עיונים בביקורת פנימית

התפתחות מתמדת

חמש מגמות | נקודת מבט רחבה של הצמרת המקצועית הגלובלית על השסוגיות המרכזיות שיעצבו את המקצוע

מהפיכת המידע האנליטי בביקורת הפנימית בארגון

כיצד לבקר בענן

דצמבר
2016

בגיליון הקודם (מס' 3) של כתב העת פורסם מאמר פרי עטו של עו"ד קוחלני בנושא "מדור ביקורת במגזר השלטוני", עקב טעות דפוס נשמט שמו של כותב המאמר.

IIA ישראל - איגוד מבקרים פנימיים בישראל בע"מ

כתובת למשלוח דואר **ת.ד. 29281 תל אביב 61292**

טל **03-5116617** | פקס **03-5116647** | לתגובות והערות **theiiaisrael@gmail.com**

תוכן עניינים

דבר הנשיא

דורון כהן, רו"ח
נשיא IIA ישראל - איגוד המבקרים הפנימיים

בהסתכלות רחבה על עולם הביקורת הפנימית אפשר לזהות מגמות שעמן מבקרים פנימיים יצטרכו להתמודד ב-5 עד 10 השנים הקרובות, ובהן סביבת סיכונים תנודתית, רגולציה גוברת, ציפיות גבוהות של מחזיקי העניין, סיכוני טכנולוגיה מורכבים ועוד.

משמעות מגמה זו היא שתמהיל עבודת הביקורת הפנימית יצטרך להשתנות. הדגש על בחינת תהליכי הממשל התאגידי וניהול הסיכונים בארגון יבוא על חשבון בדיקות הבקרות והציות המסורתיות. המבקרים יידרשו להתמקד יותר בהערכת ניהול הסיכונים האסטרטגיים, נושא שרבים נמנעים ממנו בשל מורכבותו והכורח ללמוד אותו ולפתח מיומנות מתאימה.

גם הדרישות מתפקיד המבקר פנימי חוות שינוי משמעותי. מבקר פנימי בעידן הנוכחי חייב להיות בעל כישורים מגוונים, כגון יכולת אנליטית, חשיבה עצמאית, ידע במערכות מידע ויכולת גבוהה בניתוח נתונים.

גיליון זה מכיל מאמרים מרתקים וחדשניים מהארץ ומהעולם. אנו מקווים שהוא יסייע לכם להתעמק בהבנת התמורות העוברות על המקצוע על מנת להיערך אליהן באופן מיטבי. אתגרי המקצוע, כפי שתוארו לעיל, מחייבים כוח אדם איכותי ומקצועי ברמה הגבוהה ביותר.

מאז חוקק חוק הביקורת הפנימית בשנת 1992 היו מספר יוזמות לשנותו, יוזמות שנמשכות גם בימים אלה.

האיגוד פועל מול גורמים בממשל וברשות המחוקקת על מנת להשפיע שהתיקון שיחוקק יסייע לחיזוק מקצוע הביקורת הפנימית, לחיזוק מעמדם של המבקרים הפנימיים ולשיפור רמתם המקצועית.

דבר העורכת

שרון ויטקובסקי טביב, רו"ח
CIA, CRMA

החודשים האחרונים של השנה הם התקופה שבה כל מבקר פנימי מכין את התכנית לשנה הבאה. בכך נכללים לא רק נושאי הביקורת, אלא גם משאבי הביקורת, הטכניקות והכלים שבהם יעשה שימוש.

בהקשר הזה עולות לא מעט שאלות: מתי לאחרונה עצרנו ובחנו את פעילותנו ברמה האסטרטגית? האם הגדרנו יעדים למדידת ההצלחה שלנו כמבקרים? האם ניתחנו את החוזקות והחולשות שלנו?

בעוד שתכנית שנתית מבוססת סיכונים מנחה את הביקורת הפנימית לאורך השנה, הרי שתכנית אסטרטגית מתווה את הדרך מעבר לעתיד הנראה לעין.

בגיליון זה של כתב העת "עיונים בביקורת פנימית", הרביעי במספר, בחרנו להתמקד בנושא התפתחות מתמדת של מקצוע הביקורת הפנימית.

חלק רחב מהשיח הנוכחי בנושא הביקורת הפנימית עוסק במגמות העתידיות של המקצוע - היכן נהיה בעתיד ואיך נערכים לכך. לא מעט שאלות העוסקות ברבדים שונים מטרידות את קברניטי המקצוע (וגם אותנו): איך הביקורת הפנימית מתאימה את עצמה לציפיות של בעלי עניין, ממש כמו יתר חברי ההנהלה, ונתפסת כגורם "מבין עניין"? איך ניתן למנף את הידע של הביקורת הפנימית לצורך שיפור האפקטיביות של הציות בארגון באופן שוטף? כיצד ניתן לפתח בקרב צוות הביקורת חשיבה אסטרטגית? איך ניתן להבהיר את הגבולות הלא ברורים שבין עבודות ייעוץ לביקורת פנימית? כיצד מתקדמים יד ביד עם שינויים טכנולוגיים, ואיך להכשיר את צוותי הביקורת הפנימית של העתיד?

כיום - יותר מתמיד - הארגונים השונים נדרשים להתאים את עצמם למציאות דינמית ולשינויים מפתיעים שמתרחשים לעתים במהירות רבה. במציאות כזאת מערך הציפיות מהמבקר הפנימי רק הולך וגדל, ואנו נדרשים להתאים את עצמנו.

הגיליון הנוכחי עוסק, בין היתר, בחידושים המתהווים בעבודת ביקורת פנימית מבוססת אנליטיקס תוך השוואה לביקורת המסורתית. דגש נוסף בגיליון ניתן להבנה לעומק של סיכונים טכנולוגיים, סייבר ושירותי ענן. עוד מתמקד הגיליון בניהול סיכונים וממשל תאגידי וביחסי הגומלין של המבקר הפנימי עם "מעגלי ההגנה" האחרים בארגון ובוחן גם נושאי סיכון חדשניים, ובהם סיכונים אסטרטגיים שעל המבקר הפנימי לבחון.

אני בטוחה כי גיליון זה יסייע בידינו, המבקרים הפנימיים, בבנייה ובהיערכות מושכלת לקראת השנה הבאה.

ברצוני להביע את תודתי לחברי המערכת, אשר שקדו על הכנת הגיליון והוצאתו לאור, ובמועד כתיבת שורות אלו כבר נרתמים לעריכת הגיליון הבא של כתב העת בנושא "צעד אחד קדימה".

תודה מיוחדת למרגלית שפרבר על הירתמותה ותרומתה הרבה להפקתו של כתב העת בפורמט זה.

בהזדמנות זו אני מתכבדת גם לפנות אליכם הקוראים בקריאה להצטרף אלינו ולקחת חלק פעיל בעשייה המקצועית של כתב העת.

משולחן האגוד

עדכוני מערכת כתב העת

מערכת כתב העת החליטה כי החל מהגיליון הבא, כתב העת ייצא באופן קבוע פעמיים בשנה בסמוך לחג הפסח ובסמוך לחגי תשרי. לפיכך, הגיליון הבא שכותרתו תהיה "צעד אחד קדימה" יתפרסם בין החודשים מארס לאפריל 2017. ניתן לשלוח מאמרים מוצעים עד ה-15 בינואר 2017.

שינויים לחוק הביקורת הפנימית

מאז חוקק חוק הביקורת הפנימית בשנת 1992 היו מספר יוזמות לשנותו, יוזמות שנמשכות גם בימים אלה. IIA ישראל איגוד מבקרים פנימיים בישראל (להלן האיגוד), פועל מול גורמים בממשל וברשות המחוקקת על מנת להשפיע שהתיקון שיחוקק יסייע לחיזוק מקצוע הביקורת הפנימית, לחיזוק מעמדם של המבקרים הפנימיים ולשיפור רמתם המקצועית.

עיקרי השינויים שהאיגוד פועל לקדמם הם:

- החלת חוק הביקורת הפנימית על גופים שכיום הוא אינו מוחל עליהם או קיים ספק אם הוא מוחל עליהם, כמו מינהל בית נשיא המדינה, מינהל הכנסת, מינהל מבקר המדינה, הסוכנות היהודית, קרן קיימת לישראל, ההסתדרות הציונית העולמית, קרן היסוד, צה"ל וכדומה.
- בשונה מכל תאגיד אחר, במשרדי ממשלה ויחידות הסמך אין ועדת ביקורת. לפיכך, נוצר צורך בהקמת ועדה מקצועית במשרד המשפטים, אשר תהיה בעלת סמכות הכרעה במחלוקות במספר עניינים מרכזיים הקשורים לביקורת הפנימית במשרדי הממשלה ויחידות הסמך, כגון תכנית העבודה של המבקר הפנימי, מינוי המבקר הפנימי, והפסקת כהונתו.
- עיגון מעמדם ותנאי העסקתם של המבקרים הפנימיים במשרדי הממשלה ויחידות הסמך, על מנת לחזק את מעמדם, ובכך להגדיל את המשקל המיוחס לביקורת הפנימית בגופים המבוקרים. בהתאם להמלצות ועדת פרידמן, מוצע כי המבקר הפנימי ישובץ במשרה שמעמדה מקביל לתפקיד סגן מנהל כללי, ובאופן זה אף ייקבע שכרו. סטייה מהקניית מעמד זה למבקר הפנימי תתאפשר רק בהחלטה מנומקת בכתב על ידי הוועדה שצוינה לעיל.
- קיום זיקה בין התואר המהווה תנאי כשירות למבקר פנימי לבין מקצוע הביקורת הפנימית.
- חיוב גוף ציבורי בפרסום שנתי של גילוי שיכלול פרטים על מסגרת הביקורת הפנימית, כפי שנתקיימה אצלו בשנה החולפת, וזאת על מנת למנוע מצב שבו גוף ציבורי ממנה מבקר פנימי כדי לצאת ידי חובה בלבד, ואינו מאפשר למבקר לפעול ביעילות או שאינו מייחס חשיבות להמלצותיו.
- הרחבת רשימת התפוצה של דוחות הביקורת הפנימית והסדרת האופן לאיסוף תגובות המבוקרים לטיוטת הדוח ואופן ההתייחסות בדוח הביקורת לתגובתם.
- ההבהרה שאין לקבוע תקופת כהונה קצובה מראש למבקר פנימי, וכן לאפשר למבקר הפנימי להשמיע את דעתו בדבר הפסקת כהונתו, וככל שהמבקר הפנימי סבור כי הפסקת הכהונה נובעת משיקולים ואינטרסים זרים לתפקודו.
- תיקון לנוסח הנוכחי בחוק שלאחריו תכנית העבודה השנתית תיקבע בהתייעצות עם הממונה על המבקר הפנימי ולא באישורו, על מנת לחזק את עצמאותו ואת אי תלותו של המבקר הפנימי.
- מינוי עובדים במשרד המבקר הפנימי יעשה רק באישורו של המבקר הפנימי.

שיתוף פעולה עם לשכת המבקרים הפנימיים של קניה

במסגרת הקשרים הבינלאומיים הענפים שנוצרו עם איגודים מקבילים ברחבי העולם, פנה IIA Kenya בבקשה לאיגוד לשיתוף פעולה וסיוע בארגון סדנה מקצועית למבקרים פנימיים ראשיים מבנקים, חברות ממשלתיות ועוד ממדינתם. האיגודים בנו תכנית לסדנה מקצועית בהשתתפות מרצים מקניה ומישראל ובשילוב סיורים בת"א ובירושלים. הסדנה נערכה במהלך חודש נובמבר 2016 בהשתתפות כ-50 משתתפים.

עדכונים גלובליים

הכנס השנתי של לשכת המבקרים הפנימיים האירופית ECIIA בשטוקהולם שבדיה

מדי שנה מתכנסת לשכת המבקרים הפנימיים האירופית ECIIA לכנס השנתי שלה. השנה התקיים הכנס בשטוקהולם שבשבדיה בתחילת אוקטובר 2016. נושאו העיקרי היה "GRC" - Governance, Risk-Management, Control"". כלומר - "ממשל תאגידי, ניהול סיכונים ובקרה".

בכנס נטלו חלק כ-800 משתתפים, ולאור התגובות החיוביות מנושא הכנס, הוחלט לייחד גם את הכנס בשנה הבאה (באזל/שוויץ 9/2017) לנושא זה.

הכנס כלל הרצאות מעניינות ובהן:

הרצאה לגבי פרשיית השחיתות ב-FIFA, ביקורת על תרבות הארגון, ביקורת בסביבה תרבותית שונה (כגון סין) ועוד

תובנות עיקריות מההרצאות:

- ממשל תאגידי נאות מתקיים, בין היתר, כאשר הדירקטוריון דוחף את אפו פנימה, אך את אצבעותיו שומר לעצמו (באנגלית זה נשמע קצת יותר טוב: "BOD members should put their noses in but their fingers out").
- חברי ועדת ביקורת צריכים שהמבקר הפנימי ישמור עליהם ועל הארגון באמצעות מתן תובנות באשר לממשל התאגידי, ניהול הסיכונים, בקרה וציות לרגולציה.
- ביקורת פנימית בחברה גלובאלית צריכה להתאים את עצמה לתרבות המקומית. ביקורת בסין שונה מהותית מביקורת בארצות המערב (למשל). אבל בעת ביקורת בחו"ל לא רק המבקר (תרתי משמע) לומד, אלא גם המבוקרים בחו"ל לומדים. הלימוד הוא הדדי.
- הביקורת הפנימית באירופה מורכבת בשל הצורך להתייחס גם לרגולציה של המדינה שבה מבוצעת הביקורת וגם לרגולציה האירופית, שלעתים סותרות זו את זו.
- ה- CRO (מנהל הסיכונים הראשי) של IKEA שיתף את המשתתפים במיוחדות של הביקורת הפנימית בחברה, שבה מנהל הסיכונים הראשי הוא גם המבקר הפנימי, גם קצין ציות וגם אחראי על הבטיחות והאבטחה (כולל אבטחת מידע) וגם על הקו החם... ובנוסף הוא מדווח למנהל הכספים (CFO) ולא לדירקטוריון או למנכ"ל. עד כמה שהמשתתפים השתדלו לשמור על "נימוס ואורך רוח אירופאים", הם לא יכלו להתאפק בהרצאה זו והביעו את תדהמתם (בלשון המעטה) מסטיית הבקורת הפנימית ב-IKEA מהכללים והתקנים המקצועיים בפרט וממשל תאגידי נאות בכלל.

חלק מהחומרים שהוצגו בכנס ניתן למצוא באתר /http://www.eciiastockholm2016.eu/speakers

בהמשך לכנס התקיימו האסיפה הכללית של כל סניפי ECIIA ובהם IIA ישראל, ומפגש הנהגת סניפי ה-ECIIA עם נציגי ה-IIA הבינלאומית. באסיפה הכללית, פרט לנושאים מנהלתיים שוטפים כמו אישור דוחות כספיים ואישור התקציב, נדון שינוי התקנון, ובתוכו (בין היתר) שינוי אופן ההצבעה מקול אחד לסניף להצבעה יחסית לפי כמות החברים בסניף.

המשימה העיקרית של ה-ECIIA היא להיות קולם של המבקרים הפנימיים בפרלמנט של האיחוד האירופי, בבתי הנבחרים במדינות אירופה ובמוסדות השונים ברחבי היבשת, על מנת לקדם את מקצוע הביקורת הפנימית ולהפיץ פרקטיקות מובילות בממשל תאגידי.

במפגש עם נציגי ה- IIA העולמית, נמסרו התובנות הבאות:

- בסין קיימים כמיליון מבקרים פנימיים, מתוכם 35,000 בעלי הסמכת CIA.
- דירקטוריון ה-IIA הבינלאומי אישר חובת 2 שעות CPE שנתיות שיוקדשו לאתיקה, מתוך סה"כ שעות ה-CPE השנתיות, וזאת החל משנת 2017.
- יוקם מאגר בינלאומי של מרצים בביקורת פנימית על נושאיה, לפי תחומי התמחות, שפות וכדומה.
- תכנית "COSO Certificate Program": ה-IIA הבינלאומי הוא אחד מ-5 הארגונים שנותנים חסות ל-COSO. יקוימו סדנאות בנושא - תחילה למדריכים ולאחר מכן ליתר החברים.

את האיגוד ייצג רו"ח דורון רונן, משנה לנשיא האיגוד.

עדכון התקנים המקצועיים הבינלאומיים של לשכת המבקרים הפנימיים העולמית (IIA)

לשכת המבקרים הפנימיים העולמית (IIA) מעדכנת מעת לעת את התקנים המקצועיים על מנת להתאימם לאתגרי הסביבה העסקית והמשתנה ללא הרף. תהליך העדכון כלל חשיפה של טיוטת התקנים לתגובות והערות והסתיים באוקטובר 2016, והחל משנת 2017 ייכנסו לתוקף התקנים המעודכנים.

השינויים העיקריים לתקנים יכללו:

- שני תקנים חדשים העוסקים באמצעי הזהירות שעל המבקר הפנימי הראשי לנקוט כאשר הוא מתבקש ליטול אחריות על פעילות מעבר לניהול יחידת הביקורת הפנימית, והתייחסות למצב שבו הביקורת הפנימית מבצעת מטלת הבטחה על פעילות לגביה ביצעה מטלת ייעוץ בעבר.
- התאמת התקנים לעקרונות הליבה של הביקורת הפנימית.

מהפיכת המידע האנליטי בביקורת הפנימית בארגון

מאת **לינור דלומי**, רו"ח
גמליאל תומר, רו"ח

מבוא

תמורות מהירות בתהליכים עסקיים, גידול בהיקפי המידע הנשמר בארגונים והגידול במרחב הסיכונים שאליהם חשוף הארגון מהווים אתגר למבקר הפנימי, כיום יותר מתמיד.

מעבר מתהליכים ידניים לתהליכים אוטומטיים, וריבוי תהליכים המבוצעים ללא מגע יד אדם, מדגישים את חסרונות המתודולוגיות הקיימות המבוססות על דגימה ידנית.

גידול מתמיד בהיקפי המידע, זמינותו, גודלו ומורכבותו, בין אם מובנה (בעל מבנה ותוכן מוגדרים) או שאינו מובנה, מאלצים את הביקורת הפנימית לרכוש יכולות מתקדמות הקשורות לאיסוף המידע, אחסונו וניתוחו (למשל, זיהוי אוכלוסיות חריגות לתחקור הביקורת).

כיום כבר ברור מעל לכל ספק כי ככל שהסביבה העסקית מורכבת יותר, כך הציפיות של בעלי העניין השונים מגופי הביקורת הפנימית גדולים יותר. הם תובעים תובנות עמוקות יותר מהמידע הארגוני הקיים, אשר מגובות בעובדות ברורות שיהוו בסיס לתמיכה בתהליך קבלת החלטות ניהוליות. הם ידרשו מהביקורת הפנימית מיקוד מתמיד בגורמי הסיכון שאליהם חשוף הארגון. דרישה זו של בעלי העניין תוכל לבוא על סיפוקה באופן המיטבי ככל שהמידע שעליו תתבסס עבודת המבקר הפנימי יהיה איכותי יותר, כזה שכולל ניתוח אוכלוסיית מידע גדולה, וכזה שידווח בזמן אמת או בסמוך לו. בעלי העניין מצפים כי המידע שיקבלו יסייע לניתוח מצבו של הארגון, או לחלופין ישמש אותם ככלי תומך בהחלטות ניהוליות ו/או ככלי תחקור אוכלוסיית המידע המבוקרת.

להשגת מטרות אלו, הביקורת הפנימית נדרשת לבחון את אפקטיביות ניהול הסיכון על ידי שימוש בכלים מתקדמים שיאפשרו הפקת ערך ממשי ועסקי לארגון.

Data Capital ™ (ערך/ הון המידע)

מידע הוא אבן היסוד של כל ארגון ומהווה אחד מנכסיו העיקריים של הארגון. יש המכנים אותו כמטבע של המאה ה-21.

הגידול בהיקפי המידע הנשמרים בארגון יצר ברוב החברות מסד נתוני עתק ("ביג דאטה") הכולל נתונים מבוזרים שאינם מאורגנים על פי שיטה מסוימת. נתונים אלה מגיעים ממקורות רבים, בכמויות גדולות, בפורמטים שונים ובאיכויות מגוונות, ונהוג לאפיינם בחמש תכונות (חמשת ה-V-ים):

Volume נפחי מידע הולכים וגדלים.

Velocity מהירות זרימת המידע גדלה בקצב מתמיד.

Variety הגיוון במאפייני המידע הולך וגדל.

Volatility קצב זרימת המידע הולך וגדל.

Veracity מהימנות איכות נתונים מוטלת בספק.

האתגר בניהול נתוני העתק בכלל וניתוחם בפרט הוא גדול. מסדי הנתונים הקיימים כיום בארגונים אינם בנויים לאחסון ולניתוח כמויות מידע גדולות, שאינו מובנה לפי תבניות אחידות וידועות מראש. עם זאת, העלות הזולה יחסית של אמצעי האחסון מאפשרת לאותו מידע, המגיע משלל מקורות (אתרי אינטרנט, רשתות חברתיות, מכשירים סלולריים, מצלמות אבטחה, חיישנים ועוד), להיאגר בארגון, להשביח מידע קיים ולהוות כלי תומך להחלטות ניהוליות המתקבלות לאחר ניתוחם, או לחלופין להוות כלי תומך לבחינת יישום החלטות ניהוליות ועסקיות בארגון.

Data Analytics

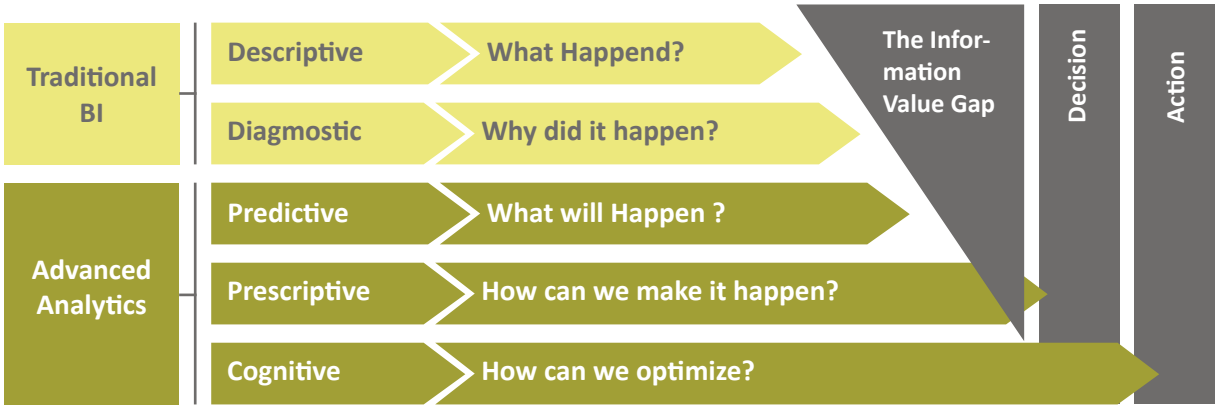
המושג Data Analytics מייצג תהליך של בחינת נתונים גולמיים במטרה להסיק מסקנות ותובנות בנוגע לסוגיה עסקית. תהליך זה מאפשר לארגון לחשוף דפוסי התנהגות ואירועים חריגים ולבסס תובנות הנוגעות לנושא הנבחן.

ביקורת אנליטית היא שילוב של טכנולוגיות העוסקות בכריית מידע (Data Mining) והצגתו (Data Visualization). טכנולוגיות אלו מאפשרות איתור ושליפת נתונים ממאגרי המידע.

