, המהווה את הסטנדרט הבינלאומי הנושא זה, בבנקים שטרם ביצעו זאת באופן וולונטרי.

בקרה פנימית בסיכון מעילות סקירה תהליך ביקורת במערכת הבנקאית

1. מבוא

כל ארגון נתון לסיכון של ביצוע מעילה בידי עובדיו, מנהליו או הצדדים אחרים הקשורים אליו. מעילה עשויה לפגוע בארגון עצמו, בלקוחותיו, בצדדים שלישיים ובאינטרסים ציבוריים. התאגידים הבנקאים אינם חריג לעניין זה, והסטטיסטיקה הבינלאומית אף מעלה כי ענף הבנקאות והפיננסים בעולם סובל מריבוי מעילות (Occupational Fraud), בהשוואה לענפים אחרים (איור 1).

איור 1 – שיעור המעילות לפי ענפים, מתוך סקירה בינלאומית¹



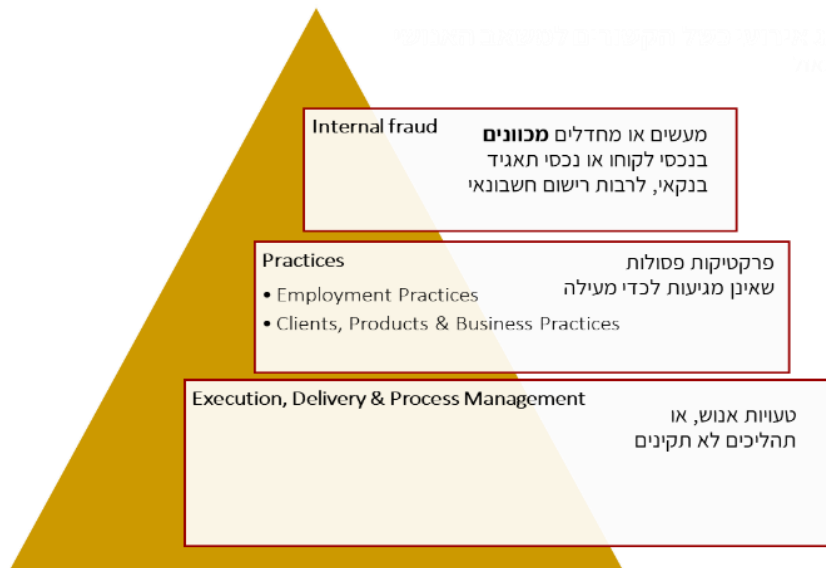
מקור: Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE, AICPA, IIA)

חלק מהסיכונים התפעוליים בכל ארגון, ובבנקים בכלל זה, נובע מעצם העובדה שארגונים מופעלים על ידי בני אדם. מעילה היא הסיכון הקיצוני ביותר הנובע מהגורם האנושי – פעילות מכוונת שנועדה לפגוע בנכסי הבנק, לקוחותיו או אינטרס ציבורי אחר. לצד פגיעה מכוונת, יתכנו פרקטיקות עבודה לא נאותות וטעויות אנוש. איור 2 מדגים באופן תמציתי סיווג אירועי כשל הנובעים מהגורם האנושי להלן, בהתאם להנחיות של ועדת באזל.²

¹ Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE, AICPA, IIA).

² הפיקוח על הבנקים החיל הנחיות אלה של ועדת באזל בדבר סיווג מפורט של אירועי הפסד, במסגרת נספח ב' להוראת ניהול בנקאי תקין מספר 350 בנושא ניהול סיכונים תפעוליים.

איור 2 - אירועי כשל תפעוליים הנובעים מהגורם האנושי



מקור: הפיקוח על הבנקים, על בסיס הנחיות באזל, שאומצו בהוראות ניהול בנקאי תקין.

המערכת הבנקאית בישראל משקיעה משאבים רבים במניעה ובגילוי המוקדם של מעילות, ובטיפול בתוצאות של אותן מעילות שהתרחשו בפועל. לאורך קרוב לשני העשורים האחרונים לא התרחשו בה מעילות משמעותיות, אשר לבנקים היה קושי אמיתי בהתמודדות עמן. עם זאת, גופים פיננסיים במדינות אחרות חוו גם בעשור האחרון אירועי מעילה משמעותיים.³ משכך, המערכת הבנקאית נדרשת להמשיך ולשמור על ערנות גבוהה כלפי אפשרות התרחשותה של מעילה מהותית ולקיים מערכי ניטור ובקרה מתאימים. נוכח זאת, הפיקוח על הבנקים השלים באחרונה סבב של תהליכי הביקורת שנועדו לבחון את מסגרת ניהול הסיכון וסביבת הבקרה הפנימית בתאגידים הבנקאים.⁴ במסגרת תהליכים אלו זוהו תחומים שבהם נדרשו התאגידים הבנקאיים להמשיך בתהליכי החיזוק של ניהול הסיכונים והבקרה הפנימית.

הפרק הראשון בסקירה זו יפרט בתמצית את ההוראות העיקריות החלות על המערכת הבנקאית בנושא זה. הפרק השני יביא בתמצית את הדרישות העיקריות שהופנו למערכת הבנקאית בעקבות הממצאים שאותרו בתהליך הביקורת שביצע הפיקוח על הבנקים.

