

ליווי פרויקטים על ידי הביקורת הפנימית הנחיות IIA ו- ISACA

כנס איגוד המבקרים הפנימיים - IIA
5.1.2017

יעל רוזן, רו"ח, מבקרת פנימית ראשית - קבוצת הבנק
הבינלאומי, סגנית נשיא IIA ישראל.

- הגדרת מקצוע הביקורת הפנימית על פי ה- IIA:
ביקורת פנימית היא פעילות בלתי תלויה ואובייקטיבית של **הבטחה וייעוץ** אשר מיועדת להוסיף ערך ולשפר את פעילות הארגון. היא מסייעת לארגון להשיג את מטרותיו בהבאת גישה שיטתית וממוסדת, לשם הערכה ושיפור האפקטיביות של תהליכי ניהול הסיכונים, בקרה, פיקוח וממשל תאגידי.
- שירותי הבטחה (Assurance): הינם בחינה אובייקטיבית של ממצאים ע"י הביקורת הפנימית, כדי לספק הערכה בלתי תלויה, או דעה או מסקנה לגבי הישות, הפעילות, התפקיד, התהליך, המערכת או כל עניין קשור אחר. אופייה והיקפה של מטלת הביקורת נקבעים ע"י המבקר הפנימי.
- שירותי ייעוץ (Consulting): הם מטבעם פעולות מייעצות, והן בדרך כלל מבוצעות לבקשה ספציפית מצד לקוח מטלת הייעוץ. אופי והיקף מטלת הייעוץ כפופים להסכם עם לקוח המטלה.
- שירותי הייעוץ כוללים בדרך כלל שני גורמים: המבקר הפנימי ולקוח מטלת הייעוץ. ראוי שהמבקר הפנימי ישמור על אובייקטיביות כאשר הוא מבצע מטלת יעוץ ואל לו לקבל אחריות ניהולית.

תחולת התקנים המקצועיים על שירותי הבטחה ושירותי ייעוץ

- **תקני תכונות (Attribute standards)** – עוסקים בתכונות הנדרשות מיחידים ומארגונים המבצעים ביקורת פנימית.
- **תקני ביצוע (Performance standards)** – מתארים את אופי הביקורת הפנימית ומספקים קריטריון איכות, שבהשוואה אליו ניתן למדוד את ביצועי השירותים המסופקים.

תקני תכונות ותקני ביצוע תקפים לכל שירותי הביקורת הפנימית.
[יחד עם זאת, קיימים בחלק מהתקנים הבדלים אשר מובהרים באמצעות ביאורים נפרדים לגבי שירותי הבטחה ולגבי שירותי ייעוץ]

➤ **סוגיה לדיון: האם פעילות ליווי פרויקטים ע"י הביקורת הפנימית נמצאת בקטגוריה של שירותי הבטחה או שירותי ייעוץ?**

- **תקני יישום (Implementation standards)** – מרחיבים את תקני התכונות ותקני הביצוע על ידי פירוט הדרישות לשירותי ההבטחה או שירותי ייעוץ.

➤ תקן 1000 – מטרה, סמכות ואחריות:

התקן: המטרה הסמכות והאחריות של הביקורת הפנימית חייבות להיות מוגדרות בבאופן רשמי בכתב האמנה (צ'רטר)...
הביאור ביחס לשירותי הייעוץ: אופי שירותי הייעוץ חייב להיות מוגדר בכתב האמנה של הביקורת הפנימית.

➤ תקן 1130 – פגיעה באי התלות או באובייקטיביות:

התקן: פגיעה למעשה או לכאורה באי תלות או באובייקטיביות, חייבת להיות מדווחת לגורמים המתאימים. אופי הגילוי תלוי באופי הפגיעה.
הביאור ביחס לשירותי הייעוץ:

- מבקרים פנימיים רשאים לתת שירותי ייעוץ, הנוגעים לפעולות להן היו אחראים בעבר.
 - אם קיימת אפשרות לפגיעה באי תלות או באובייקטיביות של מבקרים פנימיים, הקשורות לשירותי יעוץ מוצעים, חובה לתת לכך גילוי ללקוח לפני קבלת מטלת הייעוץ.
- [לעומת זאת נקבע ביחס לשירותי הבטחה כי מבקרים פנימיים חייבים להימנע מלתת שירותים לגבי תחום מסוים שבעבר היה תחת אחריותם. האובייקטיביות יכולה להיחשב כנפגמת אם מבקר פנימי נותן שירותי הבטחה לגבי תחום שהיה באחריותו בשנה שחלפה]**