החידוש בביקורת פנימית מבוססת אנליטיקס, לעומת הביקורת המסורתית, הוא שהראשונה תשתמש במידע הארגוני ותייצר ממנו תובנות המזינות את תהליכי קבלת ההחלטות בארגון. כמו כן, בביקורת מבוססת אנליטיקס, נלקחת בחשבון כל האוכלוסייה המבוקרת, בהתאם לתקופה המבוקרת, והיא כוללת את הנתונים אודות האוכלוסייה המבוקרת מכל המערכות המעורבות בתהליך העסקי. לעומת זאת, הביקורת המסורתית תמשיך להיות מבוססת על תהליך מחזורי שתחילתו בזיהוי ידני של מטרות הביקורת, המשכו בהערכת אפקטיביות הבקרות באמצעות בדיקתן, וסופו בדגימת אוכלוסייה למדידת אפקטיביות הבקרות או הביצועים התפעוליים. בנוסף, ביקורת פנימית מבוססת אנליטיקס משלבת ניתוח נתונים על בסיס מודלים סטטיסטיים, המאפשרים זיהוי אוטונומי של חריגים מבלי שהוגדרו באופן ספציפי מראש על ידי המבקר, זאת בניגוד לביקורת המסורתית שמזהה חריגים על סמך מודלים דטרמינסטיים בלבד (לדוגמה Rule Base, כלומר ניתוח נתונים על פי חוקים עסקיים שנועדו לבחון הלימה בין הרגולציה ונוהלי הארגון לבין הקיים בפועל בתהליך העסקי).

הטמעת ביקורת פנימית מבוססת אנליטיקס תצמצם את המגבלה המובנית של הסתמכות מסורתית על מדגמים מוגבלים בהיקפם שנלקחו ממאגרי המידע של הארגון.

יישום תהליכי ביקורת מבוססי אנליטיקס בארגון נשען על שלושה נדבכים עיקריים: המשאב האנושי, מאגרי מידע ויכולות טכנולוגיות. מחזור הניתוח מתחיל מאיסוף נתונים, ממשיך בניתוחם באמצעות כלים אנליטיים וסטטיסטיים, ומתקדם לבניית תובנות וידע עסקי. הניתוח משלב גם ניתוח סטטיסטי, כאשר בשילוב עם שיטות ניתוח משולבות אחרות יכול הארגון לפתח מודלים של חיזוי ובקרה מתמשכים. כלומר, שימוש בטכניקות של אנליטיקס מגביר את ניצול המשאבים הארגוניים, מאפשר לארגון לחזות בעיות פוטנציאליות, ומסייע לו לעבור לגישה פרואקטיבית של קבלת החלטות. משכך, ביקורת פנימית מבוססת אנליטיקס תאפשר לביקורת הפנימית לאתר ולנתח נתונים כדי להרכיב להנהלת הארגון תובנות חוזות פני עתיד, המתמקדות בהשאת הערך העסקי של הארגון ולהקטנת פער המידע כפי שמודגם באיור הבא:



האיור ממחיש את הפער הקיים בין בחינת המידע הקיים בארגון לתהליך הפקת החלטות ניהוליות. ניתוח המידע בראייה היסטורית מספק למקבלי ההחלטות תמונת מראה של הסוגיה העסקית הנבחנת, וממנה נדרשים מקבלי ההחלטות לפרש את המפה העסקית העתידית שתתמוך בהחלטות עסקיות. פער זה מטופל בתהליכי Data Analytics המספק למקבלי ההחלטות ראייה צופה פני עתיד בהתייחס למידע הקיים בארגון, ומשקלל את אופן קבלת ההחלטות על ידי שימוש במודלים המאפשרים לארגון לבחון את השפעת מגוון האירועים בהתנהלות עתידית.

ביקורת מתמשכת (Continuous Auditing) וניטור מתמשך (Continuous Monitoring)

הביקורת האנליטית עצמה תבוצע בשני וקטורים במקביל, על ידי שתי פונקציות נפרדות בארגון:

ביקורת מתמשכת (Continuous Auditing) מבוצעת על ידי "קו ההגנה" השלישי - יחידת הביקורת הפנימית, וניטור מתמשך (Continuous Monitoring) מבוצע על ידי "קו ההגנה" הראשון והשני - היחידות העסקיות.

על פי הגדרות ה-IIA, ביקורת מתמשכת היא ביצוע הערכה מתמשכת של גורמי סיכון או אמצעי בקרה, המבוססת על היקף נתונים או עסקאות עצום. זאת בשונה מביצוע הערכות תקופתיות של גורמי סיכון או אמצעי בקרה מבוססי מדגם. ביקורת מתמשכת כוללת ניתוח של מקורות מידע אחרים העשויים לחשוף אירועים חריגים בסביבה העסקית של הארגון, כדוגמת זיהוי אירועי אבטחת מידע, שימוש שאינו הולם בהרשאות למערכות המידע, זיהוי אירועים חריגים בתהליכים עסקיים, שינויים שאינם מורשים בהגדרות מערכות מידע, בחינת אפקטיביות הבקרות האפליקטיביות או הפרדת תפקידים.

ניטור מתמשך מאפשר שימוש בדגימה רחבה ומטריציונית המגדילה את הביטחון של ההנהלה בנושא הביקורת, ומאפשר החלפת דגימות ידניות בניתוח אנליטי תוך שמירה על יכולת כיסוי של 100% מהאוכלוסייה הנבדקת.

ניתוח נתונים וניטור רציף של בקרות (במקום שימוש בטכניקות דגימה בלבד) מביאים לארגון ערך מוסף בכך שמאפשרים ליחידות העסקיות (קו ההגנה הראשון והשני) לבצע ניטור מתמשך שאינו תלוי במועד הביקורת. המשמעות היא שיחידות עסקיות אלו יוודאו באופן רציף ציות לנהלים, תקנות, הוראות ותהליכים על פי כוונת ההנהלה, על ידי ניתוח פרואקטיבי של חריגים באוכלוסייה המנותחת, אשר יאפשר יצירת מודל של חיזוי אנליטי להתרעה על חריגות, ללא צורך בהכרח בביקורת יזומה.

יתרונות שימוש במתודולוגיית אנליטיקס בביקורת הפנימית

טכנולוגיות העוסקות באיתור מידע (Data Mining) והצגתו (Data Visualization) מאפשרות איתור ושליפת נתונים ממגוון מאגרי מידע בארגון הנוגעים לתהליך העסקי. ביקורת אנליטית תתבסס על נתונים אורכיים (נתונים לאורך זמן). ככל שמשך התקופה גדול יותר, כמות הנתונים גדולה יותר, ומכאן שרמת הדיוק בזיהוי הסיכונים שאליהם חשוף הארגון בתהליך תגדל. כאמור, שילוב אנליטיקס יפיק לדרג הניהולי תוצר המבוסס על תובנות עסקיות מהמידע הארגוני הקיים, לרבות ניתוח דפוסי נתונים על פני מערכות מרובות עסקאות. תובנות עסקיות אלה יתארו את העתיד, עם דגש על דפוסים אנליטיים לניבוי תחזיות, נתונים להדמיה וניתוחים של מצבים שונים. תובנות אלו יסייעו להנהלה לקבל החלטות מהירות, אפקטיביות ומדויקות. כמו כן, שימוש בכלים אנליטיים יאפשר איתור רציף מבעוד מועד של מעילות והונאות, שגיאות או מגמות שליליות תוך איתור הסיבות לחריגים ובחינה מעמיקה של הסיבות לליקוי/טעות. יישומים אלו, המייצרים ערך מוסף משמעותי לארגון, ניתנים להעברה לשימוש רציף ביחידה העסקית המבוקרת.

יתרון נוסף הוא שיפור דרמטי ביכולות הבקרה על ביצועים עסקיים, תפעוליים ופיננסיים. הארגון יעבור מביצוע ביקורות נקודתיות לביקורות רחבות ומקיפות יותר. טכניקות אלה יאפשרו למבקר הפנימי למזער את השימוש בביקורת המבוצעת באופן ידני, להסיט תשומות מביקורות מוטות תשומות כ"א לביקורות ממוכנות, וליצור מפת סיכונים דינמית המושפעת מהביצועים העסקיים של הארגון. השימוש בטכניקות אנליטיקס יסייע למבקר לענות על שאלות כדוגמת: "מה קרה ולמה?" "היכן הבעיה?" "מה נדרש לעשות כדי לפתור אותה?" ו"מה יקרה אם המגמות הללו ימשכו"?

בעזרת שימוש באנליטיקס, יוכל המבקר הפנימי לבצע ניתוח מתוחכם של מפת הסיכונים שאליה חשוף הארגון ולטפל בגורמי הסיכון ביעילות. יישום טכניקות חיזוי ותחקור, כמו גם אוטומציה של רוטינות המאיצות את הערכת הסיכון הארגוני, מאפשרים לביקורת הפנימית להתמקד באופן אינטנסיבי בסיכונים הנוכחיים ובאלה המתהווים שאליהם חשוף הארגון, ואף מספקים לארגון מידע מהיר שבו הוא יכול להשתמש כדי לקבל החלטות לגבי הסיכונים שזוהו. שילוב אנליטיקס יביא להנהלה ערך מוסף בדמות יכולת מתמשכת לבקר ולמזער סיכונים אלה, תוך קבלת החלטות איכותיות וכמותיות הקשורות ברמת הסיכון שזוהה.

תועלת מהשימוש בכלי ניתוח וחיזוי בביקורת הפנימית

השפעה

- יכולת חיזוי להשפעה של ליקוי בודד על תהליך/הפעילות/הארגון
- הצעות למודל תהליכי/עסקי משופר בעתיד המלצות חכמות יותר
- שיפור תהליך בקרה ע"י פתרונות אנליטיקס
- יצירת שפה אחידה בין המבקר למבוקר וקיום דיאלוג מתמשך בתהליך הביקורת

ביטחון

- הגדלת הביטחון בביקורת באמצעות דגימה רחבה יותר
- החלפת דגימות ידניות בטסטים אנליטיים
- יכולת לכיסוי 100% מהאוכלוסייה הנבדקת
- יכולת כיסוי החלטות על בסיס מידע אמין ואיכותי
- מעבר מדגימה אקראית לדגימה מושכלת

ניתוח סיבות

- איתור סיבות לחריגים באמצעות כלים ייעודיים
- בחינה מעמיקה וזיהוי של סיבות לליקוי/טעות

תובנות

- שיטות ביקורת חדשות המתמקדות בערך עסקי
- יכולת מתן תובנות עסקיות בתחום הנבדק ובתחומים משיקים
- יכולת הצלבת נתונים בין תחום לתחום
- תובנות חוזות פני עתיד

אתגרים בשימוש במתודולוגיית אנליטיקס בביקורת הפנימית

השימוש באנליטיקס בביקורת פנימית מחייב התמודדות עם אתגרים לא פשוטים. להלן העיקריים שבהם:

- חוסר פתיחות מצד הארגון לקבל ממצאים שלא בדוח כתוב, אלא באמצעות כלי ויזואלי המאפשר תחקור מעמיק.
- שוני בתפיסה בין "חריג" שהתקבל בבדיקות ה-Rule Base לבין "חריג סטטיסטי" (תצפית חריגה ביחס לאוכלוסייה שאליה היא מושוות).
- קושי בשליפת נתונים ממערכות המידע הקיימות בארגון.
- טיוב נתונים המגיעים ממגוון מאגרי מידע וערוצי מידע ויצירת קובץ נתונים אחוד.
- התמודדות עם ערכים חסרים בשדות.
- מחסור בנתונים - למשל, עומק תקופה, כמות רשומות נמוכה יחסית להסקה סטטיסטית ומספר מאפיינים קטן. כל אלה מקשים לבסס מסקנות באופן אנליטי.

דוגמאות ליישום אנליטיקס כחלק מעבודת הביקורת הפנימית

ביקורת שכר אנליטית

המניע העסקי לביצוע ביקורת זו הוא צמצום חשיפות החברה בנושא השכר, מכיוון שתהליך השכר מורכב וכפוף למספר גדול של חוקים, רגולציה, ושינויים תכופים בהגדרות תפקידים. לפיכך, תהליך זה יכול לחשוף את החברה לסיכונים משמעותיים, כגון סיכוני תביעות מצד עובדים, קנסות לפי דיני העבודה, חשיפה למעילות והונאות וכיו"ב.

בשונה מביקורות קודמות, שבהן צוות הביקורת ביקש לדגום מספר מוגבל של אירועים ו/או תלושי שכר של עובדים - החליטה ההנהלה על שילוב כלים אנליטיים בביקורת, החלטה שתאפשר לבחון את תהליך השכר במלואו, על פני מספר שנים, לרבות כל המערכות המעורבות בתהליך השכר: מערכת דיווח נוכחות של הארגון, מערכת ה-ERP של הארגון, מערכת עיבוד השכר וקובצי מס"ב. כמו כן, תהליך הביקורת כלל את כל אוכלוסיית העובדים בהתאם לתקופת הביקורת ולא התבסס רק על מדגם של עובדים. מטרת העל היא יצירת מנגנון לזיהוי חריגות בשכר באמצעות ניתוח כלל מרכיבי השכר (סמלי שכר), בהתבסס על כלים אנליטיים, מודלים סטטיסטיים ושימוש בכלי ויזואליזציה לצורך המחשת התובנות ותחקור תופעות חריגות.

ביצוע תהליך הביקורת כלל יצירת בסיס נתונים אחוד המורכב מכל נתוני תלושי השכר, מערכת ה-ERP של הארגון, מערכת עיבוד השכר והמס"ב, וביצוע ניתוחים אנליטיים וסטטיסטיים על מאגר הנתונים שהתקבל.

הנגשת תוצר הביקורת כוללת פיתוח כלי תחקור המכיל את כלל נתוני השכר בכלי ויזואלי, שבו הדוח הופך להיות דוח "חי" ואינטראקטיבי ומאפשר לבצע תחקור ולהפיק תובנות עסקיות בצורה ידידותית למשתמש. כלומר, עיבוד של מיליוני רשומות (כ-120 מיליון) לכדי תמונה ברורה של ממצאים חריגים (למשל, עובד שהערך שקיבל בסמל שכר ספציפי, חורג מהממוצע בתוספת שתי סטיות תקן של קבוצת העובדים הדומים לו מבחינת דרגה/ותק, תפקיד בחודש מסוים). תמונה כזו מאפשרת לצוות הביקורת לדגום בצורה מושכלת, מתוך מאגר החריגים ולא באופן אקראי.

להלן דוגמה לגיליון אחד (מתוך מספר גיליונות) שאופיין בכלי הוויזואליזציה והיווה תוצר לביקורת. בתרשימים ניתן לראות כי הגודל מבטא את כמות החריגים. לחיצה על "דירוג" ספציפי יסנן את יתר הגרפים בגיליון בהתאם. באופן דומה, לחיצה על "תפקיד" ספציפי יסנן את הגרפים העוקבים בהתאם.

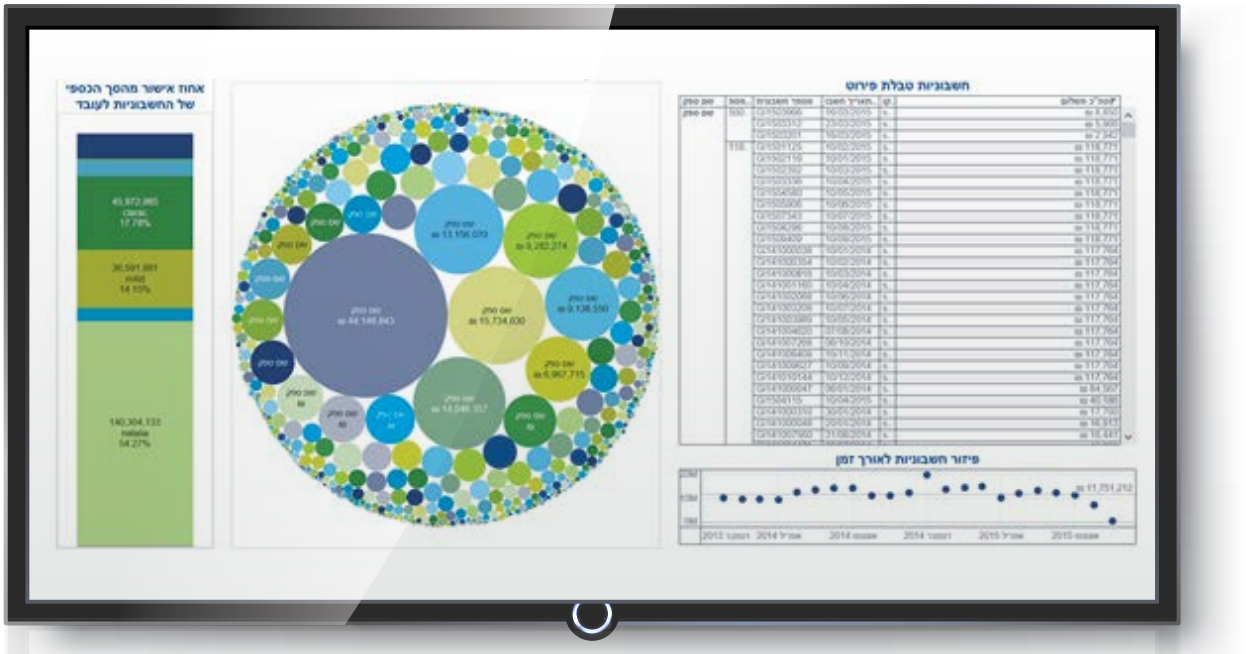
צילום מסך מכלי תחקור שפותח לצוות הביקורת

ביקורת רכש אנליטית

לפניכם דוגמה נוספת לתכנית ביקורת על תהליך הרכש ותשלומים לספקים שבוצעה בחברה המתקשרת עם מאות ספקים ומבצעת אלפי פעולות תשלום חודשיות. הסיכונים שהביקורת תבקש לבדוק בתהליכים אלו כוללים פגיעה בניהול תזרים המזומנים, פגיעה במוניטין, וכמובן סיכוני הונאה ומעילה, שבגינם התבקשה הביקורת לאתר גורמים שיאפשרו להנהלת החברה למנוע מעילות והונאות ולשמור על ניהול תקין של תהליכי הרכש ותשלומים לספקים.

תהליך הביקורת הוגדר ככזה שיתמקד בכל מעגל הרכש, החל מדרישת הרכש ואישור ההזמנה, עובר לקבלת הטובין/שירות וכלה בביצוע התשלום לספק. אולם, בעוד הביקורת המסורתית הייתה מבקשת לדגום מספר מוגבל של אירועים - החליטה ההנהלה על שילוב כלים אנליטיים בביקורת, החלטה שתאפשר לבחון את תהליך הרכש במלואו, על האוכלוסייה כולה, על פני מספר שנים ותוך זיהוי מוקדי סיכון קיימים ופוטנציאליים. יחידת האנליטיקס ביצעה את התהליך באמצעות ניתוח ממוחשב והצלבה של מסד הנתונים הקיים בחברה הקשור לתהליך הרכש: נתוני ספקים והתקשרויות, דרישות רכש, הזמנות רכש, בקרת איכות, חשבוניות ותשלומים לספקים. שימוש בטכנולוגיות אנליטיות אלה מאפשר לארגון להשיג בקרה אפקטיבית על תשלום חשבוניות, לבצע מעקב אחר התקשרויות עם ספקים, ולזהות התנהלות חריגה או דפוסים יוצאי דופן בתהליך, לרבות אנומליות, תוך ניתוח החריגות שנצפו בשרשרת התשלומים והחיובים. התוצר שהעבירה הביקורת הפנימית להנהלת החברה התבסס על החריגות שזוהו, ויאפשר לחברה לבנות תכנית ביקורת המכוונת לאזורים שבהם זוהו החריגות.

בדוגמה זו ניתן לראות התפלגות חשבוניות לאורך זמן ואת ערך החשבונית לכל ספק. ניתן לבצע סינון על ספק ספציפי ולראות את כל הפרטים לגביו, לרבות כמות חריגים לספק לאורך זמן (אם ישנם). ניתן לזהות ענפים שמהם מגיעים ספקים חריגים, יחידות ארגוניות שלא פועלות בהתאם לנוהלי הרכש של החברה, תקופות ספציפיות לאורך השנה שהן חריגות ועוד.



צילום מסך מכלי תחקור שפותח לצוות הביקורת

צילום מסך מכלי תחקור שפותח לצוות הביקורת

טכניקות אנליזה אלו, בתהליך הביקורת, אפקטיביות לא רק בתהליך ספציפי כדוגמת רכש, אלא בכל תהליך ארגוני הטומן בחובו סיכון המפוזר על מספר אתרים גיאוגרפיים או פעילות אופרטיבית גלובלית.

דוגמה זו, המתארת שימוש בטכניקות אנליטיות בביקורת הפנימית, היא אחת מיני רבות. אפשר לציין בהקשר זה גם בדיקה אחרת שבוצעה במסגרת ביקורת פנימית בקרב חברה קמעונאית. הביקורת בחנה נתוני מכירות אל מול נתוני הוצאות בגין מדיה ופרסום (Return On Marketing Investment) במשך תקופת זמן זהה. באמצעות טכניקות אנליטיות שונות נותחו מגמות וחריגות מהיחס הישיר בין הגידול בהוצאות לגידול במכירות. תוצאות הבדיקה אפשרו להנהלה לבחון את תהליך אפקטיביות הפרסום שבוצע על ידי החברה במדיות השונות.

עולם האנליטיקס מאפשר למבקר לבצע ביקורת חכמה ואיכותית יותר במגוון תהליכים ארגוניים, כגון שכר, הפרשות פנסיוניות, הכנסות, ניהול קשרי לקוחות, הוצאות שיווק ופרסום, תפעול מוקדי טלמרקטינג, שרשראות אספקה, זיהוי מגמות דמוגרפיות, ניהול מערכות מידע ועוד.

מתודולוגיה הטמעת אנליטיקס בתהליך ביקורת פנימית

שלב	תיאור	מה נדרש להצלחת התהליך?
1	הגדרת שאלת המחקר והנושא הנבדק	זהה את הסיכונים לתהליך הביקורת הרלוונטי. התחל את הניתוח באזורי סיכון גבוהים.
2	הבנה של מסגרת הפעילות והתהליכים העסקיים	ודא כי אתה מבין את התהליכים העסקיים והסיכונים הטמונים בתהליכים אלו. חשוב ששלב זה יבוצע על ידי תהליך סיעור מוחות בין חברי צוות הביקורת, במטרה להציף מגוון רחב של סיכונים ותרחישים אפשריים, קביעת ערכים תקינים וחריגים ועוד.
3	הגדרת בסיסי הנתונים הנדרשים	הגדר את מערכות המידע הקשורות בתהליך וישויות המידע הנדרשות לתחקור.
4	ניתוח ראשוני (High-Level) לצורך תיקוף מול הגורם העסקי	ניתוח ראשוני של המידע שהתקבל (לדוגמה - סטטיסטיקה תיאורית) וטיובו מול הגורם המבוקר.
5	הפעלת מודלים דטרמיניסטיים	פיתוח מודלים דטרמיניסטיים (על סמך כללים עסקיים) לאיתור מקרים החורגים מתחומי הערכים התקינים.
6	ביצוע ניתוחים סטטיסטיים ביצוע	ניתוחים סטטיסטיים לזיהוי אוכלוסיות חריגות שישמשו כבסיס לאוכלוסיית דגימה.
7	הפעלת מודל אנליטי	פיתוח מודלים אנליטיים לזיהוי קשרים בין ישויות המידע וזיהוי חריגים.
8	סינתזה של תוצרי הניתוח לתובנות עסקיות	פיתוח מודלים אנליטיים לזיהוי קשרים בין ישויות המידע וזיהוי פיתוח שכבת ויזואליזציה להפקת תובנות עסקיות ותחקור חריגים מניתוח המידע בתהליך המבוקר.

