ISOX: היבטי מערכות המידע

כך בוחנים ומעריכים את סביבת הבקרה במערכות המידע שבשימוש הארגון, לאור הדגש על תחום זה ב־ISOX > חנן טויזר, דורון כהן

אחד הנדבכים החשובים ב־ISOX הוא הערכה ובחינת של סביבת הבקרה במערכות המידע אשר בשימוש הארגון, שכן ליקויים בבקרה זו משפיעים באופן ישיר על איכות הדיווח הכספי. מקובל לומר, שחברה לא יכולה ליישם SOX בהצלחה כאשר קיימים ליקויים מהותיים במערכות המידע.

בקרות במערכות המידע נחלקות לבקרות אפליקטיביות ולבקרות כלליות. הראשונות הן בקרות ממוחשבות במערכות המידע התומכות בתהליך העסקי. בקרות אלו מוטמעות במערכות המידע ונותנות מענה לסיכונים בתהליכים העסקיים, לדוגמא: אבטחה מפני שינויים לא מורשים במאגר מידע (כגון מחירונים ותעריפים), מניעת קליטת חשבונית ספק כפולה והגדרת חוקיות לקליטת פקודות יומן תקינה.

מאחר שהבקרות האפקטיביות מהוות חלק בלתי נפרד מהתהליך העסקי, הרי שהגדרתן, עדכונן ובדיקתן נעשים כחלק בלתי נפרד מיישום ה־SOX בתהליכי הדיווח הכספי העיקריים של הארגון ולא כפרויקט נפרד.

בקרות כלליות בסביבת מערכות המידע (ITGC) הן בקרות מיחשוב כלליות, שנועדות לתמוך בניהול פעילויות ובבקרות עליהן, כגון: תהליך גיבויים ומדיניות אבטחת מידע. ארגונים רבים בעולם נוהגים לבסס את יישום ה־ITGC על מסגרת ה־COBIT – מודל מקיף הכולל מגוון רחב של תהליכים ויעדי בקרה בסביבה טכנולוגית ואינו תלוי בפלטפורמה מסוימת.

ה־COBIT מספק מבנה שבעזרתו ניתן לארגן את פעילות מערכות המידע ולמנף את התהליכים והמשאבים, כך שהתוכניות האסטרטגיות של מערכות המידע יתורגמו באופן מעשי בכל רובדי הארגון ויביאו לתוצאה העסקית המצופה.

נהוג לחלק את בקרות ה־ITGC לחמישה תחומים עיקריים: סביבת הבקרות, פיתוח מערכות,שינויים במערכות, תפעול המחשוב ואבטחת מידע. לכל תחום יש בקרות רלוונטיות, אותן יש להתאים בהתאם לשוני בין אופי עבודת הארגונים והמשאבים העומדים לרשות הארגון.

שלבי יישום ITGC

הגדרת מערכות קריטיות: לא כל מערכות המידע ייכנסו לתחולת ה־ISOX. מערכות המידע בארגון כוללות דואר אלקטרוני, מערכות נוכחות, מערכות לניהול משאבי אנוש ומערכות תפעוליות שונות (כגון: הנדסה, שירות לקוחות ויישומי משרד). יישום ITGC מופנה בעיקרו למערכות הקריטיות המשפיעות על הדיווח כספי, והתשתיות עליהן מושתות המערכות.

לצורך עמידה בהוראת התקנה אין צורך להכיל את בקרות ה־ITGC על כלל המערכות, אלא יש להגדיר את המערכות הקריטיות בהתאם להשפעה על הדיווח הכספי. במרבית הארגונים המערכות הקריטיות יהיו מערכת הכספים, המערכת הלוגיסטית, והתשתיות אשר עליהן הן מושתות.

הערכת סיכונים: הגדרת החשיפות הטמונות בכל המערכות הקריטיות. על מנת לספק כיסוי מלא של כלל הבקרות הרלוונטיות לחברה, יש לבחון לגבי כל אחת מהן את החשיפה לסיכונים לכל אחד מחמשת תחומי ה־ITGC. הנגזרת של הערכת הסיכונים תהיה הצבת המערכות הקריטיות אל מול הסיכונים הגלומים לחברה בשימוש בהן.

מיפוי בקרות: הגדרת הבקרות אשר מצמצמות את הסיכונים שזוהו. טבלת בקרות היא מכלול הבקרות הכלליות על מערכות המידע אשר נועדו להפחית את הסיכון הפוטנציאלי שעלה בהערכת הסיכונים. בהמשך יוגדרו בקרות המפתח, שהן בקרות ברמת סיכון גבוהה, והללו ייבחנו בהמשך, בשלב בחינת אפקטיביות.

במסגרת ניתוח הבקרות מול הסיכונים הפוטנציאליים, נבחנות גם הפעולות הנוספות שעל הארגון לבצע על מנת לצמצם חשיפות קיימות. על ההנהלה להצהיר, כי הבקרות אשר מפורטות בטבלת הבקרות מיושמות בדיוק מירבי.

בחינת אפקטיביות הבקרות אשר מצמצמות את הסיכונים שזוהו. בדיקה זו יש לבצע בהתאם למתודולוגיה מסודרת, ומטרתה לוודא שהבקרה שהוגדרה אכן עובדת ואפקטיבית. יש לבצע את הבדיקות באופן מתועד שיאפשר את בדיקות רואה החשבון בהמשך. לאחר מכן יש לרכז את הליקויים אשר עלו ולבחון את הצורך בבדיקות חוזרות.

ליקויים בניתוח פערי בקרה: בחינת משמעות הליקויים וסיווג רמת הליקוי. יש לסווג כל אחד מהליקויים בהתאם להשפעה אשר יכולה להיות לו על הדיווח הכספי, על פי שלוש רמות: ליקוי, ליקוי משמעותי, חולשה מהותית. על שני האחרונים יש לדווח לוועדת הביקורת ובעלי המניות, בהתאמה. על ההנהלה להתייחס לדרך בה היא מתמודדת עם תיקון הליקויים.

התפתחות מערכות המידע וההסתמכות עליהן בדיווח הכספי ובתהליכי קבלת ההחלטות מחייבים בקרה יעילה וצמודה, במיוחד לנוכח הדגש על כך ב־SOX ובמקבילו הישראלי. פרויקט ITGC איכותי יציף את נקודות החולשה במערך הבקרה, יציע אפשרויות לשיפורן ויוודא בעתיד שיושמו כל הלקחים שהופקו מהתהליך. ●

רו"ח דורון כהן וחנן טויזר,
מאהן־קנה ניהול בקרה