דגשים בתקני התכונות בנוגע לשירותי יעוץ (המשך 1)

▪ תקן 1210 – מקצועיות:

התקן: מטלות הביקורת הפנימית חייבות להתבצע במקצועיות ובזהירות מקצועית ראויה. הביאור ביחס לשירותי הייעוץ: המבקר הפנימי הראשי חייב לסרב לקבל מטלות ייעוץ או להשיג ייעוץ או סיוע מתאימים, אם סגל הביקורת הפנימית חסר ידע, מיומנות ויכולות אחרות, הדרושים לביצוע מטלת ייעוץ, כולה או חלקה.

➤ תקן 1220 זהירות מקצועית ראויה:

התקן: מבקרים פנימיים חייבים ליישם זהירות ומיומנות המצופים ממבקר פנימי מוכשר וזהיר במידה סבירה. זהירות מקצועית ראויה, אין משמעה היעדר היכולת לטעות.

הביאור ביחס לשירותי הייעוץ:

מבקרים פנימיים חייבים לנהוג בזהירות מקצועית ראויה במטלת ייעוץ על ידי הפעלת שיקול דעת בנושאים הבאים:

- צרכים וציפיות של לקוחות, כולל אופי, עיתוי ודיווח תוצאות מטלת הייעוץ;
- מורכבות יחסית והיקף העבודה הדרוש להשגת יעדי מטלת הייעוץ;
- עלות מטלת הייעוץ יחסית לתועלת הפוטנציאלית ממנה.

[נושאים נוספים שנדרש לשקול ביחס לשירותי הבטחה: היקף העבודה הדרושה להשגת יעדי מטלת הביקורת, נאותות ואפקטיביות של תהליכי ממשל תאגידי, ניהול סיכונים ותהליכי הבקרה, הסתברות לטעויות משמעותיות, לאי סדרים ולאי ציות]

➤ תקן 2010 – תכנון:

התקן: המבקר הפנימי הרשאי חייב להכין תכנית עבודה מבוססת סיכונים, בהתאם למטרות הארגון, על מנת להחליט על סדרי העדיפויות של הביקורת הפנימית. הביאור ביחס לשירותי הייעוץ: ראוי שהמבקר הפנימי ישקול לבצע מטלות ייעוץ המבוססות על פוטנציאל לשיפור ניהול הסיכונים, להוספת ערך לארגון ולשיפור פעולתו. מטלות הייעוץ שהתקבלו חייבות להיכלל בתכנית העבודה.

➤ תקן 2120 – ניהול סיכונים:

התקן: ביקורת הפנימית חייבת להעריך את האפקטיביות ולתרום לשיפור תהליכי ניהול הסיכונים.

הביאור ביחס לשירותי יעוץ:

- במהלך ביצוע מטלת ייעוץ, מבקרים פנימיים חייבים להתייחס לסיכונים הקשורים למטרות מטלת הייעוץ, ולהיות ערניים לקיומם של סיכונים משמעותיים נוספים.
- בהערכתם את תהליכי ניהול הסיכונים של הארגון, מבקרים פנימיים חייבים לשלב ידע אודות סיכונים שהושג במהלך מטלות ייעוץ.

[ניתן דגש לסינרגיה בין שירותי הבטחה ושירותי ייעוץ]

- בעת סיוע להנהלה במיסוד או שיפור תהליכי ניהול סיכונים, מבקרים פנימיים חייבים להימנע מלקחת על עצמם אחריות ניהולית ע"י ניהול סיכונים בפועל

[ניתן דגש לשמירה על אי תלות ע"י הימנעות מתפקידים נוספים]

דגשים בתקני הביצוע בנוגע לשירותי יעוץ (המשך 1)

➤ תקן 2130 – בקרה

התקן: הביקורת הפנימית חייבת לסייע לארגון בשיפור בקרות אפקטיביות על ידי הערכת האפקטיביות והיעילות של הבקרות ועל ידי קידום שיפורן המתמיד.
הביאור ביחס לשירותי יעוץ: בהערכתם את תהליכי הבקרה של הארגון, מבקרים פנימיים חייבים לשלב ידע אודות בקרות, שהושג במהלך מטלות יעוץ.