המידע בסקירה הוא מצרפי לכלל המערכת, ואינו מאפיין אף בנק ספציפי. בנוסף לסקירה האמורה, מנהל הפיקוח על הבנקים תהליך ביקורת פרטני בכל אחד מהבנקים, ומוסר לה ממצאים ודרישות ספציפיים, ובהמשך עוקב אחר מילוי הדרישות.

³ למשל, פרשות Wirecard בגרמניה, Wells Fargo בארה"ב, בנקים בינלאומיים שביצעו מניפולציות בשוק ה-Libor.
⁴ הפיקוח על הבנקים אינו מבצע ביקורת חקירתית ואין הוא עורך ביקורת שנועדו לאתר מעילות פוטנציאליות. האחריות לביקורת ולמניעה ואיתור מעילות מוטלת על התאגידים הבנקאיים ובפרט על מנהליהם הבכירים.

2. דרישות עיקריות החלות על המערכת הבנקאית

2.1 ממשל תאגידי והמסגרת לניהול הסיכון (Risk Management Framework)

הבנקים מחויבים לנהל את סיכון המעילות בהתאם לתפיסה של שלושה קווי הגנה, בדומה ליתר הסיכונים. לכל קו הגנה, ולכל פונקציה ספציפית בכל אחד מקווי ההגנה, מוקצה תפקיד מסויים בניהול הסיכון (ראה איור 3 להלן).⁵

בקו ההגנה הראשון הנהלת כל החטיבות העסקיות נושאת באחריות מרכזית לניהול הסיכונים.⁶ לקו שני ושלישי תפקידים משלימים בלבד:⁷ בקו ההגנה השני, פונקציות בלתי תלויות,⁸ ללא כפיפות כלשהי לחטיבות עסקיות, למעט מנכ"ל, משלימות את הפעילות של קו ההגנה הראשון, באמצעות תכלול הסיכון ודיווח עצמאי להנהלה ולדירקטוריון; בקו ההגנה השלישי – הביקורת הפנימית של תאגיד בנקאי נהנית מאי תלות מוגברת גם בהשוואה לשומרי הסף האחרים – מבקר פנימי ראשי איננו כפוף, במישרין או בעקיפין, למנכ"ל של תאגיד בנקאי, אלא מהווה זרוע הפיקוח של הדירקטוריון.

יחידות ארגוניות רבות משתתפות בניהול הסיכון, ומשכך יש חשיבות גבוהה לפעילותן הסדורה והמתואמת, ובהירות לגבי תחומי האחריות והסמכות שבהן נושאת כל אחת מהיחידות. בהירות זו מושגת על פי רוב באמצעות ניסוח מסמכי מדיניות ברורים,⁹ קווי דיווח סדורים, הכשרות והדרכות, קביעת יעדים מתאימים למשתתפים והקפדה על קיום המדיניות בהתנהלות בפועל. מטרת הביקורת הייתה לוודא ניהול סיכונים בשלושה קווי הגנה, כאשר לכל אחד מהמשתתפים בניהול הסיכון בכל אחד מקווי ההגנה הוגדרה האחריות לניהול הסיכון, ניתנו הסמכויות המתאימות והוקצו משאבים נאותים. בנוסף, בדק הפיקוח את המתודולוגיה לניהול הסיכון ואת התהליכים המרכזיים.

2.2 מסגרת בקרה פנימית

הבקרה הפנימית של הבנקים נבחנה על ידי הפיקוח על הבנקים על פי מסגרת הבקרה הפנימית של COSO – יוזמה למאבק במעילות בתאגידיים של גוף המשותף ללשכת רואי חשבון בארצות הברית, לשכה בינלאומית של מבקרים פנימיים ואגודות חשבונאים נוספות בארצות הברית.¹⁰ כיום COSO מהווה סטנדרט בינלאומי מקיף ושלם, המשלב ממשל תאגידי, ניהול סיכונים ובקרה פנימית. הדגש המיוחד ניתן לבקרות רוחב ארגוניות (Entity Level Controls) – תהליכים ארגוניים רחבים אשר עשויים להקשות על ביצוע חלק מהמעילות או לסייע לגילויין בתוך זמן סביר;¹¹ וסביבת הבקרה (Control Environment) – תרבות ארגונית של משמעת והרתעה מפני התנהגות לא נאותה. סטנדרט הבקרה הפנימית של COSO מקובל על הרגולטורים המובילים בעולם. הבנקים וחברות כרטיסי אשראי בישראל מחויבים לעמוד במסגרת COSO מכוח הוראות המתייחסות לדיווח כספי והמחילות על הבנקים מקטעים מהוראות חוק ה-SOX האמריקאי.¹² כפועל יוצא מכך, מסגרת הבקרה הפנימית בתאגיד בנקאי חייבת להתייחס למכלול הסיכונים בעלי פוטנציאל השפעה, ישירה או עקיפה, על הדיווח הכספי, ובכלל זה על סיכון להתרחשות מעילה.

⁵ הדרישות האמורות נכללות בהוראה 310 בנושא "ניהול סיכונים", בהוראה 350 בנושא "ניהול סיכונים תפעוליים", ובהוראות נוספות המתייחסות לפעילויות מסוימות או לפונקציות מסוימות.