גורמי מפתח ליישום נכון של אנליסטיקס בארגונים

- זהה היכן אתה נמצא: הערך את היכולות הנוכחיות שלך, קבל תמונה מדויקת של הפערים. התמקד בפירות התלויים נמוך על העץ ופתח מפת דרכים אנליטית לטווח הארוך.
- שאל שאלות קשות: ודא אילו שאלות חשובות לארגון, לאסטרטגיה ולסדרי העדיפויות.
- העצם את איתור הסיכונים בארגון - איתור ותגובה מהירה לסיכונים הם המפתח להשגת יתרון תחרותי.
- האץ את תהליך קבלת ההחלטות בדבר תובנות המושגות באמצעות אוטומציה של תהליכים קבועים המופעלים על המידע המורכב של הארגון.
- הפוך את אספקת המידע לאוטומטית - ספק אותה להנהלה, ליחידות העסקיות וליחידות הביקורת.
- חתור למגע - התפוקה חייבת לכלול תובנות ומתן מענה על צרכים, על מנת לאפשר למנהלים לקבל החלטות מבוססות עובדות. בעלי העניין השונים בארגון ירצו לראות את המידע, כי הוא הבסיס לקבלת החלטות. המטרה היא להביא את הניתוח ואת המידע כמה שיותר קרוב לשולחנם של מקבלי ההחלטות. יש לשקול שימוש בכלים כדוגמת SAS, ACL ו TABLEAU.
- פתח תרבות מבוססת עובדות. שלב יכולות אנליטיות בתהליך קבלת ההחלטות.
- תרגל אנליטיקס. התאם את הטכניקות לעבודה שאתה רוצה לבצע.

סיכום

בישום אנליטיקס כחלק מעבודת הביקורת הפנימית יש אתגרים אך גם יתרונות רבים. על מנת לעבור לביקורת מבוססת אנליטיקס, על ההנהלה לחשוב מחוץ לקופסה. עליה לדעת לשאול את השאלות הנכונות ולשקול עובדות אנליטיות חדשות, כאשר היא עומדת לקבל החלטה ולוודא כי הכלים האנליטיים והטכנולוגיות שתיישם חייבים לתמוך באסטרטגיה הכללית של הארגון.

קניין רוחני | היבטי ביקורת פנימית הלכה למעשה

מאת **משה כהן,** רו"ח, CRMA
רן מילמן, רו"ח

המאמר מתבסס על תכנית הביקורת בפרסום ה- IIA - auditing the process Intellectual Property מאת ג'יימס פרגסון

מבוא

בעידן המודרני ארגונים רבים מחזיקים בקניין רוחני, כולל פטנטים, עיצובים, מותגים מסחריים, תהליכי עבודה ייחודיים ומאמרים. ההחלטה על הצורך בהגנה על הקניין הרוחני היא אחת ההחלטות שיש לקבל בארגון כחלק מהצורך בשמירה על נכסיו.

בארגון המחזיק בקניין רוחני, תפקידו של המבקר הפנימי הוא:

בחינת יכולת הארגון לזהות את הקניין הרוחני שלו;

בחינת האופן שבו הארגון מעגן את אחיזתו החוקית בקניין הרוחני שלו;

יכולת הארגון לשמור על הקניין הרוחני שלו.

במאמר זה נסקור את הסוגים העיקריים של הקניין הרוחני, ונציין את הנקודות העיקריות שבהן צריך המבקר הפנימי להתחשב בעת הערכת הסיכונים המהותיים הקיימים בתהליך.

מהו קניין רוחני?

קניין רוחני הוא מונח משפטי המגדיר זכויות הקשורות בפרי יצירתו של האדם. בעוד ההגדרה היא רחבה וכוללת מגוון רחב של נכסים, במאמר זה נתמקד בעיקריים שבהם:

פטנטים

סימנים מסחריים

זכויות יוצרים

סודות מסחריים

השלושה הראשונים הם זכויות שברוב מדינות העולם ניתן להגן עליהן בחוק. בניגוד אליהם, היכולת להגן על הסוד המסחרי היא פחותה אך עדיין קיימת בחלק מהמדינות. לפני שנסקור את תהליכי עבודת הביקורת, נערוך היכרות קצרה עם נכסי הקניין הרוחני ונאמוד את ההבדלים העיקריים ביניהם.

פטנט - זכות משפטית בהמצאה שאינה מאפשרת לאחרים להשתמש בה לתקופת זמן מוגבלת. זכות זו מוענקת על ידי מדינה או חבר מדינות לכל המצאה תועלתית (מכונה, תהליך ייצור וכו') או עיצוב, בהתאם למידת הערך שיש בהמצאה מבחינת היצירתיות, וחשוב מכל - מבחינת חדשנות.

סימן מסחרי - מקור הזיהוי הבלעדי של ספק ומבדיל אותו מספקים/מוצרים אחרים. סימן מסחרי מתייחס למילים ייחודיות, ביטויים, עיצובים וסמלים. אין חבות לרשום את הסימן המסחרי על מנת להגן עליו בחוק, אך רישום כאמור יכול לחזק את מאמצי ההגנה המשפטיים בעת הצורך.

זכויות יוצרים - כוללות את הפרסומים המקצועיים והמקוריים של הארגון ושליחיו. זכות זאת מבוטאת בעיצוב היצירה ובצורתה האומנותית, וכוללת חומרים כתובים, צילומים, אנימציות, סרטי וידאו וכדומה. בישראל, כמו בעולם, זכויות היוצרים מעוגנות בחוק. מכאן שרישום בגוף ממשלתי או באמצעות עו"ד יכול להוות חיזוק לקו ההגנה במקרה הצורך אך אינו בהכרח נחוץ.

סוד מסחרי - מידע פרטי השייך לארגון. בניגוד לשאר סוגי הקניין הרוחני החשופים לציבור, ההגנה המשפטית על קניין זה היא קשה ומורכבת יותר משום שהחוקים השומרים עליו פחות ממוקדים מאלה השומרים על הזכויות האחרות שצוינו לעיל. מכאן שהאחריות המרבית בהגנה על זכויות אלה "נופלת" על הארגון.

מה בין סוד מסחרי ופטנט?

במקרים רבים יכולים הסוד המסחרי והפטנט להגן על אותן היצירות, ולכן על הארגון לבחור את הדרך שבה הוא שומר על הקניין שלו. בכל אחת מן האפשרויות יש יתרונות וחסרונות. בטבלה הבאה נבחן את היתרונות והחסרונות של הסוד המסחרי לעומת הפטנט.

סוג הקניין	פטנט	סוד מסחרי
דוגמא	קופקסון חברת טבע	חברת קוקה קולה
חשיפה לציבור	חייב לחשוף את ההמצאה	אין חשיפה של ההמצאה
תקופת ההגנה	20 שנה. ב-2014 פגה תקופת ההגנה ומאז חברות מתחרות החלו ליצר תרופות דומות	בלתי מוגבלת
הגנה משפטית	חזקה	חלשה
תקפות הזכויות	מרגע הגשת הבקשה לרשות הממשלתית הרלוונטית	מיידית
עלויות ראשוניות	עלויות עריכה ורישום	אין עלויות רישום
משאבים הנדרשים לתחזוקה	עלויות חידוש אחת לכמה שנים	עלויות הכרוכות בבניית מערך ארגוני המגן על סודיות היצירה
חיקוי הנדסי (פיתוח לאחור)	קיימת הגנה מכך בתקופת ההגנה	אין הגנה. במהלך השנים קמו לחברה מתחרים רבים המנסים לשחזר את ההצלחה (RC, פפסי וכו')

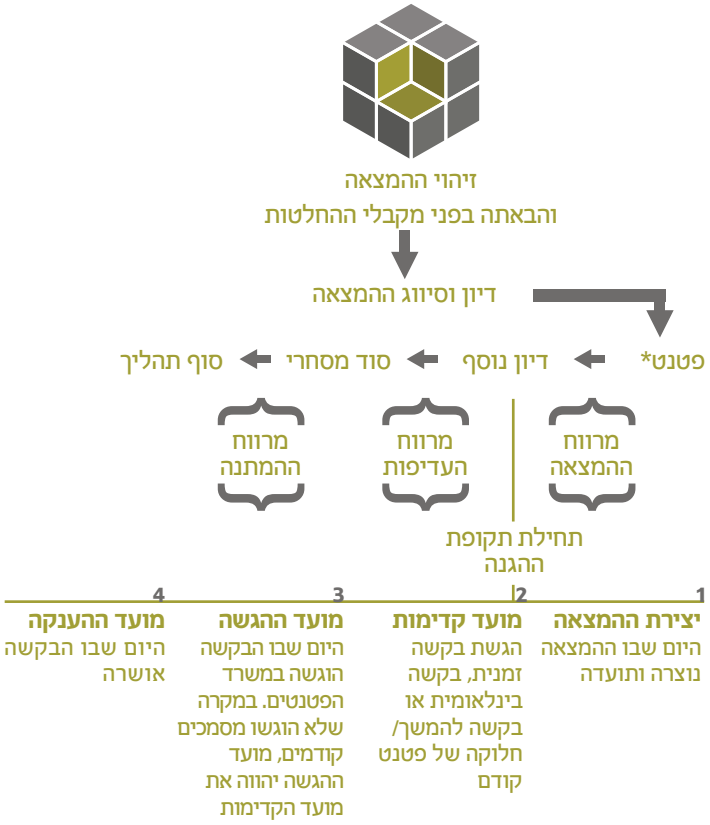
זיהוי הקניין הרוחני

זיהוי הקניין הרוחני הוא תהליך מתמשך הדורש השקעת משאבים של הארגון. הקניין הרוחני יכול להיווצר במחלקות שונות בארגון. מחלקת מחקר ופיתוח יכולה ליצור פיתוח חדש למוצר קיים, מחלקת פיתוח עסקי יכולה לחתום על חוזה לשיתוף פעולה עם ארגון אחר לצורך פיתוח משותף של מוצר חדש, ומחלקת השיווק יכולה לפרסם ידיעה באתר הארגון החושפת פרטים על המוצר החדש של החברה. במקרים אלה גלומות חשיפות רבות לגניבת ההמצאה על ידי גורמים חיצוניים או פנימיים. היכולת של הארגון לזהות את הקניין הרוחני שלו וליצור תהליכים המאפשרים לו בקרות מונעות ובזמן אמת, תאפשר לו להגן על נכסיו. באופן זה, תפיסת הקניין הרוחני ושיוכו לארגון יכולים להיעשות בצעדים פשוטים כגון:

- החתמת אנשי הפיתוח על חוזים המשמרים את הזכויות בקניין הרוחני לארגון.
- רישום מהיר של הקניין הרוחני או שמירה על סודיותו.
- חתימה על חוזים עם צד שלישי המבטיחים שמירה על זכויות הארגון בהמצאות משותפות עתידיות.
- כתיבת נוהלי עבודה סדורים המונעים פרסום או זליגה של מידע חסוי.
- ביצוע הדרכות שוטפות וריענון הידע של העובדים בדבר חשיבות הקניין הרוחני בארגון.

טיפול בקניין הרוחני

מרגע זיהוי הקניין הרוחני הפוטנציאלי, הארגון צריך לקבל שורת החלטות הקובעות כיצד יש לטפל בקניין הרוחני הזה. על הארגון לבצע בדיקות מקדימות בדבר החופש ליצור (FTO) על מנת לוודא אי הפרה של זכויות קניין של ארגונים אחרים. בהמשך, הארגון צריך לקבל שורה של החלטות בדבר האופן שבו יש לשמור על הקניין הרוחני (לדוגמה, פטנט או סוד מסחרי) ובאילו מדינות (אם בחר לרשום כפטנט). במקרה של פטנט, יש חשיבות עליונה למועד ההגשה. מועד זה יכול לקבוע את הזכאות לפטנט במקרה של קיום המצאות דומות. להלן תרשים לדוגמה לתהליך שעובר פטנט מההמצאה ועד לקבלת הפטנט:



ביצוע ביקורת בנושא קניין רוחני

ההכנה לביקורת הפנימית בנושא הקניין הרוחני צריכה להתחיל בבחירת צוות הביקורת. לאנשי הצוות חייבת להיות היכרות מעמיקה עם הארגון, עם הסביבה העסקית שבה הוא נמצא ועם המדינות שבהן הוא פועל. בנוסף, חברי הצוות חייבים לגלות הבנה בעולם הקניין הרוחני, ולכן חשוב כי צוות הביקורת יעבור הכשרה מקצועית בנושא. הכשרה מעין זאת יכולה לכלול קורסים וסדנאות בנושא הקניין הרוחני, שיחות עם גורמי מקצוע (לדוגמה, עם עו"ד בתחום הרישום והליטיגציה של פטנטים), איסוף חומרים מהרשת (תכניות ביקורת פנימית, מאמרים, פרסומים של גופים מקצועיים, פורומים של אנשי מקצוע וכו'). לבסוף, ניתן לקבל מידע נוסף מהגוף המבוקר עצמו באמצעות שיחות עם ההנהלה הבכירה, השתתפות בכנסים מקצועיים פנימיים וקריאת חומרים רלוונטיים של הארגון.

הביקורת הפנימית יכולה להיערך במגוון רחב של דרכים הנוגעות לקניין הרוחני בארגון. **מיקוד הביקורת יכול לכלול אחד או יותר מהנושאים הבאים:**

- יעילות תפעולית בתהליכי העבודה הקשורים בהיבטי הזיהוי, הפיתוח והניהול של הקניין הרוחני;
- מילוי הדרישות החוזיות והאחריות הארגונית בכל הקשור בקניין הרוחני;
- מילוי הדרישות הרגולטוריות ועמידה בחוקים הרלוונטיים באזורי הפעילות השונים;
- ההיבט הפיננסי והחשבונאי הקשור בקניין הרוחני.
- שמירה על הקניין הרוחני במערכות המידע של הארגון.

קביעת מיקוד הביקורת צריכה להיערך בהתאם לסקירה הראשונית של הקניין הרוחני הקיים בארגון, תהליכי העבודה הרלוונטיים וזיהוי ואמידת הסיכונים הקיימים בהם.

את הביקורת יש להתחיל בסקירה ראשונית של הגוף המבוקר ושל תהליכי העבודה הרלוונטיים לנושא הביקורת. סקירה זו תספק למבקר הפנימי ולצוותו הבנה ראשונית של זהות האחראים על הקניין הרוחני בארגון (פנימיים וחיצוניים) ומהי המחויבות של הגורמים הללו לשימור הקניין הרוחני הקיים ולזיהוי קניין חדש שיכול להוסיף ערך לארגון. במהלך הסקירה הראשונית על

המבקר לתעד את כלל הנהלים הרלוונטיים בנושא ואת המסמכים המתארים את גישת ההנהלה ואת תהליכי העבודה הקיימים בארגון. מסמכים כאלה יכולים לכלול מצגות הנהלה, דיווחים לדירקטוריון, פרוטוקולים של דיונים פנימיים, תרשימים של תהליכים פנימיים בחברה, התכתבויות פנימיות וכו'. הסקירה הראשונית תאפשר למבקר למפות את המבנה הארגוני ואת תהליכי העבודה בארגון, ולהתחיל לגבש הבנה של הסיכונים שבפניהם עומד הארגון והיכן נמצאות החשיפות המהותיות.

כאשר המבקר עומד להעריך את הבקרות הקיימות בארגון לצורך שמירה על הקניין הרוחני, חשוב שיבין כיצד הארגון מזהה את הקניין הרוחני הפוטנציאלי הקיים בו ואת התהליך שהארגון מקיים לצורך הפיכתו לנכס. יש לוודא כי הארגון יודע מה שייך לו ומתחזק רשימת מלאי הכוללת את כלל החוזים והרישיונות הקיימים ואת המידע הרלוונטי לגביהם. לצורך כך, על המבקר להכיר את תהליך "תפיסת" הקניין הרוחני בארגון.

על המבקר לבחון האם קיימים תהליכי עבודה ונהלים סדורים המאפשרים את זיהוי הקניין שנוצר והעברתו לגורמים האמונים על כך לצורך "תפיסתו".

לצורך קבלת נקודות מידוד, ניתן להיעזר במדדים המתפרסמים באתרים של הרשויות השונות. כך לדוגמה ניתן לראות מהו הזמן הממוצע שלוקח ל-USPTO להחזיר למגיש הבקשה את הפעולה המשרדית הראשונה שנעשתה בהקשר לבקשה שלו. יש לציין שתשובה זו יכולה להיות בקשה לחומרים נוספים ו/או שינוי בבקשה. בכל מקרה, אי קבלת כל תשובה בנושא הפנייה בטווח זמן זה צריכה להדליק נורות אדומות בארגון.

מטרת המבקר היא לבחון את תהליכי קבלת ההחלטות, הביצוע והמעקב בארגון. **כחלק מזה יכול המבקר לבחון:**

- האם ההנהלה מקיימת דיון לזיהוי הקניין הרוחני, לסיווגו ולאופן הטיפול בו - מועד ההגשה, מקום ההגשה הגיאוגרפי וכו'?
- האם הארגון מיישם באופן נאות את ההחלטות שהתקבלו על ידי ההנהלה בדרך, בזמן ובמקום שנקבעו?
- האם מבוצעת בקרה אחר טווח הזמן שבין יצירת ההמצאה לבין הגשתה לרשויות?
- האם מתנהל מעקב סדור ומתועד אחר השלבים שבהם נמצא הקניין הרוחני בדרך לקבלת הפטנט?
- האם מבוצע מעקב אחר הזמנים בין שלב לשלב מיום ההגשה ועד ליום קבלת הפטנט?

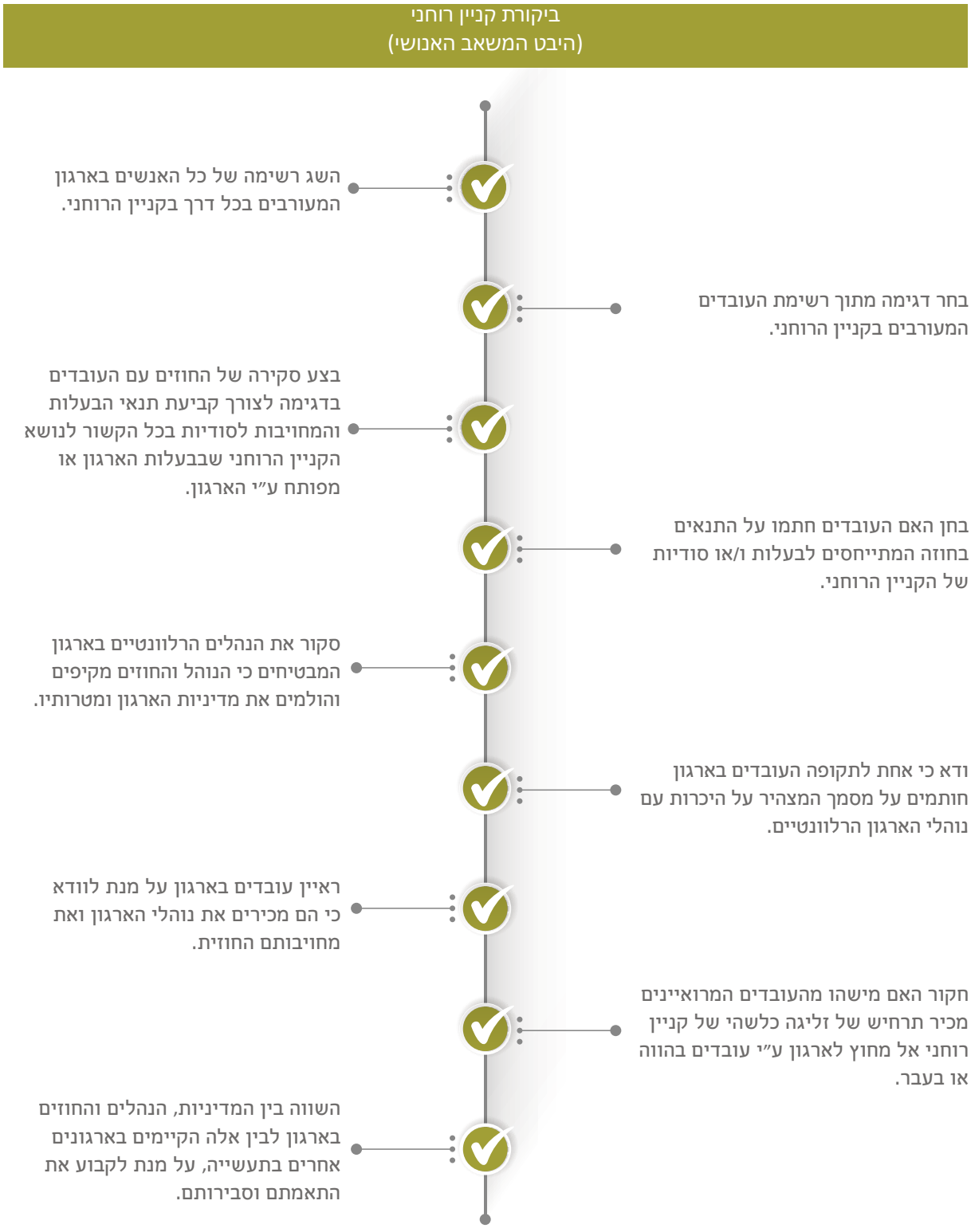
לעתים יבחר הארגון לא לרשום את ההמצאה כפטנט אלא לשמור אותה כסוד מסחרי. אין זה אומר שבמקרה זה לא צריך להחזיק תיעוד להמצאה. על המבקר הפנימי לבחון את יכולתו של הארגון לזהות ולתעד את הסודות המסחריים שלו ולשמור עליהם. בתוך כך, על המבקר לבחון כי כל מי שחשוף לסודות המסחריים, לרבות עובדים, קבלני משנה וספקים, חתומים על מסמכים משפטיים תקפים המחייבים שמירת סודיות.

סיכונים והזדמנויות בקניין הרוחני

בעוד שלכל ארגון קיימים סיכונים הקשורים בפעילות הייחודית שלו, יש מספר חשיפות הרלוונטיות לכל ארגון המחזיק בקניין רוחני. חשיפות אלה כוללות, בין היתר, גניבת קניין רוחני, כישלון ברישום הקניין או בחידוש הרישיון שלו, וחוסר בתקשורת בארגון בין גופים וממשקים שונים היוצרים קניין רוחני לבין אלה האמונים על השמירה עליו. על המבקר לוודא כי מדיניות ונוהלי הארגון נותנים מענה לסיכונים אלה. מלבד זיהוי הסיכונים בתהליך, ביקורת פנימית בנושא הקניין הרוחני יכולה להפנות את תשומת הלב של ההנהלה להזדמנויות הקיימות בו. אחת כזאת ניתן למצוא בבחינת החופש ליצור שהוזכרה לעיל. בעוד הבדיקה נועדה לצורך בחינה של אי קיום המצאות קודמות, סקירת השוק והפטנטים הקיימים בו יכולה לתת להנהלה תמונה על מצב התחרות בשוק, הבנת המגמות הקיימות לפי אזור גיאוגרפי וטכנולוגי וזיהוי כישרונות בתעשייה.

חשוב לזכור שבעולם של ממציאים שמתחדש כל הזמן, זיהוי החולשות בתהליך הקניין הרוחני הוא תהליך מתמשך שיש לבחון אחת לתקופה. בעולם כזה, עבודת המבקר הפנימי היא להתעדכן בהתפתחויות החלות בארגון עצמו, בסביבה העסקית שלו וברגולציה, ולוודא כי הארגון מתאים את הבקרות שלו לשינויים החלים בהם.

דוגמה למדגם ביקורת הרלוונטי למשאבי האנוש בחברה:



ECIIA Conference 2017 is coming to Switzerland!

IIA Switzerland is pleased to announce that the ECIIA Conference 2017 will be held in Basel. The ECIIA Conference will be taking place at the Congress Center Basel from Wednesday 20 September to Friday 22 September 2017.

The theme for the conference is "From Insight to Influence". We aim to deliver a world-class program covering current issues impacting the profession.