[ניתן דגש לסינרגיה בין שירותי הבטחה ושירותי יעוץ]

➤ תקן 2201 – שיקולי תכנון

התקן: בתכנון מטלת הביקורת חובה על מבקרים פנימיים לשקול את מטרות הפעילות הנסקרת, הסיכונים המשמעותיים לפעילות...נאותות ואפקטיביות הממשל התאגידי, תהליכי ניהול הסיכונים והבקרות וההזדמנויות לבצע בהם שיפורים משמעותיים.
הביאור ביחס לשירותי יעוץ: מבקרים פנימיים חייבים להגיע להבנה עם לקוחות מטלת יעוץ לגבי מטרותיה, היקפה, תחומי אחריות, ושאר ציפיות הלקוח. במטלות משמעותיות, חובה לתעד הבנה זו.

[ההתייחסות להגעה להבנה עם הלקוחות, כאמור לעיל הינו ייחודי לשירותי יעוץ]

דגשים בתקני הביצוע בנוגע לשירותי יעוץ (המשך 2)

➤ תקן 2210 – מטרות מטלת ביקורת

התקן: לכל מטלת ביקורת חייבות להיקבע מטרות. הביאור ביחס לשירותי ייעוץ:

- מטרת מטלת הייעוץ חייבות להתייחס לתהליכי הממשל התאגידי, ניהול הסיכונים, והבקרה במידה המוסכמת עם הלקוח.
- מטרת מטלת הייעוץ חייבות להיות עקביות עם האסטרטגיות, המטרות וערכי הארגון.

➤ תקן 2220 – היקף מטלת ביקורת

התקן: ההיקף שנקבע חייב להיות מספק כדי להשיג את מטרות מטלת הביקורת. הביאור ביחס לשירותי ייעוץ:

- במהלך ביצוע מטלת ייעוץ, מבקרים פנימיים חייבים להבטיח, כי היקף מטלת הייעוץ מספק כדי לעמוד במטרות עליהן הוסכם. אם מבקרים פנימיים מפתחים הסתייגות בנוגע להיקף המטלה במהלכה, חובה עליהם לדון עם הלקוח אודות הסתייגויות אלה, על מנת לקבוע אם להמשיך בביצוע מטלת הייעוץ.
- במהלך מטלות ייעוץ, מבקרים פנימיים חייבים להתייחס לבקורות באופן עקבי למטרות המטלה, ולהיות ערניים לסוגיות בקרתיות משמעותיות.

דגשים בתקני הביצוע בנוגע לשירותי יעוץ (המשך 3)

➤ תקן 2240 – תכנית ביקורת למטלת ביקורת:

התקן: מבקרים פנימיים חייבים להכין תכניות ביקורת מתועדות להשגת מטרות מטלת הביקורת.

הביאור ביחס לשירותי ייעוץ: תכניות למטלות ייעוץ עשויות להשתנות בצורה ובתוכן בהתאם לאופי מטלת הייעוץ. **[דגש לגמישות בתכנון מטלת ייעוץ]**

➤ תקן 2330 – תיעוד המידע

התקן: מבקרים פנימיים חייבים לתעד מידע רלבנטי כדי לתמוך במסקנות ובתוצאות מטלת הביקורת.

הביאור ביחס לשירותי ייעוץ: המבקר הפנימי הראשי חייב לפתח מדיניות משמורת לרשומות של מטלות הייעוץ, לרבות אופן שחרור המידע לגורמים פנימיים וחיצוניים. המדיניות חייבת להיות עקבית עם הנחיות הארגון, הנחיות רגולטוריות רלבנטיות או דרישות אחרות.

➤ תקן 2410 תבחינים (קריטריונים) לדיווח

התקן: הדיווח חייב לכלול את מטרות מטלת הביקורת והיקפה כמו גם המסקנות המתאימות, ההמלצות ותוכניות ליישומן.