⁶ חטיבות כמו בנקאית, עסקית, נכסי לקוחות, בינלאומית ועוד.

⁷ סעיף 4(א) הוראה 310 בנושא ניהול סיכונים.

⁸ פונקציות כמו מנהל סיכונים ראשי, חשבונאי ראשי, היועץ המשפטי, קצין הציות.

⁹ מדיניות לניהול סיכונים תפעוליים, וסיכוני מעילות בפרט, מדיניות בקרה פנימית ועוד.

¹⁰ COSO Internal Control – Integrated Framework.

¹¹ כאן הכוונה לבקרות רוחב, כמו רטציה, היעדרות רציפה, קו חם לדיווח (ראה בהמשך). זאת להבדיל מבקרות ספציפיות השלובות בכל אחד מתהליכי העבודה.

¹² בהתאם להוראות הפיקוח על הבנקים, בנקים וחברות כרטיסי אשראי כפופים להוראות ה-SOX בהיקף רחב יותר בהשוואה לחברות ציבוריות רגילות.

2.3 זיהוי מעילות ודיווח עליהן

בשל החשיבות הרבה של אמון הציבור במערכת הבנקאית הוטלה על התאגידיים הבנקאיים חובה חוקית לדווח לפיקוח על הבנקים על כל חשד סביר לביצוע מעילה.¹³ הפיקוח על הבנקים מצדו מוודא את שלמות הטיפול בתוצאות המעילה על ידי הבנק (תחקור מעילה, מניעת נזקים מלקוחות, הפקת לקחים בהיבט של בקרה פנימית, ויידוע הגופים הרלבנטיים, בהתאם לעניין¹⁴), וכן מדווח מדי שנה לכנסת ולציבור נתונים כוללים על מעילות שהתרחשו במערכת הבנקאית.¹⁵ האחריות לדיוק ושלמות הנתונים אודות מעילות והטיפול בהן מוטלת על התאגידיים הבנקאיים. פקודת הבנקאות מטילה אחריות ישירה על תאגיד בנקאי ואף אחריות אישית מוגברת על מנכ"ל התאגיד הבנקאי בגין נכונות הדיווח.¹⁶ תכליתה של פעילות זו היא ליצור שקיפות ביחס לנעשה בתחום זה במערכת הבנקאית, ולוודא העדר פגיעה בלקוחות כתוצאה מאירועי מעילה שהתרחשו בפועל.

3. סיכום עיקרי תהליך הביקורת

3.1 ממשל תאגידי והמסגרת לניהול הסיכון

ככלל, המערכת הבנקאית מנהלת את הסיכונים שלה, ובכלל זה הסיכון למעילות, בשלושה קווי הגנה. עם זאת, בבנקים שונים ובעוצמות שונות נדרש שיפור וחיזוק בהיבטים המפורטים להלן.

איור 3 - דוגמה למבנה ממשל תאגידי בניהול סיכון המעילות

דירקטוריון		ועדת ביקורת	הוועדה לניהול סיכונים
מנכ"ל			קו הגנה 3
קו הגנה 1		קו הגנה 2	הביקורת הפנימית
חטיבות הבנק, המבצעות פעילות בנקאית שוטפת, וחטיבות הנותנות שירותים לפעילות זו מנהלי החטיבות והיחידות האחרות נושאים באחריות לניהול הסיכון במסגרת פעילותם		+ פונקציית ניהול הסיכונים הבלתי תלויה + חשבונאי ראשי + יעוץ משפטי + ציית	
+ חטיבה קמעונאית + חטיבה עסקית + חטיבת שווקים פיננסיים		+ עשויות להתקיים חטיבות ויחידות נוספות: • נכסי לקוחות • חדשנות • ניהול חברות בנות	
+ החטיבה לטכנולוגיית המידע + חטיבת משאבי אנוש + רכש ולוגיסטיקה + ביטחון		+ דוגמאות ליחידות בקרה בקו הגנה ראשון: • בקרת איכות • המשכיות עסקית • בקרת סיכונים	
• הגנת הסייבר • אבטחת מידע • בקרה תקציבית			

מקור: פיקוח על הבנקים

13 סעיף 178 לפקודת הבנקאות והוראת ניהול בנקאי תקין 351 בנושא "מעילות של עובדים ונושאי משרה".
 14 משטרת ישראל, כאשר קיים חשד סביר לביצוע עבירה פלילית; רשות ניירות ערך; רשויות מס וכיו"ב.
 15 סעיף 278 לפקודת הבנקאות.

16 סעיף 178 לפקודת הבנקאות. כיום תאגיד בנקאי נדרש לדווח לפיקוח על הבנקים על מעילות, כהגדרתן בסעיף 178 לפקודת הבנקאות, בהתאם להוראת ניהול בנקאי תקין 351 בנושא "מעילות של עובדים ונושאי משרה". ההוראה מתייחסת בנפרד לדיווח אירועים מהותיים. הוראת דיווח לפיקוח על הבנקים מספר 808 בנושא "מעילות של עובדים ונושאי משרה" מסדירה את אופן הדיווח. חובת דיווח לפיקוח על הבנקים לפי הוראה 351 חלה לצד חובת הדיווח על אירועים חריגים לפי הוראה מספר 301 בנושא "דירקטוריון" (ראו סעיפים 9 ו-62 (ג) בהוראה 301).