What will be expected:

- 2 conference days with plenary sessions and several tracks with concurrent sessions
- more than 40 outstanding speakers
- Welcome Reception on Wednesday 20 September in the Museum Kleines Klingental in Basel
- Gala Dinner with traditional touch of Basel
- Modern bright daylight flooded congress center

Join us at the ECIIA Conference 2017 and be part of the greatest internal audit event ever organized in Switzerland. You'll embark on an exciting educational journey, rich with insights for internal auditors at every level and an unique opportunity of networking.

Registration will start in the beginning of 2017.

Mark your calendar now. Additional details will be available soon.

Each year, the ECIIA Conference is arranged in different European countries. IIA Switzerland has been selected to host the Conference of the ECIIA (European Confederation of Institutes of Internal Auditing) in 2017.The mission of the ECIIA is "Furthering the development of Internal Audit and its role in promoting good governance at the European level". Our members include the National Institutes of Internal Audit in the countries of the European regions. Our responsibility is to help, develop, share and promote best practices in the private and public sectors. We work hand in hand with other European institutions in the field of internal auditing and control, and represent our members before governments, legislators and professionals.

Our members belong to the IIA Global network, which represents over 180,000 Internal Auditors across the world. We work in close collaboration with the IIA to promote the professional practice of internal audit in Europe.

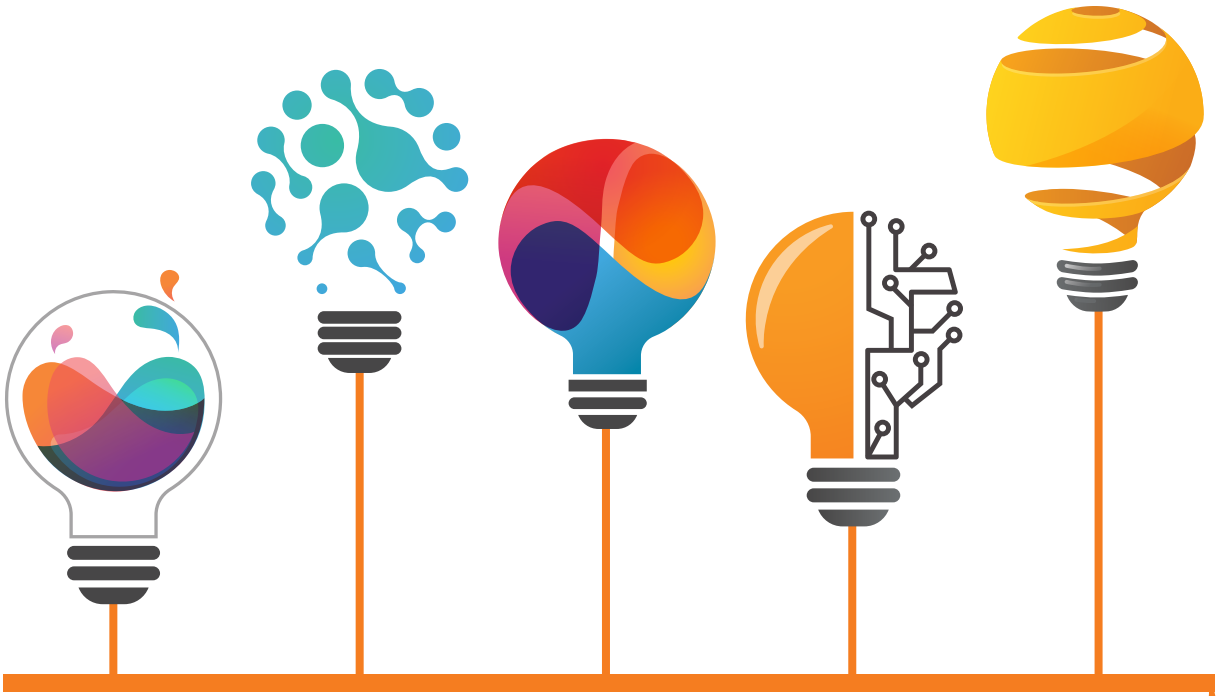
חמש מגמות נקודת מבט רחבה של הצמרת המקצועית הגלובלית על הסוגיות המרכזיות שיעצבו את המקצוע

מאת

מאמר זה הוא תרגום של המאמר Five trends שהתפרסם בגיליון פברואר 2016 של כתב העת **Internal Auditor IA**

ב עולם רצוף בשינויים תמידיים, קשה לחזות את העתיד. עם זאת, בהסתכלות רחבה על עולם הביקורת הפנימית אפשר לזהות מגמות ברורות שעמן מבקרים פנימיים יצטרכו להתמודד ב-5-10 השנים הקרובות: סביבת סיכונים תנודתית, בחינה גוברת אל מול רגולציה, ציפיות גוברות של בעלי העניין, סיכוני טכנולוגיה מורכבים ותחרות על הכישרונות הגדולים במקצוע הביקורת.

ייתכן שלמבקרים לא תהיה היכולת לחזות בדיוק כיצד חמש המגמות האלו יתפתחו בטווח הרחוק, אך מעקב אחר התפתחותן כיום יכול לסייע לביקורת הפנימית ולארגון להתכונן לקראת העתיד. כתב העת "Internal Auditor" ביקש ממבקרים מובילים במקצוע הביקורת בעולם לדון בכל אחת מהמגמות האלו, וכן בשאלה מה צריכים המבקרים הפנימיים לעשות על מנת לספק ביטחון וייעוץ בנושאים אלה בשנים הבאות.



עולם של סיכונים תנודתיים

לוסי אליוט, ACA, דירקטורית, ביקורת פנימית והערכה,
הארגון לשיתוף פעולה ולפיתוח כלכלי (OECD)

מ הירות השינוי בעולם גוברת; השינויים הם מהירים ולפעמים גם מפתיעים. התנודתיות, הרב-תחומיות והמורכבות של סביבת הסיכונים שבה עוסקים המבקרים מתגברות בצורה מתמדת. לדוגמה, משבר המהגרים הנוכחי באירופה משליך על מדיניות ציבורית וכן על המגזר הפרטי, ומשפיע גם על שירותים, שווקים וביטחון מקומיים ולאומיים - ממדים מרובים שעלולים להוביל לסיכוני ביקורת באירופה ומחוצה לה.

דוגמה נוספת היא המעבר לכלכלה דלת-פחמן, שעשויה להשפיע על מודלים עסקיים ורווחיות, ולהוביל לשינוי של פרופיל הסיכון בשנים הבאות. יותר מזה, טכנולוגיות חדישות מאיימות על שווקים קיימים ויכולות להוביל לסיכונים עסקיים אמיתיים ומידיים כגון תחרות חדשה דרך כלכלת השיתוף, כפי שחברת אובר מאתגרת את שוק שירותי המוניות המסורתי.

אם מבקרים פנימיים רוצים להיות רלוונטיים, עליהם להצליח להישאר בקצב של השינויים ולהתמודד עם הדרישות של הסיכונים המשתנים. מבקרים פנימיים אינם יכולים להרשות לעצמם יותר לשקוע באזור הנוחות של עבודת ביקורת צפויה, מחזורית, אולי אף משעממת, ובעלת תוצאות שניתן פחות או יותר לצפות אותן מראש. כעת הם עומדים בפני סביבה לא ודאית של סיכונים, שבה הביקורות ילכו ויהיו מאתגרות, מעניינות ורבות השפעה יותר, כל עוד הם יבינו לעומק את סביבת הסיכונים.

בעולם של היום, סיכונים משתנים מהר יותר מאשר תכנית העבודה של הביקורת הפנימית. לעתים הסיכונים אף משתנים במהלך מטלת הביקורת עצמה ומשפיעים הן על הביקורת הפנימית והן על הלקוח. על המבקר לנתח ולהבין סיכונים חדשים ולתקשר אותם בצורה רגישה, וכן לנהל את ההבחנה בין עבודת ביקורת לייעוץ, הבחנה שהולכת ומיטשטשת ככל שהסיכונים משתנים. על התכניות ולוחות הזמנים לביקורת להיות מותאמים למצב החדש, וכך גם המבקרים, שיזדקקו לכישורים שיאפשרו להם לשלב תובנות מתחומים אחרים, לתקשר עם אחרים ברמה טובה, להביא למודעות חוצת מגזרים ולהקשיב. בנוסף, על המבקרים להישמר מפני "נוקשות אינטלקטואלית", שבמסגרתה אין למבקר את היכולת לחשוב על סיכונים מחוץ לתבונה המקובלת של הלקוח, ולערוך חשיבה קבוצתית בצוות הביקורת.

על מנת להבין את סביבת הסיכונים החדשה הזו, מבקרים פנימיים צריכים להטיל ספק בשיטות ובתובנות ביקורת קונבנציונליות ולחשוב באופן מתמשך לגבי העתיד. לדוגמה, פיתוח הסתכלות אסטרטגית לעתיד יסייע למבקרים פנימיים לבחון מצבים עתידיים אפשריים שונים, לשמור על פתיחות ביחס לתמונה הגדולה, ולגבש הבנה טובה יותר לגבי אתגרים מורכבים בטווח הארוך. המבקרים צריכים לקחת בעצמם סיכונים באמצעות שימוש בגישות חדשות לניהול סיכונים, עדכון המסגרת הניתוחית שלהם, ובחינת דרכים, שיטות וסוגיות חדשות. כך, הסיכונים שלוקחים המבקרים יקצרו פירות. הם ישלבו בעבודה היומיומית שלהם חשיבה חדשנית ויקדמו את מדיניות ומחקר הביקורת שלהם באמצעות ניסוי וטעייה.

נכון שעבור מבקרים מסוימים, קבלת התנודתיות של סביבת הסיכונים יכולה ליצור אי נוחות. אך אם מבקרים פנימיים לא יעדכנו את דפוסי החשיבה שלהם, יבינו את העתיד, ינתחו את ההשפעה על פונקציית הביקורת הפנימית והלקוח ויתאימו את עצמם לכך, הם ייוותרו מאחור בעולם המשתנה.

ציות: מה היקפו?

ג'ונתן בלקמור, CA, שותף וראש תת-תחום סיכונים, אירופה, מזה"ת, הודו ואפריקה, EY

לאחר המשבר הכלכלי העולמי, סביבת הציות לרגולציה הפכה למורכבת יותר והקנסות גדלים ואף צפויים להמשיך ולגדול בעתיד. מאחר שכשלים בציות הם בעלי השפעה משמעותית על המיתוג ושווי השוק של ארגונים, ישנה חשיבות אסטרטגית עבור ההנהלה והדירקטוריון למנוע כשלים כאלה. בעוד שהיקף הציות ממשיך להתרחב, על ארגונים לנהל מערך מורכב ומשתנה תמידית של פעילויות ציות.

כאשר מדובר בקביעת היקף בחינת הציות של הביקורת הפנימית, אין תשובה אחת נכונה. ההיקף "הנכון" מושפע מבשלותן של הפונקציות הקיימות בארגון ויכולותיהן. ארגונים שאין בהם צוות ייעודי לנושא הציות, ירחיבו בסבירות גבוהה יותר את היקף פעילויות הציות של הביקורת הפנימית שלהם.

קימת סבירות גבוהה שיחידות ביקורת פנימית האחראיות להיבטי ציות ייקחו על עצמן פעילויות נוספות הקשורות לציות. על הביקורת הפנימית לשקול להבהיר במפורש במקרים אלה את היקף פעילויות הציות לבעלי עניין מרכזיים, לאמוד באופן מציאותי את כשירותה להעריך את דרישות הציות, ולהבהיר את הסיכונים או הפערים הקיימים בשל אילוצי משאבים או יכולות.

מבקרים פנימיים ראשיים צריכים לקרוא תיגר על המצב הקיים באמצעות בחינת השאלות הבאות:

- האם הביקורת הפנימית היא הפונקציה המתאימה לנושא סיכוני ציות ובקרות ציות?
- האם הביקורת הפנימית מתייחסת לסיכונים המתאימים הקשורים לציות?
- האם לרשות הביקורת הפנימית עומד הצוות המתאים לצורך התייחסות והוצאה לפועל של פעילויות ציות ביחס לרגולציה, כדוגמת החוק למניעת שחיתות ושוחד של עובדי ציבור זרים בארה"ב (U.S. Foreign Corrupt Practices Act), "הסטת רווחים ושחיקת בסיס המס" של ה-OECD, ופרטיות הנתונים (Data Privacy) של ה-E.U.?
- האם הביקורת הפנימית ממנפת באופן מיטבי את האמצעים הטכנולוגיים והאוטומטיזציה שעומדים לרשותה?

ישנה חשיבות רבה לכך שהביקורת הפנימית תתמקד בהפקת ערך מפעילויות הציות שהיא מבצעת. **ערך זה עשוי לכלול:**

- אינטגרציה, תקשורת, תכנון, ביצוע ודיווח משופרים בין פונקציות שונות בארגון.
- תובנות והתבוננות לעתיד, ולא רק התבוננות בדיעבד.
- קישור בין פעילויות הציות של הביקורת הפנימית לבין שיפורים בבקרות ותהליכים.
- הדגשת מגמות ואנומליות באמצעות ניתוח נתונים.
- שיתוף בלקחים שהופקו מהפרות של דרישות ציות.
- מעורבות בחזית של שינויים עסקיים מהותיים.
- סיוע להנהלה בציות לדרישות חדשות הנובעות משינויים ברגולציה או מחוקים חדשים.

יוזמות להפחתת עלויות של ישויות עסקיות וחוסר ודאות כלכלית עולמי, יוצרים לחץ גובר להפחתת העלות של דרישות הציות. ההנהלה מצפה שעלויות הציות יופחתו, אך מגלה "אפס סובלנות" לאי ציות. עליה להבין את ההשפעה של השינויים בשלבים מוקדמים של התהליך ולשאוף לכך שיהיו רשתות ביטחון לניהול כל שינוי או מעבר.

פונקציות ביקורת פנימית מתקדמות מעורבות באופן פעיל בדיון בעניין עלות הציות. הפעולות המקובלות לייעול כוללות עריכת הערכה מפורטת של פעילויות הציות והאופן שבו הן מוצאות לפועל, עריכת סקר סיכוני ציות, ומינוף האוטומטיזציה ושימוש בניתוח נתונים לצורך ביצוע בדיקות, ניתוח מגמות, איתור מוקדם של טעויות ובחינה בזמן אמת של ציות. באמצעות מינוף הידע של הביקורת הפנימית על הארגון, התהליכים והבקרות שלו, ניתן לסייע להנהלה בזיהוי סיכוני הציות הרלוונטיים וההזדמנויות לאוטומטיזציה ושיפור בתהליכים ובקרות שישדרגו את ביצועי העסק במקביל לשיפור האפקטיביות של הציות.

דרישותיהם הגוברות של בעלי העניין

קריסטין אונג, CIA, CRMA, FCA Aust, מנהלת בכירה, ביקורת פנימית, IGB Corp. Berhad

ה פרופיל של מקצוע הביקורת הפנימית עלה באופן משמעותי בשנים האחרונות הודות למאמצים בלתי נלאים ולמקצועיות שמגלים מבקרים פנימיים ברחבי העולם. בעלי עניין נעזרים במבקרים פנימיים בתחומים של ממשל תאגידי, ניהול סיכונים ובקרות. עם ההכרה הגוברת במקצוע, גם הציפיות של בעלי העניין התגברו.

רגולטורים מכירים במבקרים הפנימיים כאחד מעמודי התווך של ממשל תאגידי. ככל שהרגולטורים הפכו לאקטיביים יותר בפרסום חקיקה, קודים אתיים ודרישות סף למסחר על מנת להסדיר את סביבת העבודה הדינמית, כך הם מצפים ממבקרים פנימיים להתעדכן בהוראות החדשות ולייעץ ללקוחותיהם בהתאם. הרגולטורים גם מבקשים לקבל הערות והצעות מהמקצוע על מנת לקבל נקודת מבט שונה ביחס להשפעה של הרגולציה. במובן זה, על ה-IIA וחבריו להיות בחזית התפתחויות אלו ולהוות את קול המקצוע.

ככל שארגונים מאמצים טכנולוגיות משתנות תמידית, כך ההנהלה מצפה ממבקרים פנימיים לגלות בקיאות בבקרות של מערכות מידע ובסוגיות של אבטחת מידע, וכן להיות בקיאים במערכות מידע ברמה סבירה. מלבד ביקורות של מערכות מידע, ההנהלה מצפה ממבקרים פנימיים לספק ייעוץ בנושא הטמעת מערכות, בקרות שינויים ותכניות להמשכיות עסקית. כמו כן, ההנהלה מצפה ממבקרים פנימיים להשתמש בכלים של מערכות מידע על מנת לייעל ולהגביר את האפקטיביות של הביקורות. בעידן של נתוני עתק ("big data") וניתוח נתונים, ייתכן שדיווח על חריגים על בסיס בדיקה מדגמית עומד להיעלם מן העולם. אם אותר כשל בבקרה, ההנהלה מצפה להתעדכן במלוא ההיקף של ההשפעה או האובדן.

ארגונים ועסקים ממשיכים לגדול, לעתים באופן אורגני, אך לרוב באמצעות מיזמים חדשים או מיזוגים ורכישות. מבקרים פנימיים צריכים להישאר מעודכנים בכיוון האסטרטגי של ההנהלה ולצייד את עצמם בידע ממגוון תעשיות. כאשר לקוחות מבקשים להיוועץ בהם, המבקרים הפנימיים חייבים להיות מוכנים לבחון עסקים חדשים ולהבין את העסקים של הארגון ואת האסטרטגיה שלהם. הידע של המבקרים צריך להתפרש מעבר לעסק הנוכחי שבו מעורב הארגון, ועליהם להרחיב את מעגל הקשרים שלהם מחוץ לתחום העיסוק. אם המבקרים שואפים להיות חלק מהשדרה הניהולית, עליהם להרוויח את המעמד הזה.

הציפייה ממבקרים פנימיים היא להגדיל ולשמר את הערך של הארגון. על אף שיש למבקרים תובנות ביחס לפעילות של הארגונים המאפשרות להם להשיג מטרה זו, בעלי העניין הרחיבו את תחומי המיקוד שלהם מעבר לממשל תאגידי, סיכונים ובקרות, וכעת הם כוללים גם תחומי סביבה, בטיחות וקיימות. המבקרים צריכים ליישם את הידע שלהם בתחומים חדשים ולהרחיב אותו כך שיכלול פעילויות חדשניות, מובילות לשינוי וברות קיימא.

על מנת להמשיך לשרת בעלי עניין באופן אפקטיבי, מבקרים פנימיים צריכים להכין את עצמם לעתיד באמצעות יצירתיות, חדשניות וצימאון לידע. בנוסף, עליהם לייצר בסיס איתן באמצעות סמכות ופיתוח מקצועי. מאחר שהצורך בלמידה אינו פוסק והציפיות של בעלי העניין ממשיכות לגדול, מבקרים פנימיים חייבים להתייצב בפני האתגר - אין להם ברירה אחרת.

סיכון הטכנולוגיה הופך למורכב יותר

צ'רלי ורייט, CIA, CPA, CISA, סגן נשיא, ביקורת פנימית, Devon Energy Corp.

מ בקרים פנימיים ניצבים בפני סביבה טכנולוגית שהולכת ונהיית מורכבת יותר. דירקטוריונים וועדות ביקורת מכירים בכך שהעתיד כבר כאן, ומעסיקים את עצמם רבות בסיכון הטכנולוגיה. נושאים הנעים בין טכנולוגיית מובייל ואבטחת מידע למחשוב ענן ומדפסות תלת-ממד הופכים לנושאים אסטרטגיים לדיון ברמת הדירקטוריון. זה מבליט את העובדה שפונקציית הביקורת הפנימית צריכה להתפתח ולהגביר את יכולותיה בהיבט הביקורת הטכנולוגית.

מבקרים מנוסים בעלי הכשרה ראויה יכולים להבטיח שהטמעת פרויקטים של מערכות מידע תבוסס על מתודולוגיות איתנות של ניהול פרויקטים ותהליכי שינוי ארגוני. יש להם תפקיד קריטי בהערכה ובבדיקה של בקרות פנימיות חדשות, לרבות גישה פיזית ולוגית לאפליקציות חדשות. מבקרים יכולים גם לזהות סוגיות ופערים המונעים ניצול מלא של טכנולוגיות חדשות. ניצול חלקי של טכנולוגיות חדשות הוא בעיה נפוצה שמובילה לתפעול לא יעיל ולחריגות תקציביות.

בעוד העסקים אחראים לאסטרטגיה הכוללת וליישום של שילוב כלים מורכבים בעלי סיכון גבוה, מבקרים פנימיים יכולים להציג נקודת מבט חדשה ועצמאית ביחס להיבטים הטקטיים של שילוב אמצעים אלו. למשל, במסגרת הטמעת מערכת פיננסית חדשה, מבקרים פנימיים יכולים לסייע לבחון את תקינותן של בקרות מרכזיות ולוודא כי בקרות אלו מספיקות לצורך שמירה על המהימנות של המערכת החדשה. קיימות דרכים רבות שבהן מבקרים פנימיים יכולים להגיב לאתגר הטכנולוגי, ובראשן הכשרה. החל מקריאת מאמרים טכנולוגיים עדכניים, דרך השגת הסמכות מקצועיות, וכלה בהשתתפות בכנסים וסמינרים. כך יכולים מבקרים פנימיים לשפר את הכישורים הטכנולוגיים שלהם ולהיות ערוכים בצורה טובה יותר לשרת את לקוחותיהם.

מלבד הכשרת עובדים קיימים, על הנהלת הביקורת הפנימית לגייס עובדים בעלי ניסיון עבודה והשכלה בתחום מערכות המידע, שניתן להכשירם לעריכת ביקורות שיעניקו ערך מוסף לארגון. באמצעות מינוף מומחיותם של עובדים בעלי עבר בתחום מערכות המידע, הביקורת הפנימית יכולה לגבש תובנות מעמיקות יותר ביחס לבקרות, לסיכונים ולתהליכים הרלוונטיים. לחלופין, הנהלת הביקורת הפנימית יכולה ליצור תכניות פיתוח שבמסגרתן ישתתפו עובדי הביקורת, כל אחד בתורו, בפרויקטים בעלי זיקה טכנולוגית. כאשר יהיו בעלי תפקידים בביקורת הפנימית, יוכלו המבקרים החדשים ליישם את הכישורים שלמדו ברוטציה זו. בביקורות המצריכות סוג מסוים של מומחיות טכנולוגית, ההנהלה יכולה גם להסתייע במבקרים אורחים.

עבור ביקורת ספציפית, אם לא קיימים העובדים המתאימים במסגרת האירגון על פונקציות של ביקורת פנימית לצרף משאבים חיצוניים בעלי היכולות הטכנולוגיות הנדרשות. אמנם צירופו של צד שלישי עלול להיות יקר, אך פונקציות של ביקורת מחויבות להבטיח שמשאבים בעלי הכשרה ראויה יהיו זמינים להן לצורך ביצוע העבודה הטכנית המורכבת ביותר.

ככל שקצב השינוי גובר, כך מבקרים יכולים לצפות למספר עולה של סיכונים טכנולוגיים בארגונים שלהם. דירקטוריונים וועדות ביקורת מבקשים להבטיח שהערכה, ניהול ומעקב ראוי אחר סיכונים אלה מתבצעים באופן נאות. תפקידה של הביקורת הפנימית הוא לספק להם את הביטחון הזה.

הכשרת מבקרי 2020

קארל ארהארט, CPA, סגן נשיא ומבקר ראשי, MetLife

אצלנו ב-MetLife, אנו מכשירים את המבקרים שלנו להפוך ל"מבקרי 2020". אנו מכירים בכך שעל מנת להישאר בקצב של הציפיות המתפתחות של בעלי העניין, עלינו לפתח ולקדם באופן מתמשך את הכישורים ואת ההתנסויות שלנו.

