ביקורת פנימית וניהול סיכונים מתחרים או משתפי פעולה

מאת **יוסי גינוסר,** רו"ח, CIA, CFE, CRMA
עמית גרידי, MA

בדיקה מחודשת לאור פרסום טיוטת המסמך Enterprise Risk Management - Aligning Risk with Strategy and Performance על ידי ארגון ה-COSO בשנת 2016, ופרסום המסמך Proposed Changes to the Standards על ידי ה-IIA, אשר עתיד להיכנס לתוקף בשנת 2017

"אין התחמקות מסיכונים. יש להכיר
אותם, לנהל אותם ולהחליט את מי מהם
ניתן להשאיר בעוצמתו ומי דורש טיפול
להקטנתו או סילוקו"

פרופ' טרוור קלץ

משפט זה מתמצת את הצורך בניהול סיכונים אפקטיבי בארגון. אם לא ננהל את הסיכון, הסיכון ינהל אותנו. אם ננהל אותו, נשלוט בו ונקטין את ההסתברות שיפגע בנו. משפט זה נכון למנהלי סיכונים בדיוק כמו שהוא נכון למבקרים פנימיים.

מנהלי סיכונים בארגונים

עד לאחרונה, מנהלי סיכונים פעלו בעיקר בגופים פיננסיים ובחברות ממשלתיות, זאת מתוקף רגולציות המחייבות אותם לפעילות זו. מנהל סיכונים, בארגונים אשר אינם נדרשים להעסיק כזה, היה נדיר. כתוצאה מכך, לא היו ארגונים רבים בהם מבקר פנימי ומנהל סיכונים עבדו בכפיפה אחת והיו צריכים לשתף פעולה ביניהם ואילו בארגונים בהם פעלו שני נושאי משרה אלו, פעמים רבות התקשורת ביניהם התמצתה בממשקים ספציפיים, כגון עזרה למיישם ה-SOX או שיתוף מידע נקודתי.

לאחרונה, יותר ויותר ארגונים אשר אינם נדרשים למשרת מנהל סיכונים סטטוטורית, החלו להעסיק מנהלי סיכונים. כתוצאה מכך, ומהעובדה ששני נושאי משרה אלו משחקים תפקיד מרכזי בממשל התאגידי של הארגון ומחזיקים במידע רב ערך על סיכוני הארגון והבקרות שבו, נוצר צורך מוגבר בשיתוף פעולה.

ראיינו בעניין זה את גב' רונית בירן, המבקרת הפנימית של שיכון ובינוי מקבוצת אריסון, אשר בראיון שקיימנו עמה פירטה מניסיונה "כיום, יותר ויותר מבקרים פנימיים משכילים להבין את היתרון שבשיתוף פעולה עם מנהל הסיכונים של הארגון. בשיכון ובינוי אנחנו דואגים לקיים פגישות חודשיות שוטפות בין מחלקת הביקורת לבין מחלקת ניהול הסיכונים. רמת שיתוף הפעולה גבוהה, ומתקיים תהליך קבוע של הפריה הדדית והיזון חוזר בין המחלקות. הביקורת הפנימית נעזרת בסקר הסיכונים אשר בוצע על ידי מנהלת הסיכונים לצורך קביעת תוכנית העבודה השנתית. במקביל, מחלקת ניהול הסיכונים נעזרת במחלקת הביקורת לצורך הערכת סבירות הסיכון המבוססת גם על הערכת אפקטיביות הבקרות הקיימות בארגון המבוצעת ע"י הביקורת. כמו כן, בכוונת הארגון להקים פורום מקצועי משותף אשר יכלול את הביקורת הפנימית, ניהול סיכונים, ציות ואכיפה ומנהלת הבקרה. בתחומי הביקורת וניהול סיכונים קיימת חפיפה מסוימת בין שתי המחלקות והחכמה היא לדעת כיצד לנצל את אגירת הידע מבלי להעיק על היחידות המבוקרות, מתוך מטרה משותפת לעזור לארגון לעמוד במטרותיו."

