מודל COSO החדש (COSO 2013) לבקרה פנימית –
האם כבר יישמת? מדריך מקוצר

דרור בר-משה, רו"ח, LLM, CIA, CISA, CRISC, CRMA

אורי גלאור, רו"ח, MBA, CRM

הקדמה

בשנת 1992 פרסם ארגון ה- COSO (Committee of Sponsoring Organizations of the Treadway Commission) את מודל הבקרה הפנימית (Internal Control – Integrated Framework). המודל זכה לאימוץ ושימוש נרחב ברחבי העולם והוא מוכר כמודל המוביל לעיצוב ויישום של בקרה פנימית ולהערכת אפקטיביות הבקרה הפנימית.

בשנים שחלפו מאז, הסביבה העסקית והתפעולית השתנתה למדי, הן מבחינת מורכבותה והן מבחינה טכנולוגית וגלובלית (כגון: התרחבות לשווקים גלובליים, דרישות חוקיות ורגולטוריות, שימוש והישענות על טכנולוגיות מתפתחות, ועוד). בה בעת בעלי עניין מחפשים כיום שקיפות גדולה יותר ושלמות של מערכת הבקרה הפנימית התומכת בהחלטות עסקיות וממשל תאגידי.

ארגון ה- COSO פרסם במאי 2013 את המודל החדש שיאפשר לארגונים לפתח ולתחזק ביעילות מערכת בקרה פנימית, אשר תגדיל את הסבירות להשגת יעדי הארגון והתאמתו לשינויים בסביבה העסקית והתפעולית.

המודל החדש משמר את הגדרת הבקרה הפנימית ואת חמשת מרכיביה: סביבת הבקרה (Control Environment), הערכת סיכונים (Risk Assessment), פעולות בקרה (Control Activities), מידע ותקשורת (Information & Communication), ופעולות ניטור (Monitoring Activities), וכן משמר את חשיבות שיקול דעת ההנהלה בבואה לעצב וליישם בקרה פנימית ולהעריך את האפקטיביות שלה.

אחד השיפורים הבולטים של המודל החדש הינה הפורמליזציה של מושגי היסוד שהוצגו במודל הישן. במודל החדש הם מוגדרים כעקרונות אשר כפופים לחמשת מרכיבי הבקרה הפנימית. עקרונות אלה מבהירים את עיצוב ויישום המודל.

המודל כולל גם נקודות למיקוד המדגישות את המאפיינים החשובים הנוגעים לעקרונות שמתווה המודל.

כמו כן, המודל מרחיב את קטגוריית הדיווח הפיננסי וכולל עתה דיווח שאינו פיננסי וכן דיווחים פנימיים (נוסף על הדיווחים החיצוניים).

מאמר זה, מתאר את המודל החדש ומבוסס על פרסומי ה- COSO הרשמיים. המאמר מיועד לחברי דירקטוריון, מנכ"לים וחברי הנהלה אחרים, בבואם לדון, לעצב, ליישם ולהעריך את מערכת הבקרה הפנימית.

הגדרת הבקרה הפנימית על פי ה- COSO:

בקרה פנימית הינה תהליך, המושפע על ידי הדירקטוריון, ההנהלה ואחרים, המיועד לספק מידה סבירה של ביטחון באשר להשגת יעדי התפעול, הדיווח והציות של הארגון.

מודל ה- COSO החדש

<u>קטגוריות היעדים</u>

המודל מספק שלוש קטגוריות של יעדים, המאפשרים לארגונים להתמקד בהיבטים שונים של בקרה פנימית:

- יעדים תפעוליים – קטגוריה הנוגעת ליעילות התפעולית של הארגון, הכוללת יעדי ביצוע תפעוליים ופיננסיים.
- יעדי דיווח – קטגוריה הנוגעת לדיווחים פנימיים וחיצוניים וכן דיווחים פיננסיים ואחרים (שאינם פיננסיים), המקיפה, בין היתר, מהימנות, שקיפות או מושגים אחרים שנקבעו על ידי הרגולטורים או נהלי הארגון.
- יעדי ציות – קטגוריה הנוגעת להיצמדות לחוקים ורגולציה החלים על הארגון.