קו הגנה ראשון:

העיקרון של האחריות המרכזית של קו הגנה הראשון – מנהלי החטיבות העסקיות ודרגי ניהול נוספים – דורש המשך הטמעה וחיזוק, אף כי מסמכי המדיניות הרלבנטיים מציינים אחריות זו.

הפיקוח על הבנקים זיהה כי נדרשת תשומת לב ניהולית נוספת לבקרת סיכון המעילות בקו הגנה הראשון, ובכלל זה לתהליכים כמו זיהוי ומיפוי הבקרים שעליהם הוטלה אחריות לסיכון, לרבות עובדים שמבצעים תפקיד זה לצד משימות בקרה נוספות, הקפדה על מתן הגדרה ברורה של תחומי אחריותם וסמכותם של הבקרים; ביצוע הכשרות מתאימות.¹⁷

עוד נמצא כי המסגרת לניהול הסיכון לא מקדישה תשומת לב מספקת ליחידות ארגוניות אשר להן תפקידי מפתח בסיכון מעילות, למשל: **חטיבת משאבי אנוש**, אשר נושאת באחריות לשורה של תפקידי רוחב שלהן חשיבות מכרעת במניעת מעילות: גיוס, ניווד, בדיקות מהימנות, הדרכה, היעדרות רציפה ורוטציה, הליכי משמעת והטלת ענישה משמעתית; **יחידות שמטפלות בחשבונאות וברכש** מבצעות תפקיד בקרתי מהותי למניעת ובקרת מעילות בתחומים אלה; **לחטיבת טכנולוגיית המידע** תפקיד ייחודי בבקרת רוחב: בפיתוח בקרות ממוכנות, בקרה על הרשאות גישה למערכות, בקרות בתחום דלף מידע סייבר וכיו"ב; **נציבות תלונות הציבור**,¹⁸ המקבלת פניות ותלונות מלקוחות הבנק צריכה לדווח על כל תלונה שעלולה להצביע על התנהלות החשודה כמעילה; **מחלקת ביטחון** מבצעת תחקור בתהליכי גיוס או תחקור תקופתי, ואחראית על הגנה פיסית של מתקנים. הבנקים נדרשים להקפיד על הגדרה נאותה של תפקידי הבקרה של יחידות אלה בתחום המעילות.

קו הגנה שני:

פונקציית ניהול הסיכונים הבלתי תלויה,¹⁹ המתכללת את הסיכונים, נדרשה לחזק את פעילותה בהיבטים הבאים: לוודא שהדיווחים על מעילות ואירועים חריגים אחרים להנהלה ולדירקטוריון הינם שלמים, מקיפים ומאפשרים הסקת מסקנות לגבי הערכת רמת הסיכון, הערכת איכות סביבת הבקרה הפנימית וזיהוי חולשות שקיימות בתהליכים עסקיים ובבקרות; להביא בפני הדירקטוריון לא רק את אירועי העבר, אלא גם להצביע על חולשות העלולות להביא להתממשות סיכונים אפשריים במבט צופה פני עתיד; להוביל את המתודולוגיה לניהול הסיכון, לנתח ולצפות טיפולוגיות שונות לביצוע מעילות, ולהוביל פיתוח ושכלול של מערכות ניטור ובקרה בניהול סיכונים מהותיים; להביא לידי ביטוי את תוצרי הפעילות, כמפורט לעיל, במסמכי הסיכונים ומסמכי הערכת הנאותות של הלימות ההון,²⁰ המהווים כלי בידי הדירקטוריון בתפקידו כמפקח על פעילותם של כל קווי ההגנה בבנק.

עוד מצא הפיקוח על הבנקים כי בחלק מהמקרים המסגרת לניהול הסיכון לא מדגישה באופן מספק את תפקידן וחשיבותן של פונקציות נוספות המהוות חלק מקו הגנה השני, ובנקים מסויימים נדרשו לחדד את התפקידים שלהם כחלק מהמסגרת:

¹⁷ סעיף 10 בהוראה A 301 בנושא "מדיניות תגמול בתאגיד בנקאי".

¹⁸ נציב תלונות הציבור עשוי להיות חלק מהקו הראשון, או חלק מקווי הגנה אחרים, בהתאם להגדרה הנהוגה בבנק. הפיקוח על הבנקים הותיר את ההחלטה בדבר הכפיפות הארגונית של נציב תלונות הציבור בידי תאגידים בנקאיים. על פי הוראת ניהול בנקאי תקין A308 נציב תלונות הציבור מחויב להיות במעמד של חבר הנהלה או מדווח ישירות לחבר הנהלה. בחלק מהבנקים נציב תלונות הציבור מדווח למנהל חטיבה קמעונאית, ובחלקם ליועץ משפטי או למבקר הפנימי הראשי (בהתאם לחוק הביקורת הפנימית הותר למבקר פנימי לעסוק בבירור תלונות עובדים או לקוחות).