המתכון להצלחה הוא הסטה, ו"הרוטב הסודי" החדש הוא האופן שבו מבקרים פנימיים ממנפים נתונים ומפתחים את השימוש שלהם בניתוח נתונים. יתר הרכיבים חשובים גם הם, לרבות שילוב של חוש עסקי, מומחיות ספציפית, וידע כללי עם הכישורים הרכים של המבקר הפנימי. היעד של MetLife הוא להכשיר את המבקרים היום על מנת להקנות להם את הכישורים וההתנסויות שהם יצטרכו לספק באופן אפקטיבי בביקורות פנימיות בשנת 2020.

מדוע נתונים וניתוח נתונים הם כה חשובים? ידוע כי קצב ייצור הנתונים גדל בשיעור עצום. בשנת 2020 תופק כמות גדולה יותר של נתונים מאשר בכל המאה הקודמת לה. בידיעה זו, מבקרים פנימיים יכולים לדמיין את הציפיות והאתגרים העצומים שעמם יצטרכו להתמודד.

מאחר שמקצוע הביקורת הפנימית מבקש למקסם את השימוש שלו בנתונים, על פונקציות של ביקורת לשים דגש על הכשרת מבקרים לשימוש בנתונים וניתוח נתונים. מבקרים צריכים לחזק את הכישורים הבסיסיים שלהם, לדעת כיצד להגביר את השימוש היומיומי שלהם בנתונים, וכן לדעת מתי יש להסתייע במומחים חיצוניים. התועלת האולטימטיבית של ניתוח נתונים מתקדם היא לסייע למבקרים להתעלות על ציפיות המחר של בעלי העניין. בשנת 2020 זו תהיה הדרך הטובה ביותר להשיג את היעד של הביקורת הפנימית: להגביר ולשמר את הערך של הארגון באמצעות מתן ביטחון, תובנות וייעוץ אובייקטיביים ומבוססי סיכון. העיקרון של "מבקרי 2020" אינו מתמקד רק בנתונים וניתוחם. הוא נוגע גם לפיתוח הכישורים וההתנסויות של מבקרים פנימיים. זו הסיבה שמחלקת הביקורת של MetLife רִעננה את יכולותיה בתקופה האחרונה תוך מחשבה על ההווה ועל העתיד. היכולות החדשות שלנו כוללות ידע עסקי משולב, דפוס חשיבה של ממשל תאגידי, סיכונים ובקרות, חשיבה אנליטית וביקורתית, תקשורת פשוטה, אפקטיבית ושקופה, עבודת צוות וזריזות עבודה. התאמת מסלולי למידה פרטניים ששמים דגש על נתונים, ניתוח נתונים וחשיבה ביקורתית היא חלק משמעותי מההכשרה לעתיד.

ישנו ביקוש גבוה לכישרונות בתחום הביקורת. הארגונים המכשירים את עובדיהם תוך חשיבה על עקרון "מבקרי 2020" יהיו בעמדה הטובה ביותר לשמר את הכישרונות של היום, וחשוב מכך - למשוך את הכישרונות של מחר.

This article was reprinted with permission from the February 2016 issue of Internal Auditor magazine, published by The Institute of Internal Auditors, Inc., www.theiia.org. and has been translated from English to Hebrew."

מטוב למעולה | תכנון אסטרטגי יכול להגדיר את פונקציית הביקורת הפנימית

מאת **ריצרד צ'ימברס** CRMA, CCSA, CGAP, QIAL, CIA

המאמר הוא תרגום מהבלוג Chambers on the profession מאוגוסט 2014. בבלוג זה משתף מר צ'יימברס, נשיא ומנכ"ל לשכת המבקרים הפנימיים העולמית IIA , בדעותיו ובתובנותיו, המבוססות על 40 שנות ניסיון במקצוע הביקורת הפנימית.

אם נשווה בין פונקציות של ביקורת פנימית, סביר להניח שנמצא לא מעט הבדלים ביניהן. מחלקות בעלות ביצועים גבוהים נבדלות בדפוס החשיבה שלהן ובגישה שלהן לעבודתן. הן מכירות בחשיבות של מתן ערך מוסף, והן נתפסות על ידי בעלי העניין כמשאב חיוני. הן עושות שימוש בפלטפורמות לניהול ידע ובכלים אוטומטיים וכן מספקות לעובדים שלהן הכשרה שונה. עם זאת, ישנו מאפיין אחד שמייחד את פונקציות הביקורת הפנימית הטובות ביותר: מחויבות לתכנון אסטרטגי מקיף.

> מחלקות הביקורת הפנימית הטובות ביותר מבינות כי שני סוגי התכנון הם הכרחיים: "תכנית שנתית מבוססת סיכון תנחה את הביקורת הפנימית לאורך השנה, בעוד שתכנית אסטרטגית תתווה את הדרך מעבר לעתיד הנראה לעין"

אין הכוונה לכך שמחלקות ביקורת פנימית אינן מתכננות את הפעילות שלהן. כיום, כמעט כולן יוצרות תכנית מבוססת סיכון על בסיס שנתי, ומעדכנות אותה במהלך השנה בהתבסס על אינפורמציה חדשה. עם זאת, באופן מפתיע, מעט מאוד מחלקות של ביקורת פנימית משלבות תכנון אסטרטגי מקיף בפעילות שלהן.

מחלקות הביקורת הפנימית הטובות ביותר מבינות כי שני סוגי התכנון הם הכרחיים: כפי שציינתי ברשת החברתית "טוויטר" לאחרונה: "תכנית שנתית מבוססת סיכון תנחה את הביקורת הפנימית לאורך השנה, בעוד שתכנית אסטרטגית תתווה את הדרך מעבר לעתיד הנראה לעין".

תכנון אסטרטגי מהווה עבור הביקורת הפנימית דרך מצוינת לזיהוי, ייצור ואומדן של הערך שעליה לספק לבעלי העניין

תכנון אסטרטגי מהווה עבור הביקורת הפנימית דרך מצוינת לזיהוי, ייצור ואומדן של הערך שעליה לספק לבעלי העניין. אני מאמין כי נקיטת גישה שיטתית ומוסדרת, כדוגמת הליך שבעת השלבים הכלול בהנחיות המקצועיות של ה-IIA, תסייע להבטיח שהביקורת הפנימית תתקדם בכיוון הנכון. השלבים הם כדלקמן:

1. הבנת התחומים הרלוונטיים והמטרות של הארגון.
2. לקיחה בחשבון של מסגרת הכללים המקצועיים הבינלאומיים של ה-IIA.
3. הבנת ציפיות בעלי העניין.
4. עדכון החזון והמטרה של הביקורת הפנימית.
5. הגדרת הפרמטרים הקריטיים להצלחה.
6. עריכת ניתוח SWOT (חוזקות, חולשות, הזדמנויות ואיומים).
7. זיהוי יוזמות מרכזיות.

קל להגדיר את השלבים שיש לכלול בתכנית אסטרטגית, אך קשה יותר להבטיח תוצאות חיוביות. למרבה המזל, תכנון אסטרטגי מוצלח בדרך כלל אינו עניין של מזל. כמו פעילויות רבות של ביקורת פנימית, התכניות האסטרטגיות הטובות ביותר הן אלו המופקות באמצעות עבודה קשה ומחויבות עיקשת להצלחה על ידי כל הגורמים בארגון.

חשוב מאוד לגשת לכל שלב בתהליך בקפדנות רבה. כדי "להבין את מטרותיו של הארגון" למשל, לא די בהשגת העתק של מסמך המטרות העדכני ביותר של הארגון. נדרש גם להבין את המטרות הלא-כתובות שלו, כמו גם את התכנית האסטרטגית, התקציב, הטכנולוגיות ונכסים אחרים. בתכנון אסטרטגי מקיף של הביקורת הפנימית, כל השלבים בתהליך הם חשובים, אך אולי החשוב מכל הוא האופן שבו התכנון מתיישר עם היעדים הכוללים של הארגון. הרבה מהניתוח המבוצע במסגרת התכנון האסטרטגי נועד לצורך סיוע בפיתוח יעדים בני השגה המשקפים את המציאות העסקית.

על מנת שיהיה יעיל, תהליך התכנון האסטרטגי צריך להתפרש מעבר לפיתוח של סדרי עדיפויות ויעדים ברמה גבוהה. זאת משום שכדי ליישם את התכנית באופן אפקטיבי, יעדים אלה צריכים להיות מתורגמים למדיניות או לתכניות מפורטות המובנות ומיושמות על ידי פונקציית הביקורת הפנימית.

ראייה ברורה יותר של העתיד היא נקודת הפתיחה לשינוי חיובי. לא רק שעלינו לפתח ראייה אסטרטגית לעתיד, עלינו גם לסייע בקביעת מסגרת ותרבות להמרת הראייה לעתיד לכדי פעולות.

כפי שאמרתי, תכנון אסטרטגי אפקטיבי אינו פשוט. לצורך כך נדרשת השקעה משמעותית של זמן ומשאבים. אך אני מאמין כי פיתוח של תכנית אסטרטגית פורמלית וכתובה היא חיונית לצורך פיתוח פונקציית ביקורת פנימית אפקטיבית לחלוטין. הדבר מהווה גם חותמת איכות של מחלקות מובילות של ביקורת פנימית, מאחר שתכניות אסטרטגיות מקיפות יכולות לשמש כתכנית לשיפור משמעותי.

אם טרם שילבתם תכנון אסטרטגי בפעילות התכנון הכללית שלכם, תשקלו לבחון את ההנחיות לפיתוח תכנית אסטרטגית של ה- IIA, The IIA Practice Guide: developing the Internal Audit Strategies). זהו חלק חשוב מהקווים המנחים המומלצים על ידי ה-IIA, והוא זמין ללא תשלום לחברי ה-IIA.

This article was reprinted with permission from the February 2016 issue of Internal Auditor magazine, published by The Institute of Internal Auditors, Inc., www.theiia.org. and has been translated from English to Hebrew."

ההנחיות שלא קראתי

מאת **כפיר מנור**, רו"ח

מדוע עובדים אינם נענים להנחיות הארגון ומה ההשלכות לכך

אגונים רבים מחויבים להגדיר הנחיות בתחומים שונים לעובדים הנובעות בעיקר מדרישות של גופי רגולציה שונים.

הנחיות אלו נוגעות הן לפן האתי-התנהגותי של העובדים והן לפן המקצועי (בטיחות למשל). כחלק מתהליך ה-SOX, אנו נדרשים לבדוק האם קיים תהליך סטנדרטי לנושא הנסקר. סטנדרטיזציה היא סיבה נוספת להגדיר נהלים והנחיות בארגון.

קיימות סיבות נוספות (לבד מהרגולציה) להגדרת נהלים בארגון, כגון יעילות וסטנדרטיזציה, המשכיות עסקית, בקרה תהליכית (סיכון למעילות/גניבות), יכולת של ההנהלה לבצע שינויים, מערך הדרכות אפקטיבי, שימור ידע וכדומה.

עם זאת, אנו עדים למצבים רבים שבהם עובדים אינם מקיימים נהלים, למרות הסיכון הטמון באי עמידה בהם

הסיבות לאי ציות לנהלים

כאשר מנתחים את הסיבות לאי היענות לנהלים בארגון, ניתן להצביע על העיקריות בהן (הסיבות יוסברו בלשון יחיד אך הן רלוונטיות לעובדים ולנהלים רבים):

חוסר הכרה של הנוהל או הדרישה - העובד כלל אינו מודע לנוהל - לא עבר הדרכה מסודרת, הנוהל לא הובא לידיעתו כשהתקבל לעבודה או כשאושר, לא הוענקה לו הרשאה לצפות בנוהל במערכות הארגון וכו'. לעתים ההדרכה אינה מעודכנת או תואמת להנחיות ולעתים מתודולוגיית ההדרכה אינה מותאמת לאוכלוסייה המודרכת. כך נוצר מצב שבו הארגון אמנם משקיע בפיתוח מערך הדרכה ותקשורת לעובדים, אך בסופו של יום העובד אינו מודע לנוהל.

חוסר הבנה של הנוהל - הנוהל לא הוסבר לעובד בשפתו או במונחים ברורים לו (הנוהל נכתב בשפה שאינה שפת האם של העובד, הנוהל נכתב בשפה משפטית, וכו'). אנו עדים לכך גם בבואנו לקרוא חוזה אחיד של גופים גדולים (בנקים, חברות תקשורת וכו'). בחוזים כאלה הניסוח מובא באופן משפטי שלרובנו קשה להבינו מבחינה מהותית.

העדר דוגמה אישית - המנהל אינו מקיים את הנוהל, ומכאן מסיק העובד כי אין חובת קיום של הנוהל (מכונה באנגלית - tone at the top).

הגדרת אחריות לא ברורה - העובד חושב שהנוהל לא תופס לגביו (הנוהל אינו מגדיר מי אחראי על מה, לא ברור מהו חלקו של העובד ביישום הנוהל). לעתים הנוהל מגדיר אחריות צוותית, אולם בתוך הצוות אין חלוקת אחריות לעובד. ומכאן שלעתים גם הגדרת אחריות לפי פונקציות אינה מספקת (אם מונו מספר עובדים לאותו תפקיד, לדוגמה: מנה"ח, מחסנאי וכו').

העדר אכיפה - העובד מודע לכך שאי קיום הנוהל לא ייאכף. מאפיין זה ניכר יותר כאשר ההנחיות אינן בנות אכיפה כלל (בחלק מהמקרים הן הוגדרו כדי לצאת ליד חובה). מניסיוני הצבאי אני זוכר כי נאמר לנו בהכשרות הפיקודיות כי מפקד איכותי הוא מפקד שהנחיותיו נעשות ללא נוכחותו (כפי שאנו נוהגים לומר: רוח המפקד). המעביד אינו יכול לאכוף ולנטר כל הנחיה, שהרי תהיה לכך עלות עצומה. לכן, אם עובד אינו מקפיד על נהלים מאחר שהוא יודע שלא ייאכפו, המעביד צריך לבחון כיצד להגביר את היענות העובדים מטעמים הקשורים למוטיבציה/הזדהות/הבנה, ופחות מתוך סמכות.

ההנחיות ארוכות או מפורטות מדי - העובד אינו יכול להפנים מידע כה רב (כמו שאומרים: מרוב עצים לא רואים את היער). יש נהלים בפורמט טכני שעונים על דרישות ה-QA, אך אינם מכילים תצורה המאפשרת למידה. במקרים אלה יוצרים בארגון מערך הדרכה לנהלים באופן נפרד. במקרים רבים, מערך ההדרכה אינו מעודכן או אינו תואם את דרישות הנוהל (בגלל הכפילות). כאשר אנחנו מפיצים נוהל הכולל תהליכים רבים לגורמים רבים, העובד הבודד אינו מאתר את החלק הרלוונטי אליו, וכך הנוהל מאבד מהאפקטיביות שלו.

שינויים תכופים - כאשר הנהלים משתנים לעתים תכופות, העובד אינו יכול לעקוב אחר קצב השינויים ומבצע את ההנחיות שאליהן הוא רגיל.

בשנה שעברה דווחו בישראל **54**
מקרים של מוות כתוצאה מתאונות עבודה.

ענף הבנייה מוביל עם
למעלה מ-30 מקרים

למרות קיומן של הנחיות מפורטות בכל
הנוגע לבטיחות העובדים, בחלק מן המקרים
ההנחיות לא בוצעו על ידי העובדים

השלכות חוסר הציות

בשנה שעברה דווחו בישראל 54 מקרים של מוות כתוצאה מתאונות עבודה. מספר זה אינו גבוה ביחס לאוכלוסייה, אך כאשר מנתחים את הענפים שבהם התרחשו האסונות, נמצא כי ענף הבנייה מוביל עם למעלה מ-30 מקרים. במקרה זה הסטטיסטיקה כבר מציבה את ישראל במקום גבוה (ברמת הענף). מניתוח מקרים אלה אנו רואים כי רובם מתייחסים לתאונות של עובדים זרים. קצב הגידול של תאונות עובדים זרים עלה ב-12% לשנה. נתון מדאיג בפני עצמו.

למרות קיומן של הנחיות מפורטות בכל הנוגע לבטיחות העובדים, בחלק מן המקרים ההנחיות לא בוצעו על ידי העובדים.

נתון מדאיג נוסף שדווח על ידי משרד הבריאות הוא שבישראל כ-5,000 חולים מתים מדי שנה מזיהומים. מעיון בניתוח הסיבות המרכזיות לכך, ניתן להבחין באי שמירה על היגיינה של הצוות הרפואי (לדוגמה, שטיפת ידיים לפני הטיפול).

ברור כי טובת החולה היא הראשונה במעלה לכל רופא. לפיכך נראה תמוה מדוע חולים רבים כל כך נפגעים מזיהומים כתוצאה ישירה מהצוות המטפל. אולם אם מנתחים את הסיבות לכך, אפשר לראות כי חלק מהרופאים טוענים כי אין באפשרותם לשטוף את הידיים בתדירות הנדרשת, לאור הכמות הרבה של החולים שבהם הם צריכים לטפל.

לאי ציות לנוהלי הארגון או למדיניות הארגון, בין אם הוא נגזרת של חוק או תקנה ובין אם הוא חלק מהקוד האתי הארגוני, יש השלכות מרחיקות לכת על הארגון בכלל ועל החברה (הלקוח/העובד/הספק) בפרט. אי ציות יכול לגרום לפגיעה חמורה במוניטין הארגון, ויכולות להיות לכך השלכות כלכליות משמעותיות (אם באמצעות פרסום שלילי, תביעה משפטית, ירידה במחיר המניה וכו').

בנוסף, אי ציות ארגוני הוא מדד בסיסי ליכולת ההנהלה לנהל את הארגון, ליישם החלטות, לנתח שינויים ועוד. אם הארגון מעוניין לבצע שינויים במבנה האחזקות (למשל, גיוס הון/הנפקה/הוספת שותפים), אחד המדדים החיוניים שהארגון יימדד בהם הוא הציות הארגוני. כאשר יובן כי לארגון אין את היכולת לאכוף את ההנחיות, תהיה לכך השפעה על קבלת ההחלטה של המשקיע לקדם את העסקה.

פתרונות לשיפור מידת הציות

אם כן, מהם הפתרונות שניתן להציע כדי לאפשר לעובדים לעמוד בנוהלי הארגון?

"נוהל צריך להיות פרקטי, ברור, מתאים לשפתו של העובד"

"גזרו גזירה שווה בין עובדים ומנהלים לגבי האכיפה. נאה דורש - נאה מקיים"

- נוהל צריך להיות פרקטי, ברור, מתאים לשפתו של העובד (לרבות שפה מקצועית). ניתן לבחון האם הנוהל ברור באמצעות שיתוף של העובדים בכתיבתו, עריכת פיילוט, מבחן וכו'.
- בצעו ניטור לגבי העובדים שהשתתפו בהדרכה לנוהל, וחייבו את כלל העובדים להשתתף בהדרכה.
- גזרו גזירה שווה בין עובדים ומנהלים לגבי האכיפה. נאה דורש - נאה מקיים. אגב, ישנם ארגונים המפרסמים לכלל העובדים סטטיסטיקה (ללא שמות) של מחלקות שלא עמדו בנוהלי הארגון.
- בדקו את אפקטיביות ההדרכות של הארגון. אם ההדרכות ב-WEB או ב-E-LEARNING אינן אפקטיביות, שקלו הדרכות פרונטליות. ניתן להפריד במתודולוגיית ההדרכה לפי מחלקה/סיכון. כלומר, במחלקות שבהן הסיכון רב יותר, שקלו לבצע הדרכות פרונטליות בתדירות גבוהה יותר.
- הרתעה יכולה לסייע רק אם היא מותאמת לארגון. הרתעה משתמעת (בעלת פן ענישה/אכיפה רחב יותר) אפקטיבית הרבה יותר מהרתעה ספציפית. כאשר מיישמים מודל של הרתעה ספציפית, העובד מבצע שיקול של עלות מול תועלת. לדוגמה: איחור של שעה לעבודה - יגרור קיזוז של שעת עבודה. במקרה של הרתעה משתמעת, ארגון יכול לציין כי איחור של עובד יכול לגרום לעיכוב בתוספת שכר, לירידה בציון ההערכה השנתית, לקיזוז בונוס וכו'. גם אם ההתרעה אינה מיושמת במלואה, מחקרים מוכיחים כי החשש ל"קנס" גבוה עדיין אפקטיבי יותר מקנס ספציפי/קבוע.

נקודה למחשבה...

תחום הציות (COMPLIANCE), או כפי שישראלים רבים קוראים לו - "היענות להנחיות", נחקרי במגוון אספקטים, לא רק בהיבט של ציות עובדים לנהלים. אחת הבעיות המרכזיות ביישום של תכנית ציות (COMPLIANCE PROGRAM) היא שהארגון מנסה לכסות 100% מהמקרים באמצעות סטנדרט אחד. הבעיה העיקרית היא שהארגון מתעלם מעיקרון שנקרא לו - 1:98:1.

העיקרון קובע כי ישנו אחוז מסוים של אנשים שבכל מקרה ימלאו אחר הדרישות (גם אם אין נוהל כתוב, אין אכיפה, אין ענישה וכו'). אחוז אחד של האנשים לעולם לא יקיים את ההוראות (גם אם הענישה תהיה לא מידתית).

יתר האנשים (98%) יקיימו או לא יקיימו את ההוראות בנסיבות מסוימות. הנסיבות תלויות ברמת הבקרה, ברמת האכיפה, ברמת החניכה/ההדרכה, בהזדהות עם הארגון וכו'.

כאשר הארגון מנסה להגדיר הנחיות שיכסו את האחוז שבכל מקרה לא ימלא את ההוראות, הוא יוצר תהליך בירוקרטי (במובן הרע של המילה) מסורבל. תסכול של יתר ה-99%, יפגע ביכולת לנטר את התהליכים המרכזיים (מאחר שיש יותר מידי בקרות) וכו'. בכך תהליך ההיענות לנהלים הופך ללא ישים. בבואנו להמליץ על תהליך מבוקר יותר ויעיל יותר, כדאי שנסב את תשומת לבנו להשלכות של יישום התהליך בארגון.

IIA ישראל
איגוד מבקרים פנימיים בישראל
Institute of Internal Auditors in Israel

קורס QAR הבטחת איכות

הקורס מיועד למבקרים פנימיים | דירקטורים | מנהלים | רואי חשבון הנותנים שרותי ביקורת פנימית.

תאריכים

שלישי | **3 ינואר 2017**
רביעי | **4 ינואר 2017**

שעות

הקורס ייערך כל יום בין השעות
08:30 בבוקר עד **15:30** אחה"צ

מיקום

אודיטוריום תמר
בית לשכת רואי חשבון
רח' מונטפיורי 1, תל-אביב

מרצה

מר מיכאל פוצ'ילי חבר דירקטוריון IIA צפון אמריקה והמבקר הפנימי של רשות התחבורה המטרופוליטני של ניו-יורק יערוך קורס הבטחת איכות QAR. מר מיכאל פוצ'ילי מלמד ומכין מועמדים לבחינות ה-CIA. למיכאל מעל 30 שנה של ניסיון בביקורת פנימית בשירות הציבורי ובשוק הפרטי.

עלות

עלות לחברי **IIA** ישראל איגוד מבקרים פנימיים בישראל	**2600 ₪**
עלות לחברי לשכת רואי חשבון	**2800 ₪**
עלות לחברי לשכות אחיות (לשכת עורכי הדין, **ISACA** ישראל, איגוד מבקרי רשויות מקומיות)	**3100 ₪**
עלות לאחרים	**3500 ₪**

פרטים נוספים

- הקורס ייערך בשפה האנגלית.
- המחיר כולל:
  - השתתפות בקורס
  - ספרות מקורית (באנגלית) של ה-IIA בשווי של כ- 2000 ₪
  - כיבוד קל וארוחת צהריים קלה

בתקן 1310 של לשכת המבקרים הפנימיים העולמית ה-IIA נקבע, כי יש לבצע סקר הבטחת איכות של מערך הביקורת הפנימית, לא רק על ידי המבקר הפנימי עצמו, אלא בנוסף, אחת לתקופה, גם על ידי גורם חיצוני.