ניהול סיכונים - Best Practice

במאמר משנת 2005 של לשכת המבקרים הפנימיים העולמית (IIA) בנושא תפקיד הביקורת הפנימית ביישום סעיפים 302 ו-404 ל-SOX , נכתב כי התקנים הבינלאומיים למקצוע הביקורת הפנימית, דורשים מהמבקר הפנימי להעריך את תהליכי ניהול הסיכונים, הבקרה והניהול של הארגון באמצעות פעילויות ייעוץ וביקורת, וכן לתרום לשיפור תהליכים אלו. הכותבים ידעו כבר אז כי לא ניתן להתעלם מהמטרות הדומות של הביקורת הפנימית וניהול הסיכונים. לפיכך, קבעו התקנים תפקיד דואלי למבקר הפנימי בהיבט של ניהול סיכונים: ייעוץ וביקורת. לדוגמה, כאשר מתבצעת ביקורת בנושא רכש, ייבדקו היבטי ניהול הסיכונים של החברה בתהליך זה. במקביל, על המבקר הפנימי לייעץ להנהלה כיצד לשפר את תהליך ניהול הסיכונים.

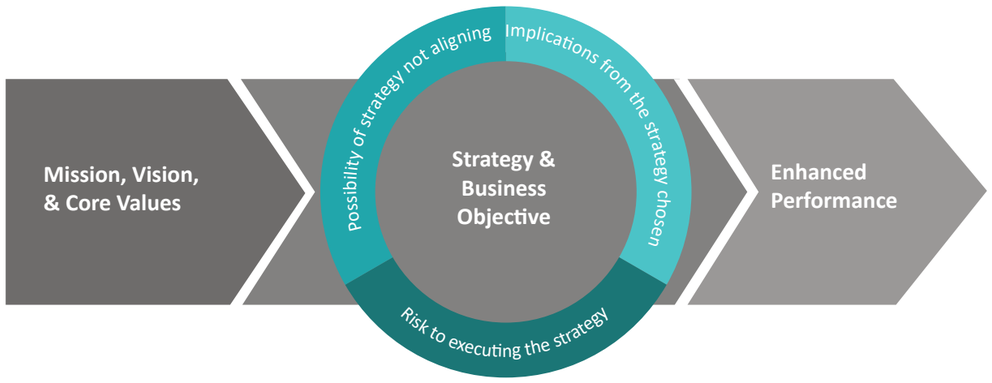
בשנת 1992 פרסם ארגון ה- COSO (Committee of Sponsoring Organizations) מסמך ראשון הנוגע ליישום של בקרות פנימיות בארגונים. במסמך זה הופיעו לראשונה 5 רכיבי בקרה אשר חיוניים למערכת בקרה פנימית טובה. מכיוון שרוב רובן של החברות אשר נדרשו ליישם SOX בחרו ב-COSO כמתודולוגית הבקרה שלהן, הן נדרשו לתעד ולהעריך את טיב ניהול הסיכונים כרכיב בקרה מרכזי. בשנת 2013 פרסם ארגון ה-COSO מסמך מעודכן בנוגע לבקרות העל בחברות.

מסמך זה הרחיב את 5 רכיבי הבקרה ל-17 עקרונות, מתוכם ארבעה עקרונות הרחיבו את מושג ניהול הסיכונים, והם:

- הארגון מזהה סיכונים הקשורים ליעדיו;
- הסיכונים מנותחים על מנת לקבל החלטה כיצד לנהלם;
- הארגון שוקל את החשיפה למעילות בהערכת הסיכונים שביצע;
- הערכת הסיכונים כוללת זיהוי השינויים העלולים לפגוע באפקטיביות מערך הבקרה הפנימית.

בעקבות מסמך זה, ניהול הסיכונים התקדם צעד נוסף לקדמת הבמה. יש לציין כי המסמך נועד לשימוש ההנהלה וגורמי הבקרה בארגון (כולל המבקר הפנימי ואחראי ה-SOX) אך לא למנהלי הסיכונים.