¹⁹ בהתאם להוראה 350 בנושא "ניהול סיכונים תפעוליים" (סעיפים 23-24), פונקציית ניהול הסיכונים התפעוליים בקו הגנה השני אחראית לשורה של היבטים מהותיים בניהול הסיכון התפעולי (אשר סיכון המעילות מהווה חלק אינטגרלי ומהותי ממנו), ובכלל זה: מדידת הסיכון התפעולי ותהליכי הדיווח; אתגור נאותות התשומות של קווי העסקים לניהול הסיכון, מדידת הסיכון ולמערכות הדיווח של תאגיד בנקאי; פיתוח והטמעה של כלים מתודולוגיים להערכת הסיכון התפעולי ומערכות לדיווח על הסיכון; תיאום הפעילויות לניהול סיכונים תפעוליים לרוחב התאגיד הבנקאי; העברת הדרכות לניהול סיכון תפעולי ומתן יעוץ ליחידות העסקיות; תיאום וקישור עם הביקורת הפנימית. חובות אלה של קו הגנה השני נגזרות גם מהוראת ניהול בנקאי תקין 310 בנושא "ניהול סיכונים".

²⁰ סעיף 736 בהוראת ניהול בנקאי תקין מספר 211 בנושא "הערכת נאותות הלימות ההון" (תהליך המכונה ICAAP) דורש מתאגידים בנקאיים ליישם בטיפולם בניהול הסיכון התפעולי קפדנות דומה לזו הנהוגה בטיפול בסיכונים בנקאיים משמעותיים אחרים (לדוגמה: סיכון אשראי).

הייעוץ המשפטי, שמלווה את הטיפול במעילה שהתגלתה, בהיבט של דיווח לרשויות המתאימות; מבצע ליווי משפטי של טיפול משמעותי; מסייע בניסוח מסמכי מדיניות ונהלים פנימיים בדבר התנהגויות לא תקינות מן ההיבט של הפרת דין או אתיקה.

פונקציית החשבונאי הראשי²¹ אף היא מהווה חלק מקו ההגנה השני²² וממלאת תפקיד חשוב במזעור הסיכון להתרחשות מעילה חשבונאית מהותית. נציין שבעשורים האחרונים מעילות חשבונאיות גרמו בחו"ל לקריסת תאגידים גדולים – דבר שהביא לחקיקה מוגברת בנושא ולמיקוד תשומת הלב של הרגולטורים בבקרה פנימית על דיווח חשבונאי. חיזוק אי התלות בגורמים עסקיים והגדרת תפקידו כשומר סף נועדו לאפשר לחשבונאי ראשי הפעלת שיקול דעת רחב גם בתחום של בקרת סיכונים מעילה.

גם **פונקציית הציות**, הכפופה על פי רוב למנהל סיכונים ראשי או ליועץ משפטי ראשי, מוגדרת כחלק מקו ההגנה השני.²³ פעילותו של קצין ציות ראשי נועדה לוודא שהתנהלות התאגיד הבנקאי ועובדיו מתבצעת בהתאם לדרישות הרלבנטיות ולנהלים הפנימיים. הפרה מכוונת של אלה, תוך ניגוד עניינים או הפקת טובת הנאה, עשויה להגיע לכדי מעילה. משכך, גם פונקציית הציות צריכה לפתח ערנות גבוהה לתחום המעילות, לדווח על חשדות סבירים ולהיות שותפה בתוכניות ההדרכה בתחום מניעת מעילות.

קו הגנה שלישי:

הביקורת הפנימית נושאת בעיקר הנטל של תחקור המעילות, זיהוי היקפן וזיהוי סיבות השורש להיווצרותן. היא ממליצה על צעדים מתקנים: צעדים משמעותיים נגד המעורבים; הסקת מסקנות בתחום האחריות הניהולית לכשל או חולשה בבקורות; השבה ופיצוי ללקוחות; הפקת לקחים ושיפורים בבקורות; ומקיימת בקרה אחר יישום המלצותיה. בתוך כך התרשם הפיקוח על הבנקים מהערך שמשיאה הביקורת הפנימית בניהול הסיכון.

בתפקידה הנוסף של הביקורת הפנימית – ביצוע הסקירה בלתי תלויה של נאותות הבקרה הפנימית בתאגיד בנקאי, דרש הפיקוח על הבנקים מהמבקרים הפנימיים להסתמך בין השאר על מידע מלא ומנותח לגבי מעילות ואירועים חריגים אחרים; תלונות ללקוחות; תלונות עובדים וגורמים אחרים, ובכלל זה תלונות אנונימיות.

עוד נדרשה הביקורת הפנימית לעגן בכתב המינוי (Charter) את הסמכות העליונה של הביקורת הפנימית בתחום ההגנה על העובדים המתלוננים מפני פגיעה אפשרית מצד גורמים כלשהם בבנק.

מנכ"ל, הנהלה בכירה ודירקטוריון:

האחריות לליקויים בפעילות התאגיד הבנקאי מוטלת על **חברי הנהלה**, כל אחד בתחומו, ומנכ"ל התאגיד הבנקאי הנושא באחריות כוללת לתפקודם התקין של כל כפיפיו, הן בקו ההגנה הראשון והן בקו ההגנה השני.