תקן 1321 של לשכת המבקרים הפנימיים העולמית ה-IIA אף מחמיר וקובע הסתייגויות בעת שימוש במילים "נערך בהתאם לתקנים המקצועיים הבינלאומיים למקצוע הביקורת הפנימית" כי: "המבקר הפנימי הראשי יכול לציין, שהביקורת הפנימית עומדת בתקנים הבינלאומיים למקצוע הביקורת הפנימית, רק אם תוצאות התוכנית להבטחת איכות ושיפור תומכות בהצהרה זו." נקודה זו חשובה, כי רבים מעמיתנו מדווחים על עמידה בתקנים מקצועיים בינלאומיים מבלי שערכו סקר הבטחת איכות, שהוא תנאי לשימוש בהצהרה זו. גם בארץ זיהו ואימצו רגולטורים את הצורך בהבטחת איכות מערך הביקורת הפנימית.

מטרת הקורס היא ליתן כלים להתכונן לקראת סקר הבטחת איכות כמבוקרים או כמבקרים.

- להכיר ולהתנסות ביישום תקנים בינלאומיים הנדרשים במסגרת ביקורת להבטחת איכות של מערך הביקורת הפנימית, תוך שימוש ב- IPPF - התקנים הבינלאומיים.
- להשיג את הידע שישמש לביצוע או היערכות לקראת תהליך הערכה עצמית תקופתית או ביקורת חיצונית להבטחת איכות מערך הביקורת הפנימית.
- הכרת הכלים והטכניקות המקובלים המשמשים לצורך הבטחת איכות.
- לבחון את הגישות המומלצות לביצוע ביקורת חיצונית להבטחת איכות, תוך סיוע לארגון בבחירת הגישה המתאימה לפעילותו.
- קבלת תעודת גמר קורס סוקר הבטחת איכות המהווה תנאי לביצוע סקרי איכות.

מסיימי הקורס יצורפו (בכפוף להסכמתם) למאגר מבצעי סקרי האיכות ממנו נבחרים מועמדים לביצוע הסקרים.

משתתפי הקורס ייהנו מהנחה בת 25% מעלות הרישום לכנס השנתי ב- 5.1.2017.

כיצד מבקרים בענן

אופיר זילביגר, CISSP, CRISC
גלעד ירון, Certified STAR auditor, Compliance leader - CSA Israel

מטרת המאמר

מאמר זה סוקר את מושגי היסוד של עולם מחשוב הענן, המודלים והמאפיינים השונים של שירותי מחשוב הענן, הסיכונים בעולם זה, תפקידו של המבקר הפנימי בתחום וגישה מומלצת לביצוע ביקורות בנושא זה.

מה זה מִחשוב ענן

אנחנו פותחים את הברז, מדליקים את האור, מפעילים את הקומקום החשמלי ושותים קפה. כל זאת ללא צורך לשאוב את המים מן הבאר ולהחזיק תחנת כוח לייצור חשמל בחצר האחורית שלנו.

ארגונים מודרניים נדרשים ליותר ויותר יכולות מחשוב על מנת לפעול ולספק את שירותיהם. עד לפני שנים אחדות, שימוש משמעותי בשירותי מחשוב הצריך החזקה של חדר שרתים, חומרה, תוכנה ומערכות הפעלה, תשתיות תקשורת ומומחים לתחזוקה של כל הרכיבים האלה.

משאבי המחשוב בענן נצרכים ממש כמו המים והחשמל. אנחנו צורכים את כמות המים שאנו צריכים, בזמן שמתאים לנו ומשלמים עבור הכמות שצרכנו בלבד.

בהינתן שירותים אלה, יכול כל ארגון להתמקד במטרותיו ולהתייחס לשירותי המחשוב כעוד הוצאה שוטפת הנדרשת לקיומו.

ארגון התקנים האמריקאי NIST, מגדיר מחשוב ענן כמודל המאפשר גישה קלה ונוחה, על פי הצורך, למאגר משאבי מחשוב (למשל: רשת, שרתים, אחסון, אפליקציות, שירותים) שאותם ניתן לצרוך או לשחרר בכל עת, במאמץ ניהולי מזערי או מעורבות מזערית של ספק השירות.

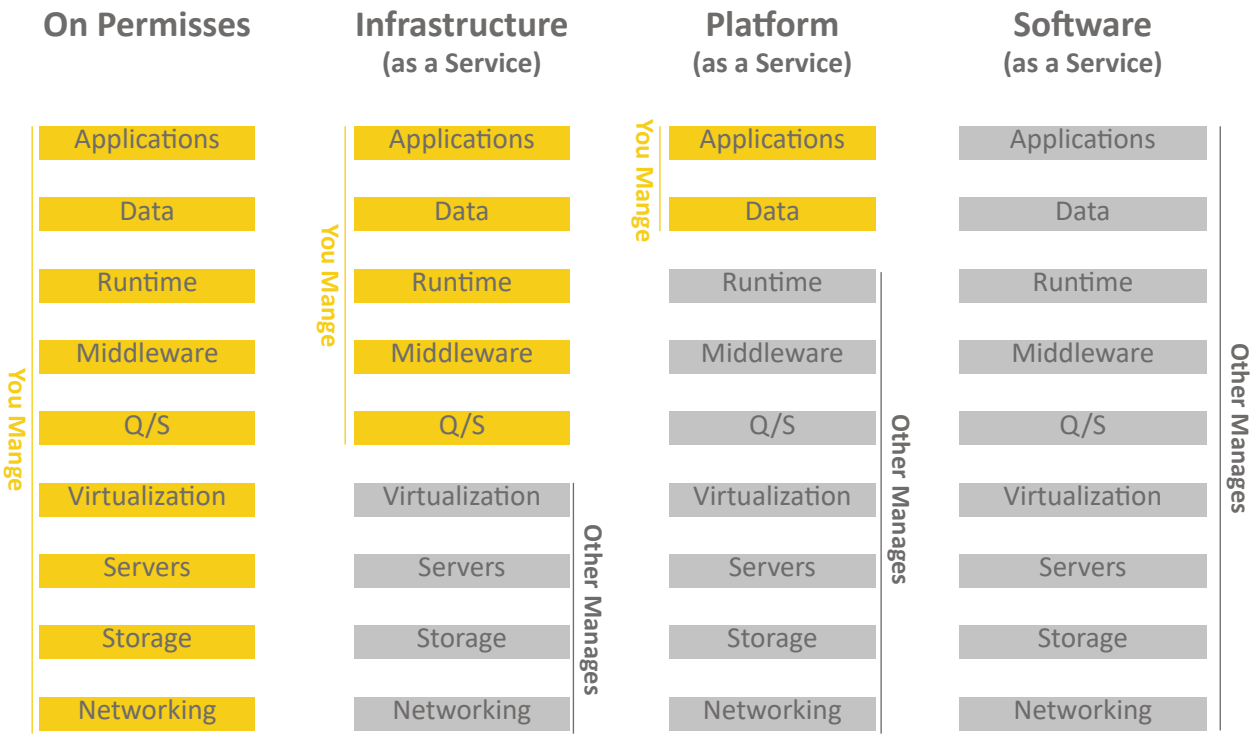
קיימים שלושה מודלי שירות בסיסיים למחשוב ענן. השוני העיקרי בין מודלים אלה הוא חלוקת האחריות בין ספק השירות לבין הלקוח:

- **תשתית כשירות Infrastructure as a Service (IaaS)** היכולת לספק תשתיות מחשוב, משאבי עיבוד, אחסון ותקשורת שבאמצעותם יכולים הלקוחות לעשות שימוש במערכות ובתוכנות. מודל זה מאפשר ללקוחות לעסוק בתחום מומחיותם, לצרוך שירותי מחשוב ללא צורך בקניית שרתים, ציוד תקשורת, מערכות הפעלה ורכיבים תשתיתיים, ולקבל סיוע של אנשי מערכת ואנשי תוכנה. יותר מזה, מודל התשלום הוא על פי השימוש בפועל בלבד - לא השתמשת, לא שילמת.
- **תוכנה כשירות Software as a Service (SaaS)** מודל שבו התוכנה והמידע הרלוונטי מתארחים במקום מרכזי (בדרך כלל בתשתית הענן). הגישה לשירותים אלה היא בדרך כלל באמצעות ממשק פשוט על מחשב הקצה כגון דפדפן.
- **פלטפורמה כשירות Platform as a Service (Paas)** מודל זה הוא שכבה נוספת מעל ה- IaaS והוא מספק שירותים נוספים המאפשרים לזרז את תהליך יישומן של אפליקציות ללא צורך לקנות ולנהל את החומרה והתוכנה הנדרשת לשם כך. שירותים אלה יכולים לכלול, בין היתר, סביבות פיתוח, טווחה (Middleware) ופונקציות כגון בסיסי נתונים, הפצת מסרים וניהול תורים.

חלוקת אחריות

חלוקת האחריות בין ספק השירות לבין הלקוח במיחשוב הענן היא סוגיה משמעותית,
המודלים השונים נבדלים זה מזה בהיקף האחריות ובחלוקתה בין הצדדים.

התרשים הבא מתאר את חלוקת האחריות בין הספק ללקוח במודלים השונים



כך למשל, אמזון (AWS), ספקית תשתיות הענן (IaaS) הגדולה בעולם, אחראית לתשתיות המפעילות את השרתים המופעלים אצלם, לאבטחתם הפיזית ולזמינותם. העדכניות, האמינות והאבטחה של מערכת ההפעלה, התוכנה והנתונים המותקנים על יחידה זו הם באחריות הלקוח. הסכמי ההתקשרות בין אמזון ללקוחותיה מדגישים את חלוקת האחריות בין ספק שירותי הענן לבין הלקוח במודל הנקרא Shared Responsibility.

מאידך, ספק כמו Salesforce.com, אחד מהספקים הגדולים בעולם של שירותי תוכנה כשירות (SaaS), אחראי לא רק על האבטחה הפיזית ועל תחזוקת התשתית של הפתרון אלא גם על התקנה, תחזוקה והאבטחה של מערכות ההפעלה, התשתיות, הנתונים והתוכנה. מודל זה מסיר חלק מן האחריות מן הלקוח. עם זאת, שימוש נאות במידע ובכלים שהספק מציע, כגון ניהול משתמשים והרשאות, הוא עדיין בתחום האחריות של הלקוח.

״המודל הישן של הפרדה ברורה בין המידע שנמצא ״בתוך הארגון״ למידע הנמצא ״מחוץ לארגון״ אינו תקף יותר. היתרון של שירות הענן - יכולת גישה אליו מכל מקום בכל עת - הוא גם הסיכון המרכזי״

ניהול סיכונים בענן

מחשוב ענן מציע לא מעט יתרונות למשתמשים בו, לרבות: ניצול אופטימלי הן בצד הספק והן בצד הלקוח.

- חיסכון כספי הלקוח אינו נדרש להקים תשתיות מחשוב בחצרו, להקדיש להם משאבים כמו שטח רצפה, חשמל, תחזוקה ואנשים. לספק יש את ״יתרון הגודל״ - לקוחות רבים מאפשרים לו לחסוך עלויות תוך ניצול יעיל של המשאבים.
- מעבר מהוצאה הונית (CAPEX) להוצאה תפעולית (OPEX).
- יכולת גידול (וקיטון) כמעט בלתי מוגבלת של משאבי המחשוב במהירות וביעילות.
- קיצור מחזור החיים של הפיתוח - התרכזות בעיקר ולא בהקמת התשתית ותחזוקה.
- קיצור הזמן הנדרש ליישום דרישות עסקיות חדשות - הקמת סביבת בדיקות, הוכחת היתכנות וייצור היא קלה ומהירה.

עם זאת, שירותי הענן מציבים לא מעט סיכונים שיש לנהל בצורה קפדנית. חשוב לבצע ניתוח שלם ומקיף של הסיכונים הרלוונטיים לסביבתו ולסביבת הספק הנבחר.

להלן מספר דוגמאות לסיכונים הנובעים ממעבר מערכות מידע לענן:

המודל הישן של הפרדה ברורה בין המידע שנמצא ״בתוך הארגון״ למידע הנמצא ״מחוץ לארגון״ אינו תקף יותר. היתרון של שירות הענן - יכולת גישה אליו מכל מקום בכל עת - הוא גם הסיכון המרכזי.

המעבר לענן גורם לאובדן חלק מן השקיפות לגבי תהליכי התחזוקה המפורטים של המערכות והמידע, מתודולוגיות העבודה שבהן נעשה שימוש, מיקומו הפיזי של המידע, הבקרות, האלגוריתמים שבהם נעשה שימוש וכדומה. רוב ספקי מחשוב הענן לא יסכימו לחלוק עם לקוחותיהם מידע מפורט בנושא זה, ודאי לא באופן שוטף.

המעבר לענן מרחיב את החשיפה של הארגון לאיומי סייבר בשל העובדה כי מידע של הארגון הופך להיות זמין במדיה ציבורית, ובדרך כלל נגיש באמצעות ממשק ציבורי באינטרנט. כמובן ישנם עוד סיכונים רבים אשר יש לתת עליהם את הדעת.

לאור מגוון הסיכונים, יש לנהל את סיכוני מחשוב הענן כחלק מניהול הסיכונים הכולל בארגון. המסגרת לניהול סיכוני ענן אינה שונה בעיקרה מכל מסגרת אחרת לניהול סיכונים. עליה לכלול תהליכים לזיהוי הסיכון והערכתו, זיהוי האיומים והפגיעויות והערכתם, ניתוח תרחישי סיכון, סבירותם והשפעתם, הצגת הסיכונים להנהלה וקבלת החלטה באשר לתגובה לסיכון, ובניית תכנית טיפול ומעקב אחר ביצועה. ראוי לציין כי COSO פרסמו מסמך ייחודי המתמקד בניהול סיכונים בסביבת מחשוב ענן.

ניהול הסיכונים במחשוב הענן חייב להיות מאמץ משותף של הארגון ושל ספקיו, והוא מתחיל עוד בטרם ההתקשרות עם הספק. חשוב להבין הן את רגישות המידע והאפליקציות והן את הבקרות הקיימות/מתוכננות אצל הספק לצמצום החשיפה.

כאשר אנו מתמקדים במבחן התוצאה מנקודת מבט עסקית (business impact), יהיו הדברים דומים מאוד לעולם המחשוב הקלאסי. הנושאים שחששנו מהם ב״עולם הישן״ כללו, בין היתר, פגיעה בזמינות, שלמות וסודיות המידע, אי עמידה בדרישות ציות ופגיעה ביעילות השירות. נושאים אלה חשובים גם בעולם הענן. ההבדל הוא בתרחישי המימוש של סיכונים אלה ועוצמתם, ובבקרות שיש ליישם כדי לצמצם סיכונים אלה.

בשירותי ענן מעורבים בדרך כלל לפחות שני גורמים - ספק השירות והלקוח שלו. במקרים רבים קיימים מספר גורמים - מספר ספקים המספקים שירותים זה לזה. יש לנהל את הסיכונים תוך הבנת המשמעויות הנובעות מכך: בנוסף על ניהול הסיכונים שלו, כל גורם אחראי גם על הסיכונים הנובעים מן העבודה מול הגורמים האחרים. נציג לדוגמה ארגון פיננסי העושה שימוש באפליקציה בענן המתבססת על ספק ענן המספק תשתיות. פריצת אבטחת מידע המתבצעת אצל ספק התשתיות עשויה להשפיע על ספק האפליקציה ובהתאמה על הארגון הפיננסי ולקוחותיו. הארגון הפיננסי לא יכול להתנער מאחריותו לתוצאות של התקרית ולהפנות את לקוחותיו אל ספק הענן כאחראי למחדל.

יש להגדיר וליישם תהליכי עבודה, דיווח ובקרה יעילים בין כל הצדדים, הלקוח והספקים. יש להבטיח כי ניהול סיכונים שוטף יהיה מובנה היטב ביחסי הגומלין בין הצדדים: על הספק לקיים וליישם מסגרת מתועדת לניהול סיכונים, להציג אותה ללקוח ולאפשר ללקוח לבחון בעצמו את הסיכונים באורח תקופתי.

כמו כן, על לקוחות וספקי שירותי הענן לבנות מערך ממשל ובקרה יעילים, ללא קשר למודל היישום של הענן. על ניהול הסיכונים להיות משותף בין הספק ללקוח על מנת להשיג את היעדים שהוסכמו.

אנו חווים יותר ויותר דרישות של לקוחות המופנות אל ספקי שירותי ענן המפרטים בקרות טכנולוגיות ותהליכיות אותן על הספקים ליישם כתנאי להסכמתם לעשות שימוש בשירותים אלה.

"אנו חווים יותר ויותר דרישות של לקוחות המופנות אל ספקי שירותי ענן המפרטים בקרות טכנולוגיות ותהליכיות אותן על הספקים ליישם כתנאי להסכמתם לעשות שימוש בשירותים אלה"

דרישות רגולטוריות בשירותי הענן

במדינות רבות בעולם קיימות רגולציות ותקנות העוסקות בהגנה על פרטיות המידע ודורשות יישום בקרות טכנולוגיות, פיזיות ומנהליות הנדרשות על מנת להגן על המידע מפני אובדן, שימוש לרעה או שינוי. בין היתר ניתן לציין את HIPAA העוסקים במידע רפואי, PCI העוסקים במידע כרטיסי אשראי, הוראות הפרטיות של מדינות באירופה (שהתעדכנו לאחרונה) ועוד. כמובן שתקנות אלו רלוונטיות גם בענן.

קיימות מספר רגולציות הממוקדות באופן ספציפי באבטחת מידע בענן. כך, למשל, בארה"ב פרסם הממשל הוראה בשם FedRAMP העוסקת בנושא זה. ההוראה מתייחסת לבקרות אבטחת מידע אשר הוגדרו בתקן 800-53 של ארגון התקנים האמריקאי NIST בהתאמה לסביבות הענן.

בעולם מתגבשים מספר סטנדרטים ספציפיים לנושא אבטחת מידע בענן. המובילים בהם הם 27017 ו-27018 של ISO, ותקן STAR של ארגון ה-Cloud Security Alliance. שלושת התקנים הללו מהווים הרחבה לתקן אבטחת המידע הבינלאומי ISO 27001 וההנחיות המעשיות ליישומו - תקן ISO 27002.

מובן כי תקנים, הנחיות והוראות כלליות נוספות בתחום אבטחת מידע והגנת הסייבר תקפים גם בעולם מחשוב הענן בהתאמה הנדרשת לסביבה זו.

בישראל מספר רגולציות העוסקות בנושא זה. ביוני 2015 פרסם המפקח על הבנקים הוראה המתמקדת בנושא ניהול סיכונים בענן. הוראה זו דורשת לקבל החלטות בנושא זה ברמת הדירקטוריון, לבחור בקפידה את המערכות והשירותים שניתן להעביר לענן, להעריך סיכונים באופן תדיר, לכלול דרישות פרטניות מספקי השירותים, לקבל דוחות מפורטים על יישום הבקרות הנדרשות ועל היכולת להפסיק את השירות בכל עת. רגולציות נוספות של בנק ישראל ושל המפקח על הגופים המוסדיים נוגעות בניהול סיכוני אבטחת מידע וסייבר, ומתייחסים בין היתר לנושא הענן.

אנו מצפים כי בתקופה הקרובה יתפרסמו הנחיות והוראות נוספות בתחום זה בארץ ובעולם בקרב מגזרים שונים כמו המגזר הממשלתי, הביטחוני, הבריאותי ועוד.

ביקורת פנימית של סביבת ושירותי הענן

ממשל תאגידי תקין דורש לקיים ביקורת על תהליכים ותשתיות מהותיים לארגון. בארגון שבו נעשה שימוש משמעותי בשירותי ענן, חשוב לכלול ביקורת על שירותים אלה כחלק מתכנית הביקורת התקופתית של הארגון.

יעדי הבדיקה של הביקורת ישתנו בהתאם לאופי השירות שהארגון מספק או צורך. אם מדובר בארגון שיישם שירותי ענן, ארגון המציע תשתיות ענן (IaaS או PaaS) או ארגון המפתח ומספק תוכנה כשירות (SaaS). מובן כי בלא מעט מקרים נמצא ארגונים שיהיו בעת ועונה אחת ספקים של שירותי ענן וגם לקוחות של שירותים כאלה.

כמו כן, מודל היישום של הענן - ענן פרטי, ציבורי, קהילתי או היברידי, ישפיע על היקף הביקורת וצורתה.

תכנון מקיף ומפורט של ביקורת זו הוא חיוני מפני שמדובר בביקורת מורכבת ביותר הכוללת היבטים שונים ורבים. מובן שאין חובה לבדוק את כל ההיבטים במהלך ביקורת אחת, אלא ניתן ורצוי לפצל את הנושא למספר תתי ביקורות שיתבצעו במועדים שונים או ברצף.

היבט נוסף הוא באיזה שלב של מעבר לענן נמצא הארגון - בחינת הרעיון, תכנון המעבר, ביצוע המעבר, כניסה מבוקרת לענן או שימוש מסיבי בו.

בנוסף על ההיבטים לעיל, הנוגעים בעיקר לשלב של תכנון הביקורת מבחינת היקפה ואופייה, ישנן מספר נקודות חשובות הנוגעות לנושאי תפעול ובקרה, שאותן ניתן לכלול במסגרת ביצוע ביקורת פנימית ומפורטות בעמוד הבא.

סיכום

ממ סמך זה כולל מספר סוגיות שמומלץ להתייחס אליהן במהלך ביקורת פנימית בסביבת ענן. נושאים אלה כוללים היבטים ארגוניים (תפקידים ואחריות), תהליך ניהול הסיכונים, דרישות רגולטוריות, בקרות טכנולוגיות, בקרות תהליכיות ופיתוח מאובטח. מִפרט מלא של בקרות אבטחת מידע ניתן למצוא במסגרות לניהול סיכוני ענן כגון STAR של ה-Cloud Security Alliance, התקנים 27017 ISO ו-27018 ISO ואחרים.

חשוב להיעזר בביקורת זו בגורמים מקצועיים. ביקורת בתחום זה מצריכה שילוב של מומחים בתחומים שונים בעלי הבנה וניסיון מערכתי ורוחבי. בין היתר יש להתמקד בהיבטים עסקיים, בתהליכי ניהול סיכונים ובשיקולי אבטחת מידע, ונדרשת הבנה טכנולוגית מעמיקה בנושא סייבר ואבטחת מידע בענן.

הסמכות בנושאים אלה, כגון הסמכת CCSK של ה-Cloud Security Alliance, יכולות לסייע בבחירת המבקרים המתאימים. כמו כן כדאי לבדוק את ההיכרות של המבקרים עם הסביבות הספציפיות של הביקורת, כגון התמחות בסביבת AWS, Azure או Google וכן בסביבות הפיתוח והאפליקציות הרלוונטיות בענן.

אנו מציעים לגשת לביצוע ביקורת בתחום סייבר בכלל, ומחשוב ענן בפרט, תוך דגש על נקודת המבט של התוקף - ניתוח הסיכונים העומדים בפני תשתיות הענן מתוך חשיבה "בראש של התוקף", חשיבה שאינה מתמקדת ברשימת של בקרות ומסמכים אלא בחשיפת נקודות חולשה טכנולוגיות ואנושיות וניסיון להגיע דרכן אל יעדים העשויים לעניין את התוקף. ניתן וכדאי לצרף לצוות הביקורת אדם בעל יכולות חשיבה כאלה.

נושאים לביקורת ענן (היבטי תפעול ובקרה)

ניתוח איומים | בביצוע הביקורת חשוב לנתח את תסריטי האיום הרלוונטיים לסביבת העבודה בענן, ולוודא שהארגון הציב בקרות בהתאם וכי קיימת פונקציה שמתפקידה לבחון באופן שוטף את יעילותן של הבקרות.

