מודל ה-COSO ERM

אורי גלאור, ARM

בשנת 1992 הופץ ע״י ה- COSO מודל מובנה של הבקרה הפנימית. מודל – COSO הינו המודל אותו מיישמות רוב החברות הנדרשות לעמוד בדרישות רגולטוריות בהקשר לדיווח כספי וגילוי. ניהול סיכונים מוגדר ע״פ ה - COSO כתהליך מובנה המאפשר זיהוי והערכת סיכונים וזאת לצורך גיבוש ויישום דרכי התמודדות עימם על מנת להבטיח את השגת היעדים. ארגון ה- COSO – committee of sponsoring organizations (ארגון התנדבותי המוקדש לשיפור איכות הדיווח הפיננסי דרך אתיקה עסקית ובקרות פנימיות יעילות),זהו ארגון מוביל בתחום המתודולוגיות לניהול סיכונים, פרסם ב- 2004 הגדרה אוניברסאלית ל-ERM(Enterprise Risk Management) .

הארגון עיצב את דרך ניהול הסיכונים המומלצת לארגונים, מתודולוגית. מודל ה- COSO ERM הוא מאוד מוכר בקרב ארגונים. בעבר היה נהוג להתייחס לניהול סיכונים במובן ה״צר״ של המילה (סיכון שע״ח, סיכון אשראי, סיכוני סחורות וכו׳). בעבר חברות היו מתמקדות בסיכון ספציפי ולא מסתכלות על התמונה הכוללת של הארגון.

כיום גישת ניהול הסיכונים מקיפה יותר, לכן ה- ERM מנסה לכסות את כל תחומי הסיכון, מסתכלת על כלל הארגון לאורך זמן ובודקת גם את הסיכונים הטמונים באסטרטגיה שלו. תהליך ניהול סיכונים כולל יצירת תוכן (מיפוי, הגדרה וניתוח הסיכונים העסקיים) וכן יצירת תהליך (בנייה ותחזוקה של תהליך ניהול סיכונים דינאמי תוך התאמה לצרכים הייחודיים של החברה).

מודל ה-COSO הינו מודל ניהול הסיכונים המבוסס על התפיסה של ה- COSO intergraded framework . חשוב לציין שקיימים שני מודלים של COSO : מודל לבקרה פנימית ומודל לניהול סיכונים. המודל לבקרה פנימית מכיל חמישה מרכיבים עיקריים הכוללים את : סביבת הבקרה, הערכת סיכונים, פעולות בקרה, מידע ותקשורת ופעולות ניטור.

COSO ERM הולך צעד נוסף כדי לספק פוקוס נרחב על הסיכונים. כתוצאה מכך מודל הבקרה הפנימית מהווה חלק מהמסגרת של מודל ה-ERM. מטרה עיקרית של מסגרת ה ERM היא לעזור למנהלים להתמודד טוב יותר עם מגוון הסיכונים שמאיימים לפגוע ביעדי הארגון. אחת ממטרות המודל היא לעשות אינטגרציה של נושאים שונים בעלי משמעות דומה בניהול הסיכונים, המסגרת הזו תוכננה כדי לקבל כמה שיותר נקודות השקפה ולספק נק׳ התחלה להערכה ושיפור של ניהול הסיכונים התאגידי בארגון.

<u>אז מדוע אנו בכלל צריכים מודל?</u>

1)<u>אחידות וסטנדרטיות ביישום פעולות ומנגנונים בארגון</u> – מאפשרת עשיית השוואה בין ארגונים שונים. כפי שבחשבונאות נהוג ליישם תקני דיווח כספיים בינלאומיים (IFRS) , על מנת שתהיה אחידות בינלאומית ולהקל על ההשוואה בקריאת דוחות כספיים בין החברות השונות. כנ"ל לגבי ה COSO , שימוש במודל אחיד בעל סטנדרטים אחידים וברורים.