בשנת 2016 ארגון ה-COSO פרסם טיוטת מסמך ייעודי לעניין ניהול סיכונים הכולל 23 עקרונות לעניין ניהול אפקטיבי של תהליך ניהול סיכונים בארגון. העקרונות במסמך מחולקים לחמש קבוצות - סיכוני ממשל תאגידי, סיכונים אסטרטגיים, סיכוני ביצוע, סיכוני תקשור מידע וסיכונים הנוגעים לניטור מערכת ניהול הסיכונים של הארגון. מסמך זה הוא המשך ישיר למסמך אשר פורסם על ידי הארגון בשנת 2004 והיווה בסיס לניהול הסיכונים של ארגון. מעיון בטיוטת המסמך משנת 2016, אנו יכולים לזהות דפוס לתוצרי ארגון ה-COSO אשר כוללים חלוקה לקבוצות ושיוך של תתי תהליכים לתהליכי על. כמו כן, ניתן לזהות כי ארגון ה-COSO נותן דגש רב בניהול הסיכונים לאסטרטגיה ויעדיו העסקיים של הארגון, כפי שמשתקף בתרשים המסביר את עקרון ניהול הסיכונים של הארגון:



זווית ראייתו של המבקר הפנימי

כידוע, אחת ממטרותיה של הביקורת הפנימית היא לאפשר לארגון לעמוד ביעדיו על ידי זיהוי סיכונים, מעקב אחר צמצומם ושיפור מערך הבקרה. עולה השאלה האם קם לפונקצית הביקורת הפנימית מתחרה? והאם על המבקר הפנימי להימנע מניהול סיכונים? שהרי חוק הביקורת הפנימית קובע במפורש כי "מבקר פנימי לא ימלא, בגוף שבו הוא משמש מבקר, תפקיד נוסף על הביקורת הפנימית, זולת תפקיד הממונה על תלונות הציבור או הממונה על תלונות העובדים, ואף זאת - אם מילוי תפקיד נוסף כאמור לא יהיה בו כדי לפגוע במילוי תפקידו העיקרי". יתרה מכך, תקני ה-IIA, אשר נוגעים לעניין אי תלותו של המבקר הפנימי, קובעים כדלקמן:

- תקן 1100 בדבר אי תלות ואובייקטיביות קובע כי "פעילות הביקורת הפנימית חייבת להיות בלתי-תלויה, ומבקרים פנימיים חייבים להיות אובייקטיביים בביצוע עבודתם".
- תקן 1110 בדבר אי תלות ארגונית קובע כי "המבקר הפנימי הראשי חייב לדווח לרמה הארגונית, המאפשרת לביקורת הפנימית למלא את אחריותה. המבקר הפנימי הראשי חייב לאשרר בפני הדירקטוריון, לפחות אחת לשנה, את אי התלות הארגונית של הביקורת הפנימית".

מהאמור בתקנים לעיל ופירושם, ניתן להבין כי על מנת שעבודת הביקורת תיעשה בצורה ראויה, מקצועית ונאותה, על המבקר הפנימי להיות נקי מכל תלות ארגונית ואפילו נפשית.

תקן 2120 של לשכת המבקרים הפנימיים העולמית (IIA) בנושא ניהול סיכונים קובע כי: "הביקורת הפנימית חייבת להעריך את האפקטיביות, ולתרום לשיפור תהליכי ניהול סיכונים".

ה-IIA דן בסוגיה זו במסמך טיוטה אשר עתיד להיכנס לתוקף בשנת 2017. יש להסתייג ולהגיד כי טיוטת תקן זו עשויה לעבור עוד שינויים וכי הוועדה המקצועית של IIA ישראל טרם תרגמה את התקן לעברית והתאימה אותו לישראל. אחד מהתקנים החדשים המפורטים במסמך עוסק בתפקידיו של המבקר הפנימי מעבר לביקורת הפנימית. מדובר בתקן מקצועי 1112 "Chief Audit Executive Roles Beyond Internal Auditing". התקן מספק דוגמאות לתפקידים נוספים אשר לעיתים מצופה מהמבקר הפנימי לבצע בארגון כגון - תפקידי ציות וניהול סיכונים. ה-IIA השכיל להבין כי המקצוע דינמי וכאשר הפרקטיקה דורשת, יש לעדכן את התקנים המקצועיים בהתאם. הארגון מבקש להכין את המבקר הפנימי לעולם החדש, מצייד אותו בסט כלים חדישים ועדכניים אשר עתידים לספק לו את היכולת לבצע את עבודתו בצורה מיטבית ומאפשר לו לממש את יעדי הביקורת בצורה הטובה ביותר עבורו ועבור הארגון בו הוא פועל.