על ה**דירקטוריון** לפקח על תפקודם התקין של כל הגופים בכלל קווי ההגנה. לצורך דיון בסיכון הנובע מהגורם האנושי עליו לבחון מידע מלא, מרוכז ומנותח על מעילות ואירועים חריגים, בין השאר, על פי היקפי הנזק, דרגות חומרה וקווי הפעילות השונים, כדי לוודא שהנהלה מזהה את סיבות השורש להיווצרות הכשלים, לרבות חולשות אפשריות בבקרה פנימית, ונוקטת בצעדים מעשיים. בנוסף, על הדירקטוריון לוודא כי הנהלה נוקטת בצעדים משמעותיים הולמים כדי לייצר הרתעה מספקת.

²¹ ראו הוראת ניהול בנקאי תקין מספר 305 חשבונאי "חשבונאי ראשי".

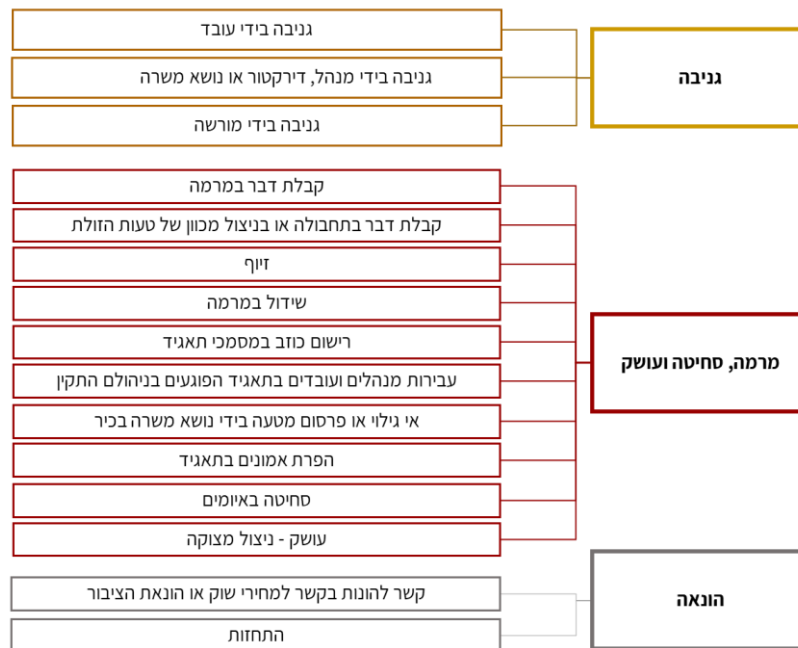
²² סעיף 4(ב) להוראת ניהול בנקאי תקין בנושא "ניהול סיכונים".

²³ סעיף 4(ב) להוראת ניהול בנקאי תקין מספר 310 בנושא "ניהול סיכונים"; סעיף 6 להוראת ניהול בנקאי תקין מספר 308 בנושא "ציות ופונקציית הציות בתאגיד בנקאי".

3.2 אפיון הסיכון

בבדיקת מסמכי המדיניות של הבנקים זיהה הפיקוח על הבנקים בחלק מהמקרים כי המושג "מעילה" מוגדר באופן עמום ובחסר. ככל שהובאו דוגמאות מסוימות, הן היו בדגש משמעותי על "גניבת כסף" מבנק או מלקוחות. זאת, בשעה שפקודת הבנקאות מגדירה כ-"מעילה" לא רק עבירות גניבה, אלא גם רשימה ארוכה של עבירות על חוק העונשין לרבות קבלת דבר במרמה או בתחבולה, זיוף, רישום כוזב, הפרת אמונים ועבירות נוספות (איור 4).

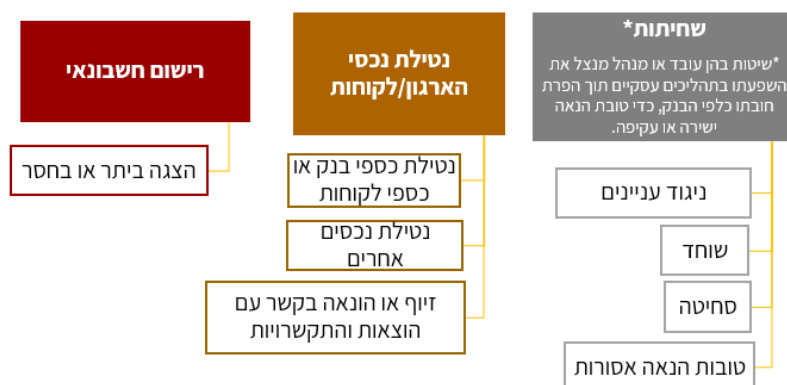
איור 4 – סוגי עבירות לפי חוק העונשין המהוות מעילה



מקור: פיקוח על הבנקים

סיווג של מעילות כפי שהוגדר על ידי המחוקק בפקודת הבנקאות, תואם גם את הסיווג שנהוג בקרב המומחים למניעת וחקירת מעילות בעולם, לפיו מחולקות המעילות ל-3 קטגוריות עיקריות: גניבה (Asset Misappropriation), שחיתות²⁴ (Corruption) ומעילה בדיווח חשבונאי (Financial Statement Fraud). איור 5 מדגים את הסיווג בתמצית:

איור 5 – סוגי מעילה תעסוקתית, על פי סטנדרט בינלאומי



מקור: Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE, AICPA, IIA); עיבוד: הפיקוח על הבנקים

²⁴ בהתאם לפסיקת בית המשפט העליון, לעניין עבירת שוחד, דין עובד בנק כעובד ציבור – ע"פ 122/84 מנצור נגד מדינת ישראל (1984).