2)<u>בסיס להשוואה בין חברות/ענפים</u>- ברגע שיש לנו מודל ניתן להשוות סקטורים של חברות ברגע שכולם מיישמים את המודל ,יש בסיס להשוואה.

3) <u>גורם חיצוני שמתווה עקרונות ללא שיקולים זרים והטיה</u>- ניהול הסיכונים הוא נושא אמוציונאלי, לכל אחד יש אינטרסים ודברים שמעניינים אותו יותר וכאלה שפחות. בסופו של דבר מדובר בהחלטות שצריך לקבל ונוצרים חיכוכים, וויכוחים ואינטריגות במהלך התהליך. כשמודדים סיכונים עפ"י פלטפורמה מסודרת זה מונע חיכוכים, אי אפשר להתווכח, או שמקבלים את המודל או שלא.

4) <u>מתן TONE AT THE TOP של ההנהלה הבכירה לגבי רמות הסיכון אותן היא מוכנה לקיים בכל אחד מרבדי הארגון</u>- זוהי בעצם ההכוונה שהמנהלים נותנים להתנהלות הארגון – יכולה להיות שמרנית או מתירנית והסיכון שיילקח יהיה בהתאם להכוונה הזו .ניהול הסיכונים נותן לנו כלי לבוא ולהגדיר את רמות הסיכון שאנחנו רוצים שיהיה לארגון. כל הנהלה מגדירה את התיאבון לסיכון (Risk Appetite) שלה, התיאבון לסיכון מוגדר כביטוי של רצון/קיבולת של הארגון לסבול רמות חשיפה גבוהות/נמוכות לסיכון וחוסר ודאות בכדי להשיג את היעדים האסטרטגיים.

5) <u>פיתוח והתאמה של המודל ע"פ המגמות בסביבה העסקית</u>- ברגע שיש מודל ניתן לעשות התאמות שרוצים בהתאם לצרכים של הארגון.

ניהול סיכונים תומך ביצירת ערך בכך שהוא מאפשר:

1. התמודדות אפקטיבית עם אירועים עתידיים פוטנציאליים שיוצרים אי ודאות.

2. מתן תגובה אשר מצמצמת את הסבירות של תוצאות שליליות, ומגבירה את הסבירות לתוצאות חיוביות.

ה COSO פרסם בשנת 2004 את המתווה שלו לניהול סיכונים, זאת ללא קשר לגודל או מיקוד הארגון המסוים, מודל מקובל באופן גורף לדיון והערכת מאמצי ניהול הסיכונים. מטרת המודל:

א. לשפר את טיב הדיווח הכספי בארגון, על מנת להגדיל את האפשרות לאיתור מוקדם ו/או למנוע תרמיות בדיווחים הכספיים.

ב. לזהות פקטורים הגורמים להונאה בדיווחים פיננסיים, על מנת למנוע מקרים כאלה.

כמובן שהאחריות למניעה ו/או לגילוי מוקדם של תרמיות בדיווחים הכספיים מוטלת בראש ובראשונה על הנהלת החברה.

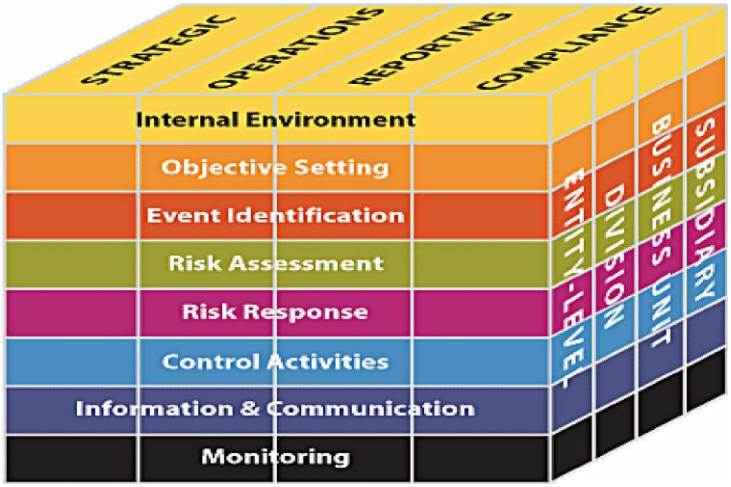
COSO הגדירו את הבקרה הפנימית כתהליך המוכוון ע״י הדירקטוריון, ההנהלה וגורמים אחרים בכדי לספק בטחון סביר להשגת :