מדיניות ובקרות | על הארגון להתאים את המדיניות ואת נוהלי העבודה שלו לסביבת העבודה בענן. במסגרת הביקורת ניתן לוודא כי הארגון הגדיר מי בוחר מערכות בענן, על פי אילו מדדים, מי רשאי לאשר, וכיצד.

תפקידים ואחריות | במסגרת הביקורת חשוב לוודא כי הוגדרה האחריות לניהול סיכוני הענן, הן מבחינה חוזית והן מבחינת יישום פרקטי. כחלק מביקורת פנימית יש לבחון מעורבות ואחריות של ההנהלה בתהליכים.

הגדרת דרישות למערכת | במסגרת הביקורת יש לוודא כי בעת פיתוח ו/או רכישה של מערכת הוגדרו דרישות אבטחת המידע הרלוונטיות, לרבות התייחסות לנושאים כגון שמירה על פרטיות המשתמשים, שמירה על חיסיון הנתונים, שמירה על שלמות המידע, שמירה על אמינות המידע, שמירה על זמינות המערכת, שמירה על שלמות תהליכים עסקיים, ממשקים עם מערכות חיצוניות, ועוד.

יישום המערכת | כחלק מתהליכי העבודה יש להקפיד על כתיבת קוד בהתאם לכללי פיתוח מאובטח. כמו כן, יש לבצע סקר קוד (Code Review) על מנת לוודא את יישום דרישות אבטחת המידע. ניתן לעשות זאת תוך שימוש בכלים אוטומטיים כגון Static Code Analyzer. על הביקורת לוודא כי נעשה שימוש בכלים אלו שמטרתם שמירה על פיתוח מאובטח.

בדיקות | יש לדאוג כי פיתוח ויישום בדיקות יכללו את כל היבטי אבטחת המידע. במסגרת ביצוע הביקורת ניתן לערוך בדיקות המתייחסות לבקרה אחר שלמות ביצוע הבדיקות תוך שימוש ברשימות תיוג מובנות וכו'.

בחינות חדירות | הואיל וכל מערכות הענן חשופות לרשת, לפני יישום מערכת חדשה חשוב לקיים מבדקי חדירות (Penetration Test).

הקשחת סביבת המערכת | מלבד האפליקציה עצמה, כל מערכת מידע כוללת רכיבי תוכנה וחומרה נוספים כגון מערכות הפעלה, בסיסי נתונים וכדומה. יש לוודא כי כל רכיבי המערכת מוקשחים בצורה מיטבית.

תחזוקה של המערכת | לאחר שהמערכת פועלת בסביבת הייצור יש לדאוג לבצע עדכוני אבטחת מידע שוטפים לתשתית המערכת (Security Patches). במסגרת הביקורת ניתן לבחון האם הוגדרו עדכונים שוטפים כאמור והאם הם מבוצעים באופן תקין.

ניהול נכסים ותצורה | נושא זה מורכב מאוד בענן, מפני שרכיבי מחשוב משתנים באופן תדיר. חשוב לעקוב אחר הנכסים הנוכחיים ולבדוק כיצד הם מוגנים.

אבטחה ותשתיות פיזית | זוהי בקרה באחריותו של הספק. בסופו של דבר מחשוב הענן נמצא במיקומים פיזיים. יש לוודא כי המיקום הפיזי אינו באזור בסיכון גבוה וכי קיימות בקרות פיזיות מספיקות, כגון גדרות, מצלמות, חיישני תנועה, בקרת אש, אספקת חשמל, דלק, מיזוג וכדומה, וכן יכולת גיבוי.

המשאב האנושי | יש לוודא כי הספק מקפיד על בחירת האנשים, מיונם, הדרכתם ובקרה על ביצועיהם וכי תפקידם ואחריותם מוגדרים היטב. כמו כן יש לוודא שלכל אחד יש גישה רק למידע הנדרש לו במסגרת תפקידו. בעת ביצוע הביקורת מומלץ לוודא גם כי נושאים אלה הוסדרו במסגרת חוזה ההתקשרות וקיימת היכולת וההרשאה המתאימה לבדוק אותם מעת לעת.

ניהול משתמשים וההרשאה המתאימה | יש להקפיד על ניהול הרשאות הגישה של עובדי הספק למערכות ולנתונים בכל הרמות - התשתית, מערכות ההפעלה, ציוד התקשורת והאפליקציות. ניתן לבחון במסגרת הביקורת את מדיניות ההרשאות ויישומה, תדירות עדכון הסיסמאות ואת הבקרה שוטפת הקיימת אחר פעולות חריגות במערכות.

טיפול ותחזוקה בציוד | בעת ביצוע הביקורת ניתן לבחון האם וכיצד מבוצעת התחזוקה השוטפת בציוד והאם היא עומדת בהנחיות היצרנים. כמו כן, ניתן לבחון האם הארגון נאלץ לפגוע בתדירות גבוהה בזמינות השירות.

המשכיות עסקית | קיום תכנית לטיפול באירועי חירום, לרבות תיעוד מסודר ותרגול.

ניהול אירועים | תהליך ניהול אירועים בענן מציב אתגרים נוספים, מעבר לאלה הקיימים בסביבת המחשוב הקלאסית. מספר מגבלות עיקריות בנושא זה כוללות את הצורך בשיתוף פעולה עם ספק המחשוב. על ניהול האירועים בענן לכלול את כל האלמנטים של ניהול אירועים בסביבות האחרות, לרבות הגדרת הסיכונים ותרחישי הסיכון, הגדרת תגובות לתסריטים ידועים, זיהוי וניתוח של האירועים, ניתוח פורנסי של האירועים, החלת האירוע, סיום האירוע, הפקת לקחים.

IIA ישראל
אינוד מבקרים פנימיים בישראל
The Institute of Internal Auditors

התפתחות מתמדת

הכנס המקצועי השנתי של הביקורת הפנימית

יום ה', 05.01.2017

Avenue, Airport City

08:00 התכנסות והרשמה - ארוחת בוקר

09:00	**מושב 101 -** מנחה: **דורון רוזנבלום**, MBA, CRISC, CISA, CRMA, CIA, סגן נשיא ויו"ר משותף ועדת הכנס - IIA ישראל - איגוד מבקרים פנימיים בישראל, שותף עזרא יהודה-רוזנבלום יעוץ בקרה וניהול סיכונים מקבוצת Kreston IL
	פתיחת הכנס: דורון כהן, רו"ח, נשיא IIA ישראל - איגוד מבקרים פנימיים בישראל
09:20	**מושב 102 -** מנחה: **דורון רוזנבלום**, MBA, CRISC, CISA, CRMA, CIA, סגן נשיא וחבר הוועדה המקצועית - IIA ישראל - איגוד מבקרים פנימיים בישראל, שותף עזרא יהודה-רוזנבלום יעוץ בקרה וניהול סיכונים מקבוצת Kreston IL
	חידושים בתקנים המקצועיים הבינלאומיים **דורון רונן**, רו"ח, CRISC, CFE, CRMA, CIA, LLM, MA - משנה לנשיא ויו"ר הוועדה המקצועית - IIA ישראל - איגוד מבקרים פנימיים בישראל, נשיא שקדם ISACA ישראל
09:45	**מושב 103 -** מנחה: **דורון רוזנבלום**, MBA, CRISC, CISA, CRMA, CIA, סגן נשיא ויו"ר ועדת הקשר ללשכות בינלאומיות - IIA ישראל - איגוד מבקרים פנימיים בישראל, שותף עזרא יהודה-רוזנבלום יעוץ בקרה וניהול סיכונים מקבוצת Kreston IL
	Appreciative auditing: Is there such a thing? Guest Keynote Speaker: **Michael J. Fucilli**, CIA, QIAL, CRMA, CGAP, CFE, Adjunct Professor for Pace University, Auditor General of the Metropolitan Transportation Authority of New-York, Board Member IIA North America
10:15	**מושב 104 -** מנחה: סטלה **קורין-ליבר**, עיתונאית ופרשנית בכירה, גלובס
	רב-שיח (פאנל): אפקטיביות הביקורת הפנימית משתתפים: **ח"כ קארין אלהרר**, יו"ר הוועדה לענייני ביקורת המדינה; השופט **יוסף שפירא**, מבקר המדינה; **יוסי בהיר**, MBA, יו"ר ועדת ביקורת פסגות; **רון לונדון**, יו"ר ועדת ביקורת כלל ביטוח; **יוסי ניצני**, MBA, יו"ר ועדת ביקורת טבע; פרופ' **שוקי שמר**, יו"ר ועדת ביקורת אל על; רו"ח **יזהר קנה**, נשיא לשכת רואי חשבון בישראל

11:35 הפסקת רישות (Networking), קפה ופירות | פיצול למסלולים מקבילים (200)

	מושבי 210 - אחריות המבקר הפנימי וכיווני התפתחות	מושבי 220 שיטות וכלים	מושבי 230 המסלול הפיננסי
מנחה:	**רון גרופל**, רו"ח, סגן נשיא ויו"ר ועדת הקשר לחברות הציבוריות IIA ישראל, לשעבר המבקר הפנימי הראשי טבע תעשיות פרמצבטיות	**דניאל שפירא**, רו"ח, דירקטור ויו"ר ועדת הקשר לכנסת - IIA ישראל	**יעל רונן**, רו"ח, סגנית נשיא וחברת ועדת הכנס IIA ישראל, מבקרת פנימית ראשית הבנק הבינלאומי; **ערן שחף**, עו"ד, דירקטור ויו"ר ועדת הקשר לגופים מוסדיים/שוק ההון IIA ישראל, מבקר פנימי ראשי - כלל חברה לביטוח

ההשתתפות בכנס מקנה למשתתף 7.5 שעות CPE

* התוכנית כפופה לשינויים
** האולמות ממוזגים, נא להתלבש בהתאם
••• בסיום הכנס תתקיים האסיפה הכללית השנתית של חברי האיגוד

מח' אירועים טל' 03-7330777
או באתר https://iia-2017.events.co.il
לחסויות: נטלי 03-7330770 natali@pc.co.il

לפרטים נוספים ורישום לכרמית:
03-7330790, carmitj@pc.co.il

12:00	**מושב 211 - ביקורת פנימית - מצב נוכחי אל מול מצב עתידי - נחיצות השינוי; לאילו כיוונים הביקורת הפנימית צריכה להתפתח על מנת שתישאר רלוונטית ובעלת ערך כלפי הארגונים השונים** **סמדר מורלי דברת**, MA, חברת ועדת הכנס IIA ישראל, מנהלת בכירה במחלקת ניהול סיכונים, Deloitte בריטמן אלמגור זהר	**מושב 221 - הערכות לשעת חירום פרקטיקות מקובלות מנקודת מבט המבקר הפנימי** **דנה גוטסמן ארליך**, רו"ח, CRMA, CIA, MA שותפה, מנהלת קבוצת ניהול סיכונים, BDO זיו-האפט	**מושב 231 - QAR עם דגשים למגזר הפיננסי** Guest Keynote Speaker: **Michael J. Fucilli,** CIA, QIAL, CRMA, CGAP, CFE, Adjunct Professor for Pace University, Auditor General of the Metropolitan Transportation Authority of New-York, Board Member IIA North America
12:30	**מושב 212 - COSO 2016 - מתודולוגיה חדשה לניהול סיכונים מודרני** **יוסי גינוסר**, רו"ח, CRMA, CFE, CIA, סגן נשיא - IIA ישראל, מנכ"ל פאהן קנה ניהול בקרה Grant Thornton Israel	**מושב 222 - מכרזים - אתגרים חדשים (והכרחיים) לביקורת הפנימית** **שמואל רוזנבלום**, רו"ח, LLM, CFE, CIA דירקטור וגזבר ויו"ר ועדת כספים IIA ישראל, שותף רוזנבלום -הולצמן	**מושב 232 - Data Analytics למגזר הפיננסי** **שלומי קוט**, רו"ח, CISA, MBA, CIA, שותף קבוצת הייעוץ EY

13:00 ארוחת צהריים רישות (Networking)

	מושבי 210 - אחריות המבקר הפנימי וכיווני התפתחות	מושבי 220 שיטות וכלים	מושבי 230 המסלול הפיננסי
מנחה:	**אורן שחר**, רו"ח, CISA, CIA, דירקטור ויו"ר הוועדה למענה לשאלות מקצועיות של מבקרים IIA ישראל, מבקר פנימי ביחידת הביקורת הפנימית - התעשייה האווירית לישראל	**אורית גדות הורניק**, MA, CIA, דירקטורית ויו"ר הוועדה להגנת חברים IIA ישראל **מנחם רהב**, רו"ח, סגן נשיא ומזכיר לשכת רואי חשבון	**גלית וייזר**, רו"ח, דירקטורית ויו"ר ועדת הקשר לבנקים IIA ישראל, מבקרת פנימית ראשית בנק מזרחי-טפחות
13:45	**מושב 213 - סיכונים אסטרטגיים, סיכונים פורצים-הערכות ומענה** **בעז ענר**, רו"ח, CIA, MA, לשעבר משנה למנכ"ל משרד מבקר המדינה, מרצה ויועץ - ביקורת פנימית וציבורית	**מושב 223 - טיפול שורש בראיית הביקורת** **גיל בר**, רו"ח, CRISC, CIA, דירקטור, יו"ר ועדת ניהול סיכונים וחבר ועדת הכנס IIA ישראל, מבקר אל על נתיבי אויר לישראל	**מושב 233 - ליווי פרויקטים על-ידי הביקורת הפנימית - התקינה והלכה למעשה** **יעל רונן**, רו"ח, סגנית נשיא וחברת ועדת הכנס IIA ישראל, מבקרת פנימית ראשית הבנק הבינלאומי; **ערן שחף**, עו"ד, דירקטור ויו"ר ועדת הקשר לגופים מוסדיים/שוק ההון IIA ישראל, מבקר פנימי ראשי - כלל חברה לביטוח
14:15	**מושב 214 - אתיקה - אי תלות של המבקר הפנימי - האמנם?** **איציק ליפל**, רו"ח, MBA, CRMA, CIA חבר הוועדה המקצועית וחבר ועדת כנסים והשתלמויות IIA ישראל, יועץ עצמאי, מבקר פנימי ראשי לשעבר של דואר ישראל ושל בנק דקסיה ישראל	**מושב 224 - הדברים שהביקורת צריכה לדעת על איום הסייבר** **מני ברזילי**, מנכ"ל חברת FortyTwo, CTO מרכז מחקר הסייבר הבינתחומי באונ' תל-אביב	

מליאת נעילה

14:45	**מושב 301** - מנחה: **לילי אילון**, רו"ח, דירקטורית ויו"ר ועדת הקשר לחברות הממשלתיות IIA ישראל, לשעבר סגנית בכירה למנהל רשות החברות הממשלתיות

Closing Session (1): Governance: You know what it is. But how do you audit it?
Guest Keynote Speaker: **Michael J. Fucilli**, CIA, QIAL, CRMA, CGAP, CFE, Adjunct Professor for Pace University, Auditor General of the Metropolitan Transportation Authority of New-York, Board Member IIA North America

15:30	**מושב 302** – מנחה: **רונית בירן**, רו"ח, CRMA, חברת ועדת הכנס IIA ישראל, מבקרת פנימית ראשית שיכון ובינוי (שו"ב) מקבוצת אריסון

מליאת נעילה: (2) צולח את החיים בעיניים עצומות **איתם ישראלי**, מנחה ומרצה למוטיבציה

16:30 Coffee to go - להתראות בכנס הבא!

בין אבטחת מידע לסייבר| תפקידו של המבקר הפנימי

מאת **אסף ויסברג,** CISA, CISM, CEGIT, CRISC, נשיא ISACA ישראל
תומר רוזנר, CCSK, MA, CISA

רקע

פתגם הסיני העתיק "הלוואי שתחיה בזמנים מעניינים", רלוונטי במיוחד בכל הנוגע לתחום ההגנה בסייבר, ומחייב אותנו להתאים את עצמנו לזמנים כאלה הן במישור האישי והן במישור המקצועי.

בעוד שגורמים שונים יענו באופן שונה על השאלה "מה ההבדל בין אבטחת מידע לבין הגנה בסייבר?", אין חולק כי סיכוני סייבר מתממשים חדשים לבקרים, ולכן ארגונים נדרשים להיערך לסיכונים אלו - כאן ועכשיו.

לדעת המחברים, תחום ההגנה בסייבר הוא שינוי אבולוציוני של תחום אבטחת המידע, כאשר בעידן הסייבר ניכרת עלייה חדה ב:

- מספר התוקפים.
- רמת התחכום של התוקפים.
- כמות המטרות לתקיפה ואיכותן.

כפועל יוצא, החלו ארגונים בארץ ובעולם להגדיל את היקף ההשקעה בתחום ההגנה בסייבר, אולם השקעה זו כשלעצמה אינה מספיקה. על הארגון להבטיח כי המשאבים המושקעים בתחום הסייבר מוקצים באופן נכון, בהתאם למפת האיומים העדכנית, תוך שימת דגש גם על תחומים שבעבר נזנחו, כגון ניטור וניהול אירועי סייבר ואבטחת מידע.

מאחר שתחום ההגנה בסייבר חדש יחסית וטרם התייצב בארגונים, נדרשת מעורבותם של גורמי ביקורת וניהול סיכונים, שיבחנו את מפת הסיכונים העדכנית ויבטיחו כי משאבים מוקצים באופן נאות - בהתאם לרמת הסיכונים העסקיים הנובעים מאיומי סייבר.

מאמר זה מבקש לתאר את מאפייני האתגרים שבפניהם ניצבים כיום ארגונים, ולהציג את חשיבות תפקידו של המבקר הפנימי ואת הערך שהוא עשוי להביא, כגורם משמעותי בתהליך ההתמרה, הן לשיפור מוכנות הארגון לעידן הסייבר, והן לצמצום הסיכון לפגיעה משמעותית בפעילות הארגון בהיבטי ציות, פיננסים ומוניטין.

התלות הגוברת של ארגונים בטכנולוגיות המידע, לצד טשטוש גבולות והזמינות של מידע ארגוני על אמצעי מחשוב פרטיים של עובדים (מגמת ה- BYOD Bring Your Own Device), משפרים ומייעלים תהליכים ארגוניים, אולם בד בבד מחוללים מצב חדש - מצב שבו מידע ארגוני רגיש נמצא ביותר ויותר אמצעי מחשוב, חלקם בעלי רמת הגנה נמוכה ואפילו ביתית

עידן הסייבר

התלות הגוברת של ארגונים בטכנולוגיות המידע, לצד טשטוש גבולות והזמינות של מידע ארגוני על אמצעי מחשוב פרטיים של עובדים (מגמת ה- BYOD Bring Your: Own Device), משפרים ומייעלים תהליכים ארגוניים, אולם בד בבד מחוללים מצב חדש - מצב שבו מידע ארגוני רגיש נמצא ביותר ויותר אמצעי מחשוב, חלקם בעלי רמת הגנה נמוכה ואפילו ביתית. במילים אחרות,

מספר המטרות או "הפרסים" עבור גורמים עוינים עולה באופן אקספוננציאלי, כאשר כ-6.5 מיליארד מכשירים מסוגים שונים מחוברים כיום לרשת האינטרנט (לפי הערכות), והצפי הוא כי עד שנת 2020 המספר הזה יגיע ל-50 מיליארד, כאשר רמת ההגנה עליהם אינה משתפרת ולעתים אף פוחתת.

בהתאם לאופי הארגון ותחום פעילותו, אותם גורמים עוינים עלולים להיות:

- גופי תקיפה של מדינות;
- האקטיביסטים (Hacktivists);
- טרוריסטים;
- גורמי פשיעה כלכלית;
- גורמים פנים ארגוניים.

אחד ממאפייני התקופה הבולטים הוא פרסום של התממשות סיכוני סייבר במגוון רחב של ארגונים. גם בעבר התממשו סיכוני סייבר ואבטחת מידע שונים, אולם אי חשיפת הנזק על ידי התוקפים סייעה לארגונים לספוג את הנזק ולהצניע את עצם האירוע. כיום, כאשר מחקרים עדכניים מראים כי 90% מהארגונים אישרו כי חוו לפחות אירוע סייבר אחד במהלך 2015, ולאחר אין-ספור מקרים של חשיפת פרטים שנגנבו במהלך תקיפות סייבר, לא ניתן עוד להסתיר את היקף התופעה. גם בארץ התפרסמו אירועים שונים, לרבות:

חדירת וירוס בפברואר 2016 למחשבי משרד האוצר במטרה להצפין קבצים ולנעול אותם לשם קבלת כופר כספי.

ניסיון סחיטה מצד עובד לשעבר של חברת לאומי קארד באוקטובר 2014, בדרישה לתשלום בסך של 3 מיליון שקלים בתמורה לאי פרסום מאגר הנתונים של 1.5 מיליון לקוחות החברה.

זליגת מידע רגיש בהיבט הביטחוני. בהתאם לדיווחים ממקורות זרים שהתפרסמו ביולי 2014, פרצו האקרים סיניים למחשבי חברות מהתעשייה הביטחונית בארץ וגנבו מידע טכנולוגי רגיש.

התפשטות הווירוס "בני גנץ" במחשבי משטרת ישראל, שהובילה בדצמבר 2012 לניתוק יזום של מחשבי המשטרה מרשת האינטרנט, נוכח החשש לחשיפת מידע רגיש.

התממשות סיכוני סייבר עלולה לפגוע במידע ונתונים בהיבטי סודיות, זמינות ושלמות, להזיק למוניטין ולפעילות עסקית, ואף להוביל לנזק פיזי

מאפייני מתקפות סייבר

בדומה לסיכוני אבטחת מידע, התממשות סיכוני סייבר עלולה לפגוע במידע ונתונים בהיבטי סודיות, זמינות ושלמות, להזיק למוניטין ולפעילות עסקית, ואף להוביל לנזק פיזי. עם זאת, מקובל לייחס לתקיפות סייבר מאפיינים המבדלים אותן מהתקיפות ה"מסורתיות" שהיו נפוצות לפני מספר שנים כמפורט להלן:

מאפיין	תקיפות "מסורתיות"	תקיפת סייבר
פרופיל התוקף	עברייני מחשב יחידים, חובבנים (script kiddies).	מדינות, טרוריסטים, האקטיביסטים, גופי פשיעה בינ"ל.
כלי התקיפה	לרוב, שימוש בכלי תקיפה גנריים הזמינים באינטרנט.	שימוש בכלי תקיפה שפותחו במיוחד, או כלים גנריים שעברו התאמות לארגון המותקף.
וקטור תקיפה	בדרך כלל, שימוש בכלים טכנולוגיים לסריקת רכיבי הרשת הארגונית וחשיפת נקודות תורפה באופן אקראי.	שימוש בכלים טכנולוגיים, וכן ביצוע מתקפות הנדסה חברתית על עובדים וספקים, הן במסגרת הארגון והן במסגרת פרטית דוגמת Facebook.
יעדי התקיפה	לרוב אקראיים, בהתאם לחולשות האבטחה שזוהו.	נכסי מידע מרכזיים ו/או מערכות ליבה המהוות פלטפורמה לתהליכים עסקיים משמעותיים. היעדים נבחרים מראש ומהווים את המוטיבציה לעצם ביצוע התקיפה.
משך ביצוע התקיפה	קצר יחסית, תוך ניסיון להפיק ערך כלשהו מהמטרות שבהן זוהו באופן אקראי חולשות.	ארוך - חודשים ואף שנים, תוך התמקדות ביעדים שהוגדרו מראש (APT - Advanced Persistent Threat).

הערכת סיכוני סייבר

השינוי במאפייני מתקפות הסייבר מחייב להרחיב את מודל הערכת הסיכונים הארגוני כך שיספק מענה גם לסיכונים הנובעים מאיומי סייבר.