להלן ההסבר שנותן ה-IIA לתקן החדש:

The chief audit executive may be asked to take on additional roles and responsibilities outside of internal auditing, such as responsibility for compliance or risk management activities. These roles and responsibilities may impair, or appear to impair, the organizational independence of the internal audit activity, or the individual objectivity of the internal auditor. Safeguards are those oversight activities, often undertaken by the board, to address these potential impairments, and may include such activities as periodically evaluating reporting lines and responsibilities, and developing alternative processes to obtain assurance related to the areas of additional responsibility.

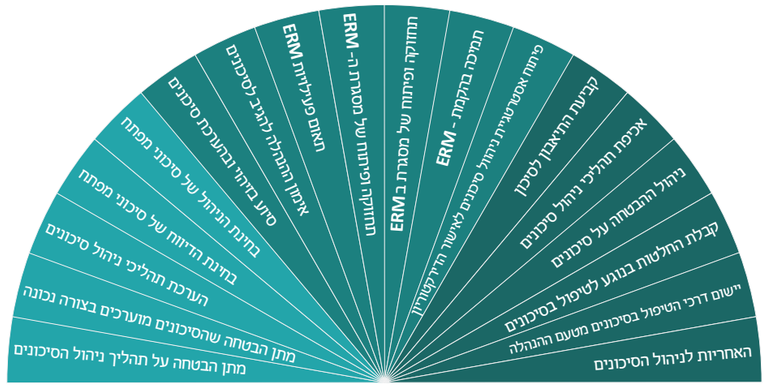
חוק הביקורת הפנימית קובע כי "המבקר הפנימי יערוך את הביקורת על פי תקנים מקצועיים מקובלים". מכיוון שתקנים אלו נקבעים ומעודכנים באופן שוטף על ידי ה-IIA, אשר מאפשר סיוע של המבקר הפנימי להנהלה בתחומים נוספים, חוק הביקורת הפנימית מאפשר סיוע של המבקר הפנימי לארגון בתחום ניהול הסיכונים.

יחד עם זאת, אל לו למבקר הפנימי לקבל על עצמו סיוע להנהלה בתחום ניהול הסיכונים אם הוא נעדר את הכישורים המתאימים בתחום זה. ואכן, תקן C1.1210 קובע כי המבקר הפנימי חייב לסרב לפעילות ייעוץ או להשיג את המומחיות הנדרשת בהיעדר ידע וכישורים הדרושים לביצוע פעילות הייעוץ או חלקים ממנה.

לדעתנו, אין בכוונת ה-IIA לטעון כי מבקר פנימי יכול וצריך לשמש גם כמנהל סיכונים של ארגון. אך המצב כיום הוא כזה שברוב הארגונים לא קיימת פונקצית ניהול סיכונים. בארגונים אלו, אל לו למבקר הפנימי להמתין עד שיאוש תפקיד זה, ובינתיים להותירו פרוץ. מכיוון שממילא תפקידו כרוך בהערכת סיכונים וצמצומם, שומה עליו לסייע להנהלת הארגון באמצעות התייחסות לנושא של ניהול הסיכונים אגב ביצוע ביקורות פנימית. ראשית, עליו לוודא שמבוצע סקר סיכונים אשר אמור לתת מענה לכלל סיכוני הארגון. לאחר מכן, כאשר המבקר מבצע ביקורת בחברה, עליו לזהות את מטרות היחידה המבוקרת, לאתר סיכונים פוטנציאלים לאי עמידה ביעדים אלו, ולבדוק את

עיצוב ואפקטיביות הבקרות שנועדו לטפל בסיכונים אלו.