1. אפקטיביות ויעילות תפעולית
2. מהימנות הדיווח הכספי – איך משתקף העסק בדוח הכספי, התרגום הכמותי לפעולות שהעסק מבצע. התקציב משקף את התכנון הארגוני שנה קדימה והדוחות הכספיים משקפים את העבר.
3. עמידה בדרישות החוק – איך הארגון ברמת ההתנהלות שלו מקיים ועומד בחוקים מבחינת התנהלות חיצונית (רשויות המס, רשות ני״ע) ופנימית (נהלים ארגוניים וכיו״ב).

מודל הCOSO ERM דומה בצורתו למודל לבקרה פנימית. המודל פורסם בשנת 2004 והוא מגדיר את הרכיבים החיוניים, השפה המשותפת לניהול סיכונים כולל ומעניק כיוון ברור והנחיות.
יעדי הארגון מחולקים ל-4 קטגוריות : אסטרטגי, תפעולי, דיווח וציות.
אסטרטגי- מתייחס למטרות ברמה הגבוהה, יישור קו עם החזון והייעוד של הארגון.
תפעולי- מתייחס לאפקטיביות וליעילות של תפעול הארגון כולל מדידת ביצועים ורווחיות.
דיווח- מתייחס לאפקטיביות הדיווח הכספי בארגון.
ציות- מתייחס לרמת הציות של הארגון לחוקים ותקנות.

ERM מתחשב בפעילויות בכל רמות הארגון, ועוזר להשיג את יעדי הארגון ב-4 קטגוריות הנ״ל.

בתמונה נוכל לראות את מודל הקובייה של COSO כאשר במעלה הקובייה נמצאות ארבעת הקטגוריות של יעדי הארגון (אסטרטגי, תפעולי, דיווח וציות) , ובקדמת הקובייה את שמונה השכבות אשר מודל הCOSO מגדיר כתהליך ניהול הסיכונים בארגון. (אשר יפורטו בהמשך המאמר).



בתמונה : מודל הCOSO ERM-.(מודל הקובייה).

המודל מיועד לסייע למנהלים בארגון לקיים ניהול סיכונים שיטתי וממוסד. יחד עם זאת, המודל יכול לשמש כמעין רשימת תיוג עבור מבקרים פנימיים אשר אליה יתייחס סקר הסיכונים שהם עורכים, זאת כדי לבסס את תכנית העבודה של הביקורת. מבקרים פנימיים צריכים להכיר את המודל ואת גישת הERM- ניהול של מכלול הסיכונים הקיימים בארגון וזאת על מנת להיות מסוגלים לקיים ביקורת על הליך ניהול הסיכונים בארגון, וכדי לסייע לארגון בתהליך ניהול הסיכונים.

מודל ה COSO מגדיר את תהליך ניהול הסיכונים בשמונה שכבות, ניהול סיכונים אפקטיבי דורש יישום של כלל המרכיבים בארגון:

1. **<u>סביבה פנימית</u>-** הסביבה הפנימית כוללת אלמנטים רבים, כולל קיום ערכים אתיים, יושר, סמכויות ואחריות, מחויבות ההנהלה והדירקטוריון וועדותיו לפעולות בקרה ופיקוח, פילוסופיות הניהול וסגנון ניהול, כשירות העובדים וההנהלה, מבנה ארגוני, ועדות ביקורת, האופן שההנהלה מאצילה סמכויות, מארגנת ומפתחת את אנשיה. זהו רכיב הבסיס לסביבת הבקרה והוא קובע את אופי הארגון ומשפיע על מודעות אנשיו לבקרה. כחלק מהסביבה הפנימית, ההנהלה מבססת ניהול סיכונים, את התיאבון לסיכון, ואת תרבות ניהול הסיכונים אשר יתמזגו עם ניהול הסיכונים בארגון.
2. **<u>הגדרת יעדים</u>-** ארגון חייב להגדיר לעצמו יעדים ומטרות לפעילותיו העסקיות. יעדים צריכים להיות מוגדרים לפני שההנהלה יכולה לזהות אירועים אשר עשויים להשפיע על יעדי הארגון. ניהול סיכונים מבטיח שההנהלה תהיה בתהליך של קביעת יעדים והחזון אשר יהיו תואמים לתיאבון הסיכון של הארגון.
3. **<u>זיהוי אירועים</u>-** זיהוי אירועים מתייחס להחלטות הנהלה של גורמים פנימיים וחיצוניים שיכולים לגרום לאיומים ולהזדמנויות בארגון. זה כולל אירועים שיכולים להיות בעלי השפעה חיובית או שלילית או שניהם. יש לבצע הבחנה בין סיכון להזדמנות כאשר סיכון יהיה אירוע בעל השפעה שלילית ואירוע שיש לו השפעה חיובית מייצג הזדמנות אשר ההנהלה מתעלת אותו לצורך השגת היעדים העסקיים.
4. **<u>הערכת סיכונים</u>-** הערכת סיכונים מאפשרת לארגון לשקול איך אירועים פוטנציאליים יכולים להשפיע על יעדים של הארגון. הערכת הסיכונים כוללת :זיהוי, ניתוח והגדרת הסיכון, המהווה מכשול העומד בדרך להשגת יעדי הארגון. על הארגון להיות מודע לסיכונים העומדים מולו ולקבוע דרכים להתמודדות איתם. ההנהלה צריכה להעריך את האירועים משתי פרספקטיבות: סבירות וחומרה. יש להעריך את הסיכון מהיבט סיכון שיורי והסיכון שורשי. הסיכון השיורי (Residual Risk) מוגדר כסיכון שנותר לאחר הטיפול בסיכון המקורי. סיכון שורשי (Inherent Risk) מוגדר כרמת הסיכון המובנה מעצם הפעילות שמקיים הארגון, בהתעלם מהבקרות הקיימות והמאפיינים הייחודיים לארגון או לתהליך.
5. **<u>תגובה לסיכון</u>-** הנהלה צריכה לזהות אופציות לתגובה לסיכון ולשקול את האפקט של האירוע מבחינת סבירות וחומרה (הקשר של הסובלנות לסיכון ועלות-תועלת), עליה לעצב וליישם אופציות כתגובה לסיכון. התגובות האפשריות לטיפול בסיכון הינן: קבלה, העברה/שיתוף, הקלה ומניעה.

א. <u>קבלה</u>-משמעות קבלה הינה קבלת הסיכון וההשלכות כתוצאה מהאירוע שעלול להתקיים, כלומר אי נקיטת צעדים לטיפול בסיכון ובהשלכותיו.

ב. <u>העברה/שיתוף</u>- נקיטת צעדים להעברת ההפסד ו/או ההתחייבות המלווה את אותו אירוע שלילי לגורם שלישי (חלוקת הסיכון ע"י גורם נוסף). כגון: ביטוח, מיקור חוץ וכיו"ב.

ג. <u>הקלה/הפחתה</u>- נקיטת צעדים לצמצום ההשלכה ו/או ההסתברות של הסיכון ע״י יישום ובקרה של בקרות בתהליכי הארגון, נקיטת פעולות להפחתת הסיכון. כגון: פיקוח תקציבי, פיתוח תכנית להמשכיות עסקית וכיו״ב.

ד. <u>מניעה</u>- נקיטת צעדים על מנת למנוע את התרחשות הסיכון הבלתי רצוי, כגון: הפסקת פעילות, איסור על ביצוע פעילויות וכיו״ב.