<u>חמשת מרכיבי בקרה פנימית</u>

בקרה פנימית כוללת חמישה מרכיבים משולבים:

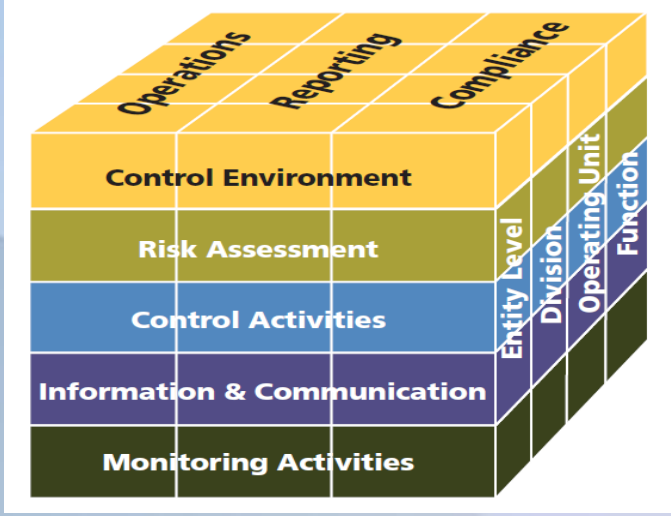
1. **סביבת בקרה (Control Environment)**- סביבת הבקרה היא קבוצה של סטנדרטים ותהליכים המספקים את הבסיס לביצוע בקרה פנימית בארגון. הדירקטוריון וההנהלה הבכירה צריכים לקבוע את ה"טון בצמרת" בנוגע לחשיבות הבקרה הפנימית, לרבות תקנים להתנהגות. סביבת הבקרה כוללת יושרה וערכים אתיים של הארגון; הפרמטרים שמאפשרים לדירקטוריון לפקח ולבצע את אחריותו; המבנה הארגוני והקצאת סמכות ואחריות; התהליך למשיכת, פיתוח ושימור של האנשים מוכשרים והקפדה על מדדי ביצוע, תמריצים ותגמולים כדי להוביל מחויבות לביצוע, וכו'.
2. **הערכת סיכונים (Risk Assessment)**- כל ארגון עומד בפני מגוון של סיכונים ממקורות חיצוניים ופנימיים. סיכון מוגדר כאפשרות שאירוע יתרחש ועלול להשפיע לרעה על העמידה ביעדי הארגון. הערכת הסיכונים כרוכה בתהליך דינמי וחוזר לזיהוי והערכת הסיכונים להשגת יעדים. הסיכון להשגת יעדים אלה קשור לקביעת הסובלנות לסיכון (Risk Tolerance). לפיכך הערכת הסיכונים מהווה את הבסיס לקביעה כיצד הסיכונים ינוהלו.
3. **פעולות בקרה (Control Activities)**- פעולות בקרה הן פעולות הנקבעות בנהלים המסייעים להבטיח שהנחיות ההנהלה יפחיתו סיכונים לאי השגת יעדי הארגון. פעולות בקרה מתבצעות בכל הרמות של הארגון, בשלבים שונים של תהליכים עסקיים ובסביבה הטכנולוגית. הן עשויות להיות מונעות או מגלות ועשויות לכלול בתוכן מגוון רחב של פעולות ידניות ואוטומטיות כגון: הרשאות, אישורים, התאמות וסקירת ביצועים. הפרדת תפקידים בדך כלל הינה חלק מהבחירה והפיתוח של פעולות בקרה. היכן שהפרדת התפקידים אינה מעשית, ההנהלה בוחרת ומפתחת פעולות בקרה חלופיות.
4. **מידע ותקשורת (Information and Communication)**- מידע נחוץ לארגון כדי לממש את אחריות הבקרה הפנימית לתמוך בהשגת יעדי הארגון. ההנהלה משיגה או מפיקה ומשתמשת במידע רלוונטי ואיכותי ממקורות פנימיים וחיצוניים כדי לתמוך בתפקוד מרכיבי הבקרה הפנימית האחרים. תקשורת הינה מתמשכת, זהו תהליך חוזר ונשנה של מתן, שיתוף וקבלת מידע נחוץ.
5. **פעולות ניטור (Monitoring Activities)**- קיום הערכות שוטפות ואחרות בכדי לוודא כי כל אחד ממרכיבי הבקרה הפנימית קיים ומתפקד. הערכות שוטפות, אשר מובנות כחלק מתהליכים עסקיים

ברמות שונות של הארגון, מספקות מידע בזמן. הערכות אחרות הנערכות מעת לעת, תשתנינה בתדירותן ובהיקפן בהתאם להערכת הסיכונים, יעילותן של הערכות שוטפות, ושיקולי הנהלה אחרים. ממצאים נבדקים מול קריטריונים שנקבעו על ידי רגולטורים, גופי תקינה אחרים או על ידי ההנהלה והדירקטוריון, וליקויים מועברים להנהלה ולדירקטוריון.