אי בהירות או טעות באשר למצבים העלולים להגיע לכדי מעילה, עלולה לפגוע בזיהוי מעילות ובטיפול בהן, וכן בשלמות התמונה המדווחת להנהלה ולדירקטוריון, וכפועל יוצא מכך להחליש את ניהול הסיכון בכללו. גישות לא אחידות לסיכון המעילות בבנקים עלולות גם לפגום בשלמות התמונה המתקבלת בפיקוח על הבנקים לגבי הערכת הסיכון.

הבנקים נדרשו אפוא לחזק את המתודולוגיה לניהול הסיכון, ובכלל זה להבהיר ולחדד את אפיון הסיכון. בנוסף, נדרשו הבנקים להדריך את המנהלים ואת העובדים לגבי מגוון סוגי התנהגות פסולה העלולה להגיע לכדי מעילה, ולחדד את הציפייה לדיווח על התנהגויות אלה. בכל מקרה של ספק לגבי התקיימותן של יסודות העבירה על הבנק לפעול לפי ניתוח משפטי

3.1 בקורת רחב ארגונית

לצד בקורת ספציפיות המוטמעות בכל פעילות עסקית, ומתבטאות לעיתים בבקרת מנהל או בקר ספציפי, הפרדת סמכויות, או בקורת ייעודיות באמצעות מערכות מידע, על הארגון ליישם בקורת רחב ארגונית, כמו: אנליטיקה לעסקאות או פעולות בזמן אמת או בדיעבד, בקרה על מנגנוני קביעת יעדים ותגמול, בדיקות רקע בעת גיוס ומעבר לתפקידים רגישים או בדיקות תקופתיות, מנגנון דיווח וחיפה (Whistleblowing), טיפול בתלונות לקוחות, עובדים ומתלוננים נוספים, ראיונות בעת פיטורי עובדים או התפטרות. אמצעי בקרה נוספים, יכולים לכלול, בהתאם למאפייני סיכון והבקורת הקיימות, ביצוע רוטציה בתפקידים רגישים וחובת היעדרות רציפה ומבוקרת תוך מילוי ממלא מקום.²⁵

מרבית הכשלים המהותיים של הגורם האנושי (מעילות והפרות חמורות אחרות) התגלו באמצעות בקורת ניהוליות או באמצעות פעילותם של גופי הביקורת והבקרה. נתח מסויים מהכשלים מתגלה בעקבות הטיפול בתלונות לקוחות. שיעור נמוך מאוד של אירועים התגלה בעקבות תלונה של עובד או דיווח אנונימי. מדובר לכאורה בשיעור נמוך יחסית לעומת המדווח בתחום זה בסקירה בינלאומית.²⁶

הדירקטוריונים של הבנקים חויבו לוודא קיומם של מנגנונים המעודדים דיווח על מעילות והפרות מהותיות אחרות (Whistleblowing), תוך מתן הגנה לעובדים המתלוננים, וכן להטמיע את מנגנון הטיפול בתלונות, לרבות תלונות אנונימיות, לצורך הערכת האפקטיביות של בקורות וביקורות.²⁷ בהתאם למסגרת הבקרה הפנימית של COSO, מנגנוני הדיווח מהווים בקרת רחב בעלת אפקטיביות משמעותית באיתור כשלים וביצירת הרתעה. גם בסקירות בינלאומיות²⁸ נודעת לטיפ המתקבל מעובדים, ספקים, לקוחות ואחרים משמעות קריטית באיתור מעילות.

הפיקוח על הבנקים דרש מחלק מהבנקים לפעול להמשך הגברת האפקטיביות של מנגנוני איתור מעילות וארועים חריגים באמצעות עידוד השימוש ב-"קו החם", תוך מתן אפשרות רחבה להגשת תלונות אנונימיות. בכלל זה, על הבנקים לוודא שערוצי הדיווח מתאימים ונגישים לכלל עובדים וכן לגורמים חיצוניים – לקוחות, ספקים ומתחרים. תאגידים בנקאיים מצופים להעביר מסרים ארגוניים בדבר ציפייה חד משמעית לדווח על מעילה או הפרה מהותית – ("Say something if you see something"), ועידוד לחשוף שיטות ביצוע, להבדיל מזהות החשודים, דבר שעשוי לעודד דיווח גם בקרב אנשים הסולדים מהלשנה, כביכול. חשיפת שיטת ביצוע תאפשר לגורמי הבקרה והביקורת לבדוק את החשד. קיימת חשיבות רבה להבטחת הגנה מפני פרסום זהותו של המתלונן והגנה אפקטיבית מהתנכלות, במידת הצורך, בהתאם למתודולוגיה בינלאומית מקובלת, ותוך שילוב בתקשור הארגוני של מידע ברור על הגנות כאמור.