התרשים הבא לקוח מתוך נייר עמדה שפורסם על ידי לשכת המבקרים הפנימיים העולמית. הוא מתאר את מגוון פעילויות ניהול הסיכונים התאגידי ומציין אלו פעילויות רצוי שיבוצעו על ידי הביקורת הפנימית, כאלה שהן לגיטימיות לביצוע על ידי הביקורת הפנימית וכאלה שרצוי כי הביקורת הפנימית לא תבצע.



סיכום

כאשר קיים מנהל סיכונים בארגון, המבקר הפנימי חייב לשתף עמו פעולה באופן שוטף ומלא. לא עוד שני תהליכים שונים ונפרדים אלא תהליכים משיקים ושלובים. על מנת להמחיש את הסיטואציה, יש לחשוב על מרוץ שליחים כאשר הביקורת הפנימית ומחלקת ניהול הסיכונים הינם שני רצים באותה הקבוצה. שיתוף פעולה מושלם יתקיים כאשר המקל יעבור מהרץ הראשון לשני, שיתוף פעולה כושל יהיה כאשר שניהם ירוצו במקביל ויתחרו ביניהם. קביעת תוכנית עבודה שנתית אינה עוד נגזרת של סקר סיכונים עצמאי שביצע המבקר, במנותק מסקר הסיכונים הכלל ארגוני שביצע מנהל הסיכונים, אלא תוצאה של חשיבה משותפת אשר אמורה לשקף התחשבות בזוויות הראייה השונות. גם לאחר קביעת תוכנית העבודה של המבקר הפנימי, עליה להיות דינמית וכאשר עולה הצורך, יש לשקול לשנותה, בעקבות ממצאים חריגים הנובעים מניהול הסיכונים השוטף של החברה. בנוסף, כאשר ניגשים להוציא ביקורת לפועל, בטרם יושבים עם המבוקרים לשיחת פתיחה, יש להבין כיצד התייחס תהליך ניהול הסיכונים של החברה לנושא המבוקר ומה היו ממצאיו. כמובן שהיזון חוזר דומה יבוצע בעבודת ניהול הסיכונים - על מנהל הסיכונים לעיין בדוחות המבקר הפנימי כדי לזהות השלכות על מערך ניהול הסיכונים בארגונים המבצעים SOX, על המבקר הפנימי ומנהל הסיכונים לעיין בתוצאת תיקוף הבקרות, אשר תעשיר את עבודתם. על שיתוף הפעולה להחל ביצירת יחסי אמון, על מנת שפונקצית ניהול הסיכונים תהיה נכונה לחשוף בפני הביקורת את תהליכי ניהול הסיכונים שהיא מבצעת, ועל מנת שניהול הסיכונים ירצה בקבלת ערך מוסף מהביקורת הפנימית. עם זאת, יש לזכור כי יתכן שלא קל יהיה למנהל הסיכונים לקבל את העובדה כי המבקר, אשר עמו הוא משתף מידע באופן קולגיאלי, עשוי להידרש לבצע עליו ביקורת בעתיד.

במאמר זה ביקשנו להראות כי רב הדומה על השונה בתהליכי ביקורת פנימית וניהול סיכונים. שיתוף פעולה בין תהליכים אלה והגורמים האחראים עליהם יכול להניב לארגון ערך רב. האם יום אחד התחומים ישתלבו לאחד? כנראה שלא. המבקר הפנימי מחזיק בתפקיד בקרת העל בארגון. זוהי בקרה הבודקת את כל שאר הבקרות. ניהול הסיכונים הינו אחת מבקרות הארגון, וכשכזה, הוא כפוף לביקורתו של המבקר הפנימי. עם זאת, כתוצאה מכלי העבודה והמטרות הדומות, על מבקרים פנימיים ומנהלי סיכונים לשתף פעולה ככל הניתן, להבין את הצרכים זה של זה ולסייע האחד לשני במקרה הצורך, להיעזר בדוחותיו האחד של השני ולהבין כיצד המידע המשותף יכול לעזור לארגון לעמוד במטרותיו ויעדיו.