<u>הקשר בין יעדים ומרכיבים</u>

קיים קשר ישיר בין יעדים (שאותם הארגון שואף להשיג), למרכיבים (אשר מייצגים את מה שנדרש כדי להשיג את היעדים) ולמבנה הארגוני של הארגון. ניתן לתאר קשר זה בצורה של קובייה.

- שלוש הקטגוריות של היעדים: תפעולי (operations), דיווח (reporting) וציות (compliance)- מוצגים במעלה הקובייה.
- חמשת המרכיבים של הבקרה הפנימית מוצגים בקדמת הקובייה.
- המבנה הארגוני של הארגון מוצג במימד השלישי של הקובייה.



בתמונה: מודל COSO 2013.

<u>מרכיבים ועקרונות</u>

זהו למעשה החידוש המרכזי של המודל. המודל קובע 17 עקרונות המייצגים את מושגי היסוד הקשורים לכל אחד מהמרכיבים. בגלל שעקרונות אלה נמשכים ישירות מהמרכיבים, ארגון יכול להשיג בקרה פנימית אפקטיבית על ידי יישום של כל העקרונות. כל העקרונות מתייחסים ליעדים תפעוליים, דיווח וציות. להלן העקרונות התומכים במרכיבי הבקרה הפנימית:

- **סביבת בקרה (Control Environment)**

1. הארגון מפגין מחויבות ליושרה וערכים אתיים.
2. הדירקטוריון מפגין עצמאות מההנהלה ומפקח על פיתוח ויישום בקרה פנימית.
3. ההנהלה, תחת פיקוח הדירקטוריון, קובעת את המבנה, ערוצי הדיווח, הסמכות והאחריות להשגת יעדים.
4. הארגון מפגין מחויבות למשוך, לפתח ולשמר אנשים מוכשרים בהתאמה ליעדי הארגון.
5. הארגון משמר אחריות לבקרה פנימית בקרב עובדיו בהתאמה ליעדי הארגון.

- **הערכת סיכונים (Risk Assessment)**

6. הארגון מפרט את יעדיו בבהירות מספקת כדי לאפשר זיהוי והערכת סיכונים הקשורים ליעדים.
7. הארגון מזהה סיכונים להשגת יעדיו בכל רבדיו ומנתח את הסיכונים כבסיס לקביעה כיצד על הסיכונים להיות מנוהלים.
8. הארגון מתייחס לפוטנציאל להונאה בהערכת הסיכונים להשגת יעדים.
9. הארגון מזהה ומעריך שינויים העלולים להשפיע באופן משמעותי על מערכת הבקרה הפנימית.

- **פעילויות בקרה (Control Activities)**

10. הארגון בוחר ומפתח פעילויות בקרה המסייעות להוריד את הסיכונים להשגת יעדים עד לרמות מקובלות.
11. הארגון בוחר ומפתח פעילויות בקרה כלליות על מערכות המידע כדי לתמוך בהשגת יעדיו.
12. הארגון ממסד פעילויות בקרה במדיניות הקובעת את מצופה ובנהלים המפרשים את המדיניות לצעדים בפועל.

- **מידע ותקשורת (Information and Communication)**

13. הארגון משיג או מפיק ומשתמש במידע רלוונטי ואיכותי כדי לתמוך בתפקוד הבקרה הפנימית.
14. הארגון מתקשר פנימה מידע , לרבות יעדים ואחריות לבקרה הפנימית, הנחוץ בכדי לתמוך בתפקוד הבקרה הפנימית.
15. הארגון מתקשר עם גורמים חיצוניים בעניינים המשפיעים על תפקוד הבקרה הפנימית.

- **פעולות ניטור (Monitoring Activities)**

16. הארגון בוחר, מפתח ומבצע הערכות שוטפות ו/או אחרות של מרכיבי בקרה פנימית, בכדי לוודא כי מרכיבי הבקרה הפנימית קיימים ומתפקדים.
17. הארגון מעריך ומתקשר ליקויי בקרה פנימית בזמן לגורמים האחראים על תיקונם, כולל ההנהלה הבכירה והדירקטוריון, לפי העניין.