6. **<u>פעולות בקרה</u>-** פעולות בקרה הינם חלק מתהליך שארגון צריך לשאוף כדי להשיג את יעדיו האירגוניים. הכולל את המדיניות וההליכים שעוזרים להבטיח שהתגובה לסיכון מיושמת בצורה נאותה.

7. **<u>מידע ותקשורת</u>**- מידע צריך להיות בכל הרמות של הארגון כדי לזהות, להעריך ולהגיב לסיכונים. מידע מגיע ממגוון מקורות פנימיים וחיצוניים בצורה איכותית וכמותית ומאפשרת לניהול הסיכונים להגיב למצבים שונים בזמן אמת. המידע צריך להיות מהימן, נגיש ולהיערך בעיתוי המתאים לגורמים הרלוונטיים בתוך הארגון ומחוץ לארגון. תקשורת צריכה להעלות ערנות בנוגע לחשיבות ולרלבנטיות של ניהול סיכונים אפקטיבי.

8. **<u>ניטור</u>-** ניטור של ניהול סיכונים מעורב בהערכה של נוכחות ושל תפקוד של המרכיבים והאיכות של הביצועים לאורך זמן. ווידוא קיומן של הבקרות ובדיקה שהבקרות פועלות באופן יעיל ואפקטיבי. ניטור יכול לקחת מקום בהתרחשות פעילות או בהערכות נפרדות.

נקודות עיקריות ביישום של COSO ERM:

1. <u>הבנה והגדרה של פילוסופיית ניהול הסיכונים של הארגון</u>- ה- ERM לא יהיה אפקטיבי אם ינוהל בשלט רחוק ממטה החברה. תהליך ניהול הסיכונים חייב להיות מנוהל ע״י אנשים אשר קרובים מספיק לסיטואציות הסיכון בכדי להבין את הפקטורים השונים סביב הסיכון והמשמעויות כתוצאה מכך. כמו כן ההנהלה חייבת להיות מעורבת בתהליך ניהול הסיכונים, ללא מעורבות ומחויבות ההנהלה לתהליך, תהליך ניהול הסיכונים לא יוכל להצליח ולא יהיה אפקטיבי.

2. <u>ERM הינו תהליך מתמשך</u>- צריכה להיות סדרת צעדים מתועדת לסקירה והערכה של סיכונים פוטנציאליים אשר ממנה ייגזרו פעולות המבססות על טווח רחב של פקטורים חוצי ארגון.

3. <u>התיאבון לסיכון</u>- תפישת התיאבון לסיכון חייב להילקח בחשבון כחלק מהתהליך. התיאבון לסיכון הינו מידת הסיכון שהארגון מוכן לקחת על עצמו.

4. <u>ראייה רחבה של הארגון</u>- כל ארגון מתמודד באופן עקבי עם אלטרנטיבות שונות לאסטרטגיה לפעולות עתידיות פוטנציאליות. יישום ERM באופן אפקטיבי אמור לשחק קלף עיקרי ולסייע בבחירת האסטרטגיות. ישנם ארגונים רבים גדולים ומורכבים. תכנית ERM צריכה להיות חוצת ארגון ולשמש תשתית התמודדות עם סיכונים מכל סוג – נמוכים וגבוהים, ע״פ התיאבון לסיכון שההנהלה הגדירה. מידת הסיכון שארגון מוכן לשאת משתנה מארגון לארגון ותלויה בנסיבות הייחודיות לכל ארגון.

הכותב הינו בוגר B.A במנהל עסקים בהתמחות חשבונאות, סטודנט מצטיין לתואר שני MBA במנהל עסקים בהתמחות מימון, עובד כמתמחה בראיית חשבון. מוסמך ARM (Associate in Risk Management) מטעם האיגוד הישראלי למנהלי סיכונים, בוגר לימודי תעודה בניהול סיכונים מטעם לשכת רואי החשבון, בוגר קורס להכשרת מנהלי סיכונים (CRO) מטעם המכון ללימודי המשך ודן אנד ברדסטריט (D&B).