הביאור ביחס לשירותי ייעוץ: דיווח על התקדמות ותוצאות מטלות ייעוץ ישתנה בתוכנו ובצורתו, בהתאם לאופי המטלה וצרכי הלקוח.

[דגש לגמישות בעיצוב התוצר של מטלת הייעוץ. התוצר של מטלת ביקורת מובנה יותר וחייב לכלול חוות דעת ו/או מסקנות]

דגשים בתקני הביצוע בנוגע לשירותי יעוץ (המשך 4)

➤ תקן 2440 – הפצת התוצאות

התקן: המבקר הפנימי הראשי חייב להפיץ את התוצאות לגורמים המתאימים.

➤ הביאור ביחס לשירותי ייעוץ

- המבקר הפנימי הראשי אחראי לדיווח התוצאות הסופיות של מטלות הייעוץ ללקוחות.
- במהלך מטלות ייעוץ, יתכן שיזוהו סוגיות בממשל התאגידי, בניהול הסיכונים ובבקורות. כאשר הסוגיות המתגלות הינן משמעותיות לארגון, חובה לדיווח עליהן להנהלה הבכירה ולדירקטוריון.

▪ תקן 2500 – ניטור ההתקדמות

התקן: המבקר הפנימי הראשי חייב להקים ולתחזק מערכת למעקב אחר התקדמות היישום של התוצאות שדווחו להנהלה.

הביאור ביחס לשירותי ייעוץ: הביקורת הפנימית חייבת לבצע מעקב אחר התקדמות היישום של תוצאות מטלות הייעוץ במידה המוסכמת עם הלקוח.

[דגש לגמישות ביחס לביצוע מעקב "במידה המוסכמת עם הלקוח"]

GTAG 12: Auditing IT Projects

- **Global Technology Audit Guide – GTAG** : סדרת מסמכים של ה- IIA הכוללים קוים מנחים למבקרים פנימיים בנושאים שונים של ביקורת בתחום טכנולוגיות המידע.
- **GTAG 12** הינו קוים מנחים לביקורת של פרויקטים לפיתוח מערכות מידע (משנת 2009).
- **תפקיד הביקורת על פי הקוים המנחים:**
- מעורבותה בשלבים השונים של מחזור החיים של פרויקט IT יכולה להיות בדרך של מתן **שירותי הבטחה** וביצוע ביקורת פורמאליות **או** מתן **שירותי ייעוץ**. אופי המעורבות **תלוי בצ'רט** של הביקורת הפנימית בארגון.
- [הערה: בקבוצת הבינלאומי הליווי של פרויקטים מהותיים כגון הסבת מערכות אוצ"ח ומסד למערכות הבינלאומי, וכגון העתקת מרכז המחשבים מת"א לשורק בוצעו כשירותי הבטחה והופצו מספר דוחות ביקורת במהלך הליווי. כמו כן, מבוצעת פעילות ליווי פרויקטים כשירותי יעוץ]**
- מעורבות הביקורת במהלך פיתוח פרויקט IT יוצרת חשיפה לפגיעה באי תלות המבקר. יש לגדר חשיפה זו ע"י שמוודאים שהמעורבות תתבטא במתן יעוץ בלבד **ללא לקיחת אחריות על קבלת החלטות בפרויקט**. כמו כן, יש לוודא שהעניין של המבקר בפתרון (במידה וקיים כזה) לא יפגע באובייקטיביות שלו.
- המעורבות היא יעילה ואפקטיבית יותר לארגון ככל שמעורבות הביקורת מתחילה **בשלבים המוקדמים** של הפרויקט, עקב עלות תיקון/שינוי נמוכה יותר בשלבים אלה.