<u>בקרה פנימית אפקטיבית</u>

המודל קובע את הדרישות למערכת יעילה של בקרה פנימית. מערכת יעילה מספקת מידה סבירה של ביטחון לגבי השגת יעדי הארגון. מערכת אפקטיבית של בקרה פנימית מפחיתה לרמה רצויה, את הסיכון לאי השגת יעדי הארגון ועשויה להתייחס לאחת, שתיים או כל שלוש קטגוריות היעדים. זה דורש כי:

- כל אחד מחמשת המרכיבים והעקרונות הרלוונטיים קיים ומתפקד. "קיים" מתייחס לקביעה כי המרכיבים והעקרונות הרלוונטיים קיימים בעיצוב ויישום של מערכת הבקרה הפנימית להשגת יעדים. "מתפקד" מתייחס לקביעה כי המרכיבים והעקרונות הרלוונטיים ממשיכים להתקיים כחלק ממערכת הבקרה הפנימית על מנת להשיג יעדים.
- חמשת המרכיבים פועלים יחד בצורה משולבת. כלומר, כל חמשת המרכיבים מפחיתים לרמה נדרשת את הסיכון לאי השגת יעד. ישנה תלות הדדית ויחסי גומלין בין המרכיבים.

מגבלות המודל

המודל מכיר בכך שבעוד שבקרה פנימית מספקת מידה סבירה של ביטחון להשגת היעדים של הארגון, מגבלות קיימות. בקרה פנימית איננה יכולה למנוע שיקול דעת או החלטה מוטעים, או אירועים חיצוניים שיכולים לגרום לארגון לאי השגת יעדיו. במילים אחרות, אפילו מערכת יעילה של בקרה פנימית יכולה לחוות כשל.

מגבלות אלו מונעות מהדירקטוריון וההנהלה מקבלת ביטחון מוחלט להשגת יעדי הארגון - בקרה פנימית מספקת ביטחון סביר אך לא מוחלט. על אף המגבלות הללו, ההנהלה צריכה להפעיל שיקול דעת בעת בחירה, פיתוח ויישום של בקרות הממזערות ככל שניתן מגבלות אלו.

המסמכים הנלווים למודל

בנוסף למודל ארגון ה- COSO פיתח את המסמכים הבאים:

- Illustrative Tools for Assessing Effectiveness of a System of Internal Control (Illustrative Tools) – כולל תבניות (Templates) ותרחישים שעשויים להיות שימושיים ליישום המודל. תבניות אלה אינן חלק אינטגרלי מהמודל והם אינם מתיימרים לכלול את כל הנושאים הנדרשים להיבחן כאשר מעריכים את מערכת סביבת הבקרה. הנהלת הארגון יכולה להתאים את התבניות כדי לשקף סוגיות ייחודיות. התרחישים מציגים מספר דוגמאות פרקטיות לשימוש בתבניות לצורך הערכת האפקטיביות של מערכת הבקרה הפנימית בהתבסס על דרישות המודל.
- Internal Control over External Financial Reporting: A Compendium of Approaches and Examples (ICEFR Compendium) – כולל גישות ודוגמאות פרקטיות הממחישות את יישום מרכיבי ועקרונות המודל בכנת הדוחות הכספיים החיצוניים. הגישות מתארות בקצרה את הפעילויות והדוגמאות הינן ספציפיות ופרקטיות באשר לכל עקרון של המודל. המסמך אינו מתיימר לכלול את כל ההיבטים של המרכיבים והעקרונות הדרושים לבקרה פנימית אפקטיבית ולכן איננו מספק בבואנו לקבוע כי כל אחד מחמשת המרכיבים והעקרונות הרלוונטיים קיימים ומתפקדים.