²⁵ הוראת ניהול בנקאי תקין מספר 360 בנושא "רוטציה וחופשה רציפה".

²⁶ דיווחים שנתיים של ארגון המבקרים החקירתיים הבינלאומי, בפועל בשיתוף עם איגוד המבקרים הפנימיים ולשכת רואי החשבון האמריקאית: Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE, AICPA, IIA)

²⁷ סעיפים 15(ג) ו-36(ו) להוראה 301.

²⁸ Report to the Nations – 2020 Global Study on Occupational Fraud and Abuse; Association of Certified Fraud Examiners (ACFE, AICPA, IIA)

רוטציה והיעדרות רציפה בתפקידים הרגישים: התאגידים הבנקאיים מקפידים ככלל על תהליכי רוטציה והיעדרות רציפה בתפקידים הרגישים. עם זאת, יש להמשיך ולחזק את השילוב ואת התיאום בין הגדרת תפקידים רגישים לצרכי רוטציה והיעדרות רציפה, לבין תהליך מתמשך ושוטף של זיהוי מוקדי סיכון. בנוסף, נדרשו התאגידים הבנקאיים להגביר את הבקרה (כניסה למשרדים או גישה למערכות) אחר עובדים בתפקידים רגישים שיצאו להיעדרות רציפה, ולהקפיד באופן מיוחד על מינוי ממלא מקום.

סביבת הבקרה

כפי שכבר נאמר, המונח סביבת הבקרה מתייחס להטמעת תרבות ארגונית של ציות ומשמעת ארגונית, במיוחד בתחום ניהול הסיכונים וביצוע הבקרה הפנימית, חוסר סבלנות כלפי עבירות והפרות, ויצירת אווירה של הרתעה, לצד תמריצים חיוביים שנועדו להגביר ניהול סיכונים ובקרה פנימית. בין כלל האמצעים המייצרים סביבת הבקרה ניתן למנות מסרים ומעשים בפועל של הדירקטוריון והנהלה, מנגנון משמעת מרתיע, טיפול במניעת ניגודי עניינים, אתיקה ארגונית ומקצועית, קמפיינים חינוכיים והדרכות לעובדים ומנהלים, הדרכת לקוחות, עידוד חשיפה של מעילות והפרות.²⁹ על ממצאי הפיקוח העלו כי בכלל התאגידים הבנקאיים מתקיים **מנגנון משמעת**, המבצע בפועל אכיפה פנימית. על התאגידים הבנקאיים להמשיך ולפעול להטמעת סביבת הבקרה והגברת הכוח ההרתעתי של האכיפה הפנימית, לצד עידוד ערנות בקרתית של עובדים באמצעות תמריצים חיוביים.

על הנהלת הבכירה של תאגיד בנקאי לוודא קיום **הדרכות עובדים ומנהלים** בנושא סיכון תפעולי, כאשר הסיכון להתרחשות מעילות מהווה חלק אינטגרלי ומהותי מהסיכון התפעולי.³⁰ הפיקוח על הבנקים חידד את ציפייתו להרחבה וחידוד של הדרכת עובדים ומנהלים בתחום מניעת מעילות, תוך מתן קווים מנחים ברורים לגבי סוגי ההתנהגות העשויים להוות מעילה, הצפת התנהגויות שעשויות להדליק נורה אדומה בקרב מנהלים ועמיתים, ותוך הדגשת העדר סובלנות לסוגי התנהגות אלה.

4. סיכום

המערכת הבנקאית שואפת להטמיע התרבות של אפס סבלנות כלפי מעילות, ומשקיעה מאמצים ניכרים לצורך כך. ציפיית הפיקוח על הבנקים היא כי המערכת הבנקאית תמשיך לשמור על ערנות גבוהה ומתמדת כלפי אפשרות התרחשותה של מעילה מהותית, ותחזק ותשכלל את מערכי ניטור הסיכונים והבקרה הפנימית, ותאמץ בעניין זה את הסטנדרטים הבינלאומיים הגבוהים ביותר (כמו מסגרת בקרה פנימית של COSO).

הבנקים פועלים על פי מסגרת הבקרה הפנימית של COSO 1992, ורק חלקם הטמיעו את המסגרת המעודכנת מ-2013. בחלק מהבנקים נמצאו חולשות ביישום הסטנדרטים שהוטמעו, הלכה למעשה. דרישות הביקורת חידדו את הצעדים שיש לנקוט בהם כדי לצמצם את הפערים.

כאמור, מכתבי הדרישות שנשלחו לבנקים מפרטות את הצעדים הספציפיים שיש לנקוט בהם לסגירת הפערים. בהמשך לביקורת בכוונת הפיקוח על הבנקים לחייב אימוץ של מסגרת COSO העדכנית באמצעות רגולציה מתאימה, כדי ליצור מחויבות לכך בבנקים שטרם ביצעו זאת באופן וולונטרי.

²⁹ OCC, Operational Risk: Fraud Risk Management Principles, 2019-37, p. 4-6.

³⁰ סעיף 8 להוראה 350 בנושא "סיכונים תפעוליים".