➤ **חמשת תחומי המיקוד בביקורת פרויקטים:**

- הלימה בין התחום העסקי והטכנולוגי, התאמה לאסטרטגיה של הארגון
- ניהול הפרויקט – מתודולוגיה ויישום לאורך השלבים במחזור החיים של הפרויקט
- מוכנות הפתרון
- ניהול שינויים בפרויקט
- הפקת לקחים לאחר היישום

➤ **סוגי הביקורות/הסקירות של פרויקטי IT :**

הביקורת הפנימית יכולה לבצע סוגים שונים של סקירות/ביקורות בהתאם לסיכונים בפרויקט ולצרכי הארגון. **צוות משולב של מבקרים עסקיים ומבקרים טכנולוגיים** מבטיח שניתן יהיה לתת כיסוי הן לסיכונים הפונקציונליים והן לסיכונים הטכנולוגיים.

➤ **הסוגים הנפוצים של הביקורות/הסקירות הינם:**

- הערכת הסיכונים בפרויקט
- הערכת מוכנות בשלבי מפתח או טרם העליה ליצור
- סקר הפקת לקחים
- בחינת ההתנהלות בשלבים שונים של מחזור החיים של הפרויקט תוך כדי ביצועו
- הערכה כוללת של המתודולוגיה לפיתוח פרויקטים.

ISACA G17: Effect of Non-Audit Role on the IS Auditor's Independence (1/2)

- **ISACA** – האיגוד הבינלאומי לביקורת ואבטחת מערכות מידע, קבע סטנדרטים (מסמכי Sxx) וקווים מנחים (מסמכי Gxx) המתייחסים לביקורת מערכות מידע.
- **G17** – הינו מסמך קוים מנחים בנוגע להשפעה של ביצוע תפקידים שאינם תפקידי ביקורת על מבקרי מערכות מידע (ממאי 2010).

להלן עיקרי ההוראות שנקבעו במסמך זה והמתייחסות למעורבות של ביקורת מערכות מידע בפעילויות שאינן פעילויות ביקורת:

- המעורבות בפעילויות שאינן ביקורת צ"ל **מעוגנת בצ'רט** של הביקורת הפנימית.
- המעורבות **אינה פוגעת באי תלות ואובייקטיביות** הביקורת כאשר הביקורת אינה לוקחת על עצמה קבלת החלטות או ביצוע תפקידים אחרים של ההנהלה (לרבות אישור מסמכי מדיניות ונהלים).
- המעורבות **אינה פוגעת באי תלות ואובייקטיביות** הביקורת כאשר הביקורת אינה מעורבת באופן מהותי בעיצוב, בפיתוח, בבדיקות, בהתקנה, בקונפיגורציה, בתפעול או בעיצוב בקרות במערכות שהינן משמעותיות ביחס לנושא שבו מבצעים ביקורת.
- בביצוע הפעילויות שאינן פעילויות ביקורת אין דרישה לאי תלות הביקורת, אולם קיימת דרישה לאובייקטיביות ומקצועיות.

ISACA G17: Effect of Non-Audit Role on the IS Auditor's Independence (2/2)

- ההנהלה וצוות הביקורת צריכים להיות בלתי תלויים ולהיתפס כבלתי תלויים בעת ביצוע ביקורת.
- בעת תכנון פעילות שאינה פעילות ביקורת, יש להביא בחשבון את ההשפעה האפשרית שתהיה לפעילות זו, על אי התלות של הביקורת בעת ביצוע ביקורת בעתיד/במקביל על אותו נושא/פונקציה.
- צעדים שניתן לנקוט כדי למנוע/להמעיט פגיעה באי התלות: פיקוח ניהולי צמוד על ביצוע הביקורת, ציוות מבקרים שונים מהמבקרים שביצעו את הפעילות שאינה ביקורת.
- במידה ואי התלות בביצוע הביקורת עשויה להיפגע או עשויה להיראות כנפגעת, עקב ביצוע פעילות שאינה ביקורת, יש לתת גילוי בדוח הביקורת בנוגע לפעילות זו על מנת לאפשר לקוראי הדוח להעריך את מידת השפעתה על הביקורת, ובנוגע לצעדים שננקטו כדי להמעיט את ההשפעה.
- (מידע שיש לשקול לכלול בגילוי בנוגע לפעילות שאינה ביקורת: האופי, העיתוי וההיקף של הפעילות, הגורמים המבצעים, הגורמים לביצועה, הצעדים שננקטו ע"מ לוודא שאין פגיעה משמעותית באי התלות בעת ביצוע ביקורת).