יישום המודל

- ה- COSO מאמינים כי כל עקרון מוסיף ערך, מתאים לכל הארגונים ולכן רלוונטי. במקרים בהם ההנהלה קובעת כי עקרון מסוים איננו רלוונטי לארגון, יש צורך לתעד את הרציונל.
- העקרונות המפורטים במודל צפויים להבהיר כיצד ליישם את המודל בעיצוב ויישום של מערכת בקרה פנימית ובהערכת האפקטיביות שלה. בנוסף, הגישה מבוססת העקרונות מסייעת להבחין מה מכוסה ומה חסר.
- המודל מתאר גם נקודות למיקוד שהינם מאפיינים חשובים של העקרונות. נקודות למיקוד עשויים לעזור להנהלה בעיצוב ויישום בקרה פנימית והערכה האם העקרונות הרלוונטיים קיימים ומתפקדים.

  המודל מכיר באפשרות כי חלק מהנקודות למיקוד אינם מתאימות או אינן רלוונטיות לכל הארגונים וכי הארגון יכול להתייחס לנקודות מיקוד אחרות.
- אחד הדגשים החשובים של המודל החדש הוא בכך שיש לרדת מרמת יעדי הארגון לרמת הסיכונים ומשם לרמת הבקרות. הבקרות החשובות הן אלה אשר מנטרלות סיכונים הנוגעים ליעדים מרכזיים של הארגון.
- בעוד שהמודל שב ומדגיש כי הקמה ותחזוקה של סביבת הבקרה הינה באחריותה הבלעדית של ההנהלה, לביקורת הפנימית תפקיד מפתח בהערכת סביבת הבקרה. פירוט העקרונות במודל מגדיל את השימוש בו על ידי הביקורת הפנימית ומסייע בבואה להעריך את עיצוב ואפקטיביות הבקרה הפנימית.
- נשמרת האבחנה בין מערך בקרה על פי COSO ובין ניהול סיכונים כולל "ERM" והתובנה ששתי מסגרות עבודה אלו משלימות אחת את השנייה.
- SOX 404 דורש כי הנהלת ארגון ציבורי תאמץ מסגרת בקרה פנימית להערכה ולדיווח על עיצוב ותפעול אפקטיבי של הבקרה הפנימית. רוב החברות הציבוריות מאמצות את מודל ה- COSO.

- במעבר מהמודל הישן לחדש ובנוגע לדיווח על הבקרה הפנימית על הדיווח הפיננסי, על ההנהלה כאמור להעריך כיצד מערכת הבקרה הפנימית מיישמת את 17 העקרונות הקשורים לחמשת מרכיבי הבקרה הפנימית. ההנהלה צריכה לדון עם הדירקטוריון לגבי התוכנית לאימוץ המודל החדש ועל הדירקטוריון לפקח על ההנהלה בבואה ליישם את המודל החדש.
- שלבי עבודה ראשוניים:

  מומלץ להנהלת הכספים בארגונים אשר מאמצים את המודל החדש (במסגרת הדיווח הפיננסי החיצוני - SOX) לפעול כדלהלן:

  - קראו את המודל החדש וזהו רעיונות חדשים ושינויים.
  - בצעו סקירה ראשונית. קבעו כיצד המודל החדש משפיע על העיצוב וההערכה של הבקרה הפנימית. העריכו את רמת כיסוי עקרונות המודל על ידי התהליכים והבקרות הקיימים וקחו בחשבון את הנקודות למיקוד.
  - זהו את הצעדים שיש לבצע במעבר למודל החדש.
    - פתחו תוכנית מעבר למודל החדש.
    - שקלו לבצע walkthrough, טסטים של בקרות והערכה של ליקויי בקרה, כדי לזהות שינויים דרושים.
    - הקפידו על גילוי נאות של המודל בו נעשה שימוש בתקופת המעבר.
  - תקשרו והדריכו את הדירקטוריון, ההנהלה ועובדים רלוונטיים.
  - דונו לגבי התהליך עם הביקורת הפנימית והמבקר החיצוני.

תחולה

ארגון ה- COSO הכריז כי המודל הישן יהיה זמין בתקופת מעבר שתימשך עד 15 בדצמבר 2014, שלאחריה יוחלף המודל הישן. ב- COSO מאמינים כי שימוש במודל הישן הינו הולם בתקופת המעבר וכי על שימוש במודל הישן הקשור בדיווח חיצוני נדרש גילוי.

ביבליוגרפיה

- COSO Internal Control – Integrated Framework, Frequently Asked Questions, COSO, May 2013.
- Internal Control – Integrated Framework – Executive Summary, COSO, May 2014.
- The 2013 COSO Framework & SOX Compliance, One Approach to an Effective Transition, by J. Stephen McNally, CPA, June 2013.