מאחר שאיומי הסייבר עלולים להוביל בין היתר להתממשות סיכוני ציות, פיננסיים ומוניטין, או לסיכונים אחרים המשפיעים על התוצאות העסקיות של הארגון, חשוב לשלב את תהליך הערכת סיכוני הסייבר כחלק מהתהליך הארגוני הכולל. להשאיר טקסט וגם להוציא ליד חיצוני בין היתר, יש לוודא כי גורמי הסיכון הכלולים במודל הערכת הסיכונים הארגוני ומסייעים בהערכת הסבירות להתממשות הסיכון מתייחסים גם לאיומי סייבר, אולם מניסיוננו לב העניין הוא יצירת הקשר בין איום הסייבר, הנזק העסקי הפוטנציאלי - והבקרות הטכנולוגיות והאחרות שיסייעו בהפחתת הסיכון.

תחכום איום הסייבר, עוצמתו והשלכותיו - במקרה שהתממש, מחייבים התייחסות בשני רבדים, במסגרת ניהול סיכוני הסייבר:

- ברובד האסטרטגי - מעורבות דירקטוריון והנהלה, לרבות קביעת מדיניות ניהול סיכוני סייבר, הקצאת משאבים וקבלת דיווחים בנושא, בין היתר בוועדת הביקורת של הדירקטוריון;
- ברובד התפעולי - גיבוש מפת איומי סייבר רלוונטית לארגון, והמלצה על בקרות שיסייעו בצמצום סיכונים עסקיים הנובעים מאיומי סייבר.

מידע נוסף ניתן למצוא בתרגום לעברית של ISACA ישראל למסמך "חוסן סייבר ארגוני: השאלות שדירקטורים צריכים לשאול", הזמין להורדה חופשית.

התייחסות כזאת תאפשר ליצור מערך ארגוני של הגנה בסייבר בעל רמת בשלות (Maturity) נאותה, וכן יכולת לשיפור מתמיד, הנדרשת לצורך התמודדות אפקטיבית עם טבעו המשתנה של איום הסייבר.

תקנים מקצועיים לשימוש המבקר

התקנים המקצועיים הבינלאומיים של לשכת המבקרים הפנימיים העולמית (IIA) אינם כוללים התייחסות מפורשת לנושאי אבטחת מידע או סייבר. עם זאת, באשר להיבטי מערכות מידע, תקנים אלה כוללים מספר הנחיות בעלות השלכות ישירות על תחומים אלה:

- הנחיה A3.1210 קובעת כי "מבקרים פנימיים חייבים להיות בעלי ידע מספק אודות עיקרי הסיכונים בתחום טכנולוגיות המידע, הבקרות וטכניקות ביקורת מבוססות-טכנולוגיה..."
- הנחיה A2.2110 קובעת כי "הביקורת הפנימית חייבת להעריך האם פיקוח וממשל טכנולוגית המידע של הארגון תומך באסטרטגיות וביעדי הארגון."

מתודולוגיית הסייבר של National Institute of Standards and Technology NIST, המכון האמריקני לתקנים וטכנולוגיה, שגובשה בשיתוף ארגוני סייבר מקצועיים ובהם ISACA, מתייחסת לחמש דיסציפלינות שבהן יש להתמקד כדי לשפר את המוכנות הארגונית להתמודדות עם סיכוני הסייבר, ולשם יכולת המענה במקרה של התממשותם:

- **זיהוי** (Identify) - פיתוח ההבנה הארגונית במטרה לנהל את סיכוני הסייבר למערכות ונכסי מידע. הפעולות הננקטות בשלב זה הן ברמת הבסיס - הבנת ההקשר העסקי, המשאבים התומכים בפונקציות הקריטיות וזיהוי סיכוני הסייבר שאליהם הם חשופים. נקיטת הפעולות הללו מאפשרת לארגון למקד ולתעדף את מאמציו בהלימה לאסטרטגיית ניהול הסיכונים הארגוני ולצרכים העסקיים. דיסציפלינה זו נוגעת, בין היתר, להיבטים הבאים: ניהול נכסי מידע, הבנת הסביבה עסקית, ממשל אבטחת מידע וניהול סיכונים.
- **הגנה** (Protect) - גיבוש ויישום של אמצעי אבטחה נאותים, שיבטיחו את פעילותם הרציפה של שירותים עסקיים, מערכות מחשב ותשתית קריטיים. מטרתה של דיסציפלינת ההגנה היא להגביל או להכיל את ההשפעה של אירוע סייבר פוטנציאלי. פונקציה זו נוגעת, בין היתר, להיבטים הבאים: ניהול בקרת גישה, שיפור מודעות העובדים, ותהליכים ונהלים להגנה על מידע.
- **גילוי** (Detect) - פיתוח ויישום של הפעולות הנדרשות כדי לזהות את התרחשותו של אירוע סייבר. דיסציפלינת הזיהוי מאפשרת לקצר את טווח הזמן הנדרש לזיהוי אירועי סייבר, במטרה לצמצם את הנזק הנגרם ממנו, והיא נוגעת, בין היתר, להיבטים הבאים: אירועי אבטחת מידע, ניטור מתמיד בהיבטי אבטחת מידע ותהליכי זיהוי.
- **תגובה** (Respond) - פיתוח ויישום של הפעולות שיש לנקוט בעת זיהוי אירוע סייבר. יכולת התגובה מאפשרת להכיל את ההשפעה של אירוע הסייבר לאחר התרחשותו. דיסציפלינה זו נוגעת, בין היתר, להיבטים הבאים: תכנון מענה לאירוע סייבר, זיהוי פורנזי, תקשור מול גורמים שונים, ניתוח ושיפור מתמיד.
- **התאוששות** (Recover) - גיבוש סדר פעולות שנועדו לתחזק את תכניות ההתאוששות והשיקום, כתוצאה מאירוע סייבר. ההתאוששות מאפשרת חזרה מהירה לתפעול רגיל תוך צמצום ההשלכות השליליות מאירוע סייבר. דיסציפלינה זו נוגעת, בין היתר, להיבטים הבאים: תכנון התאוששות, שיפורים ותקשור.

באוגוסט 2015 ציין נשיא לשכת המבקרים הפנימיים העולמית (IIA), ריצ'ארד צ'יימברס, את הצורך כי ארגונים יפעלו לשם מניעת חדירת האקרים, והדגיש כי הביקורת הפנימית יכולה לתמוך בתהליך זה. בהמשך לכך, בנייר עמדה רשמי שפרסם ה-IIA תחת הכותרת "Internal Audit's Key Role in Cyber Preparedness", הוצגו חמשת המרכיבים הנדרשים כחלק מגיבוש תהליך הוליסטי לשיפור המוכנות לאיומי סייבר :

- **הגנה** (Protection) - הביקורת הפנימית מספקת גישה הוליסטית לזיהוי (Identifying) נקודות שבהן הארגון עלול להיות פגיע. ממשל אבטחת מידע אפקטיבי הוא קריטי, והביקורת הפנימית יכולה לספק שירותי הבטחה (assurance) בהיבט זה.
- **גילוי** (Detection) - לעתים ניתוח נתונים טוב מספק לארגונים את הרמז הראשון כי משהו חריג מתרחש. הביקורת הפנימית משלבת עוד ועוד ניתוח נתונים וכלים טכנולוגיים נוספים בעבודתה. על גורמי הביקורת הבכירים לעבוד יחד עם מחלקת ה-IT במטרה להבטיח ניטור של אינדיקטורים מרכזיים, וכן ליצור יחסים מקצועיים הדוקים עם המנמ"ר ומנהל אבטחת המידע במטרה להבטיח את קיומן של בקרות הולמות ואפקטיביות.
- **המשכיות עסקית** (Business Continuity) - תכנון הולם חשוב לצורך התמודדות והתגברות על מספר תרחישי סיכון העלולים להשפיע על פעילות הארגון השוטפת, בהם תקיפת סייבר. הביקורת הפנימית יכולה לספק בטוחה בראייה כלל ארגונית כי תכנית ההמשכיות העסקית אפקטיבית ויעילה, ונותנת מענה לכך שהלקוחות ובעלי העניין יקבלו שירותים מהארגון בכל מצב.

- **ניהול משבר/תקשור** (Crisis Management/Communications) - בדומה לתכנון ההמשכיות העסקית, מוכנות לניהול משבר ותקשור בעת משבר יכולים להשפיע באופן משמעותי וחיובי על הלקוחות ועל בעלי העניין והמוניטין של הארגון. מחקר שנערך בקרב למעלה מ-350 ארגונים בשנים 2014-2016 הראה באופן עקיב כי היקף הפגיעה במוניטין של ארגונים בעלי מנגנון ניהול משבר היה נמוך ב-10% לעומת ארגונים ללא מנגנון זה. במקביל, בסקר שנערך בקרב למעלה מ-400 מנהלים בכירים מרחבי העולם, 77% מהם הגדירו את נושא ההמשכיות העסקית בהיבטי מערכות מידע כאחד משלושת הנושאים בעלי ההשפעה הרבה ביותר על המוניטין העסקי.
- **שיפור מתמיד** (Continuous Improvement) - בהיבט זה, הביקורת הפנימית יכולה לספק את הערך הרב ביותר, באמצעות מתן תובנות הנגזרות מעבודתה. מוכנות לסייבר משמעה התמודדות מוצלחת עם אירועי סייבר, אולם ללא הפקת לקחים ושיפור מתמיד, לא ניתן להבטיח את ההצלחה בהתמודדות עם האירוע הבא.

פגישה להפקת לקחים עם כלל הגורמים המעורבים לאחר התרחשות אירוע סייבר משמעותי, ובמידת האפשר גם לאחר אירועים בדרגות חומרה נמוכות, יכולה להיות לעזר רב בכל הקשור לשיפור רמת האבטחה ותהליך הטיפול באירועים. בין היתר, ראוי לדון במסגרת הפקת הלקחים בשאלות הבאות:

- מה בדיוק קרה ומתי?
- מה היה טיב המענה מצד צוות התגובה וההנהלה בבואם להתמודד עם האירוע? האם המענה היה בהתאם לנהלים הקיימים או שאלה נזנחו?
- מהו סדר הקדימות שבו נדרש היה לקבל את סוגי המידע השונים לשם טיפול יעיל באירוע?
- האם פעולות מסוימות שננקטו עיכבו את תהליך ההתאוששות?
- מה צוות התגובה וההנהלה צריכים לעשות באופן שונה בעתיד, אם אירוע דומה יתרחש?
- כיצד ניתן לשפר את שיתוף המידע עם ארגונים אחרים?
- אילו פעילויות מתקנות יכולות למנוע אירועים דומים בעתיד?
- אילו אינדיקטורים יש לנטר בעתיד במטרה לזהות אירועים דומים?
- אילו משאבים או כלים נוספים נדרשים לצורך זיהוי, ניתוח וטיפול באירועים עתידיים?

כפי שניתן לראות, המרכיבים המפורטים בנייר העמדה של ה-IIA דומים במידה רבה לדיסציפלינות הכלולות במתודולוגיית NIST.

המענה הנדרש

כמו בכל תחום אחר, על מנת לבצע ביקורת המקנה ערך לארגון, נדרש ידע בתחום המבוקר ותכנית ביקורת אפקטיבית.

לאור הצורך הגובר, גיבשה ISACA מענה נרחב לגורמים השונים העוסקים בתחום ההגנה בסייבר. עבור מבקרי מערכות מידע, העמידה ISACA בין היתר את המשאבים הבאים:

קורס יסודות ההגנה בסייבר - Cybersecurity Fundamentals. קורס זה, שהפך לאחרונה לחלק ממסלול מערכות מידע בבית הספר למנהל עסקים באוניברסיטת בר אילן, מיועד לחסרי ידע מקדים המעוניינים לרכוש את מושגי היסוד בתחום באופן שיטתי ומובנה, שיאפשר להם להוביל פעילויות ביקורת באופן מושכל ובהתאם למפת האיומים העדכנית.

נדרשת תכנית ביקורת אינטגרטיבית שנועדה לספק לארגון הערכה באשר לאפקטיביות המערך הארגוני להגנה בסייבר - הפעילויות, הנהלים והתהליכים בהיבטי מניעה, הזיהוי וההתמודדות עם סיכוני ואירועי סייבר.

נקודות חשובות לבחינת אפקטיביות מערך ההגנה מפני סייבר:

- **הבנה/היכרות עם תשתיות תומכות לנושא הסייבר** - ניהול סיכוני סייבר צריך להתבסס על תהליכי עבודה ונהלים. במסגרת זאת יש לראיין גורמי מפתח שונים בארגון, לרבות מנהל מערכות מידע, מנהל אבטחת המידע וקצין הציות, וכן לסקור מגוון מסמכים ובהם: מדיניות אבטחת מידע, תכנית תגובה לאירועי אבטחת מידע, רשימת נכסי מידע ועוד.
- **ממשל** (Governance) - מעורבות ההנהלה הבכירה במניעת אירועי סייבר בארגון. במסגרת זאת, ההנהלה הבכירה סוקרת באופן תקופתי את המדיניות וההערכות בנושא אירועי סייבר, ולצד זאת קיימת מעורבות של הדרגים הניהוליים של יחידת טכנולוגיות המידע והיחידות העסקיות בהחלטות העקרוניות המתקבלות בנוגע למניעת מתקפה סייבר ובאופן המענה למתקפה.
- **תפקיד הגורמים העסקיים במניעת אירועי סייבר** - לגורמים העסקיים יש תפקיד חשוב בהקטנת הסבירות להתממשות אירועי סייבר, זאת באמצעות ביצוע התהליכים הבאים:
  - **ניהול סיכונים** - על היחידות העסקיות לזהות את הסיכונים והפגיעויות הקיימים בתחום פעילותן, על ידי ביצוע סקר השלכות עסקיות (BIA - Business Impact Analysis) על בסיס עתי.
  - **סיווג מידע** - מתבצע בכל רחבי הארגון על בסיסי תבנית לסיווג מידע ובהתאם לקריטיות וחשיבות המידע, בדגש על מידע שיכול להוות מטרה לפשיעת סייבר.
  - **תקשור עם יחידות עסקיות בנוגע לפשיעת סייבר** - גורמי ניהול של יחידת טכנולוגיות המידע והיחידות העסקיות מקבלים עדכונים עתיים מיחידת אבטחת המידע.
  - **כרייה וניתוח של מידע** - מבוצעים במטרה לזהות תקיפות סייבר, ומשתכללים באופן רציף על ידי היחידות העסקיות.
- ניהול טכנולוגיות המידע - בהיבטי איום הסייבר, קטגוריה זו מצריכה התייחסות לשני נדבכים:
  - **אבטחת התשתיות** - בחינת אופן ניהול תשתיות המחשוב, לרבות ניהול תצורה, ניטור פעיל ודיווח על אירועי אבטחה.
  - תמיכה של הנהלת יחידת טכנולוגיות המידע בצוות תגובה לאירועי אבטחת מידע וסייבר.
- **מדיניות ונהלים לניהול אירועי סייבר** - מדיניות ניהול משבר צריכה לכלול ולהתבסס על סקר סיכונים ומיפוי של כל נכסי המידע הקשורים לרשת הארגונית. בנוסף, יש להקפיד על פעילות אפקטיבית של צוות תגובה לאירועי אבטחת מידע וסייבר, ערוצי דיווח יעילים ותחקור (forensic) מעמיק של אירועי סייבר.
- **צוותי התמודדות עם אירועי סייבר** - ERT/CSIRT CERT - Cyber Emergency Response Team, CSIRT- Computer Security Incident Response Team הם צוותים ייעודיים שנועדו לטפל באירועי אבטחת מידע; צוותים אלה כוללים חברי צוות בעלי מומחיות מסוגים שונים, כלים טכנולוגיים מתקדמים ועוד. צוותים אלה הם אחד הנדבכים המרכזיים בטיפול באירועי אבטחת מידע וסייבר במשך כל שלביהם - ניתוח הנתונים הרלוונטיים, קביעת אופי האירוע והשלכותיו, הכלתו ותחקורו. הם אמורים לקיים תרגולים על בסיס סדיר, לנקוט צעדי מניעה שונים להפחתת הסיכונים, ולהיות מצוידים בכלים הטכנולוגיים המתאימים.
- **מודעות עובדים** - יש להגביר את מודעות העובדים לצורך בזיהוי אירועים חריגים העלולים להוות אינדיקציה לאירוע אבטחת מידע וסייבר, ולהגדיר עבורם ערוצי דיווח, לרבות ציון הגורמים הרלוונטיים ודרכי ההתקשרות עמם.

כל אחד מהמרכיבים המופיעים לעיל, כמו גם מרכיבים נוספים המפורטים בתכנית הביקורת, נמדדים ומוערכים על בסיס מתודולוגיות מקצועיות בהיבטי סייבר (COBIT 5) וניהול סיכונים (COSO). תכנית הביקורת מסייעת למבקר הפנימי לגבש הערכה בדבר בשלות (Maturity) הבקרות הפרטניות בהיבטי מניעה, זיהוי והתמודדות עם סיכוני ואירועי סייבר, וכפועל יוצא - בשלות תחום ההגנה בסייבר בכללותו.

סיכום

אין ספק כי הסייבר טומן בחובו מגוון רחב של חשיפות לסיכונים, שהתממשותם עלולה לפגוע בפעילות של חברות וארגונים. העובדה כי בשלב זה ארגונים טרם ייצבו את המערך האמור לספק הגנה בפני איומי סייבר, יוצרת צורך, וגם הזדמנות, למעורבות הביקורת הפנימית, אשר תבטיח כי משאבי הארגון מתועלים באופן אפקטיבי, בהתאם למפת האיומים העדכנית והערכת הסיכונים הארגונית. לשם כך, נדרשת הביקורת הפנימית להעמיק ולחזק את הידע ואת היכולות המקצועיות בתחום ההגנה בסייבר.

מדור טכנולוגיות מידע וסייבר

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

החשיבות של מודעות העובדים לזיהוי ומניעה של התקפות סייבר

שכיחות התקפות הסייבר הולכת ועולה, וההתקפות הללו גורמות נזק רב יותר, כספי ותדמיתי. הנדסה חברתית (Social Engineering) היא פעילות מרכזית שבאמצעותה מושגת "דריסת רגל" במערכות וברשתות הארגוניות. מאמצים אלה נעשים למשל באמצעות פישינג (Phishing) - ניסיון להשיג מידע רגיש באמצעות התחזות, בדרך כלל בדואר אלקטרוני; Spear Phishing - ניסיון להשיג מידע רגיש מאדם מסוים תוך שימוש במידע פרטי כדי להגביר את הסיכוי להצלחת המתקפה; או באמצעות מתקפות מתוחכמות יותר המכוונות לדרג ההנהלה בארגון ועושות שימוש בהודעות הכוללות נוזקה (Malware). בשנים האחרונות, פעילות ההנדסה החברתית של התוקפים עברה לאינטרנט באמצעות אתרים, רשתות חברתיות ואפליקציות להתקנים ניידים (טלפונים חכמים, טאבלטים).

מומחים בנושא מסכימים כי אנשים הם נקודת תורפה מהותית בניסיונות תקיפה של מערכות ורשתות בהנדסה חברתית. הבנה זו חיונית כדי לספק מידה רצויה של אבטחת מידע.

פעולה, התעלמות, חוסר ידיעה או אי ציות של עובדים יכול להוביל לאירוע אבטחת מידע - למשל על ידי גילוי מידע רגיש (סיסמאות וכו') לגורם שאינו מורשה, התעלמות מפעילות חריגה או שימוש במידע רגיש על ידי עובד שלא לצורך ביצוע תפקידו תוך אי ציות לנהלים.

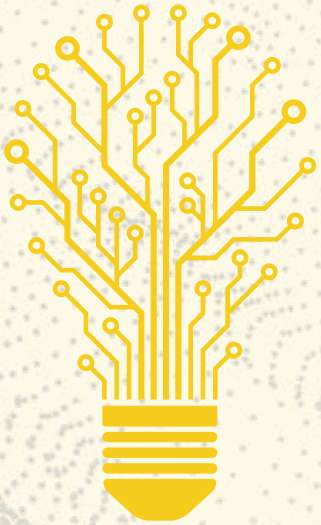
לתכנית מודעות והדרכת עובדים יש חשיבות רבה כחלק מאסטרטגיית אבטחת המידע הארגונית והיא המפתח לטיפול באיומי הנדסה חברתית. על העובדים להיות מודעים לאיומים הנפוצים, לאחריותם במניעת איומים אלה, לזיהויים ולדיווח עליהם.

בשנים האחרונות פותחו מתודולוגיות רבות בעניין בניית תכנית מודעות והדרכה באבטחת מידע בארגונים. לדוגמה, המכון האמריקאי הלאומי לתקנים וטכנולוגיה NIST פרסם תדריך מפורט בנושא (NIST SP 800-50) עוד בשנת 2003. תדריך זה מתאר את הצעדים לבניית תכנית כזו, ובהם עיצוב תכנית המודעות וההדרכה (כולל סקר דרישות, פיתוח ואישור אסטרטגיית הדרכה וכו'), פיתוח משאבי הדרכה (תוכן ההדרכות, חומרי ההדרכה וכו'), יישום תכנית המודעות וההדרכה, קביעת דרכי תקשור התכנים ומעקב תמידי אחר אפקטיביות התכנית.

סקר שנעשה לאחרונה על ידי ה-SANS מצביע Security Awareness Report 2016 על מספר אתגרים ביישום תכנית מודעות והדרכה. שלושת האתגרים העיקריים שעליהם מצביע הסקר הם: חוסר במשאבים, קשיים באימוץ התכנית וחוסר תמיכה של ההנהלה בתהליך. ביקורת פנימית בנושא תכנית מודעות והדרכה עשויה להוסיף ערך רב לארגון.

מספר רעיונות לבחינת תכנית המודעות וההדרכה:

- הירתמות של ההנהלה היא חיונית להצלחת התכנית. מומלץ לבחון את מידת המעורבות והאחריות של ההנהלה.
- יש לבדוק את מידת מעורבותם של גורמים מקצועיים בתהליך הבנייה והיישום של תכנית המודעות וההדרכה. למשל, מקובל שמחלקת אבטחת המידע אחראית על התכנים, ואילו אנשי מחלקת ההדרכה אחראים על דרכי ההנגשה ותקשור המסרים. כמו כן, חשוב לשלב גם את מחלקת הביטחון (שבדרך כלל אחראית על האבטחה הפיזית).
- יש לבחון כיצד נבנתה התכנית והאם קיים קשר מובהק למטרות הארגון, לתהליך ניהול הסיכונים, לתהליך ניהול אירועי אבטחת המידע (Incident Management) ולמגמות עולמיות.
- יש לבדוק את אופן תקשור התכנית לעובדים - האם המסר הרלוונטי הועבר לגורם הרלוונטי? מהם ערוצי התקשורת שנבחרו לשם כך?
- מומלץ לבדוק את אפקטיביות התכנית להשגת מטרותיה. ניתן לבדוק אפקטיביות באמצעות בדיקות פתע (שיחות טלפון המדמות תקיפה להשגת מידע רגיש, תרגילי התחזות ברשתות חברתיות, שליחת דוא"ל ממקור לא ידוע למייל הפנימי של העובדים כדי לבחון את ערנותם למיילים זדוניים ובדיקה האם יפתחו את הקישורים הללו, וכו'), קביעת יעדים מדידים ובחינת עמידה בהם (למשל הורדת כמות המשתמשים שהקליקו על דואר אלקטרוני זדוני שנשלח אליהם, בחינת כמות הדיווחים על אירוע חריג, וכו'), שימוש בסקרים, סריקת הרשת החיצונית לארגון והפנימית של הארגון כדי לבדוק האם דלף מידע רגיש מהארגון ומאיזה מקור בארגון, ועוד.
- יש לבחון האם פעילות המודעות וההדרכה תוקצבה בצורה מספקת. תקציב זה יכול להיקבע כאחוז מתקציב ההדרכה הכללי, אחוז מתוך תקציב ה-IT הכללי, הקצאה תקציבית לעובד, ועוד.
- יש לבדוק האם מופו קהלי יעד בקרב העובדים ולדרגם על פי סיכון. בהתאם לסיכון יש לתעדף ולהדגיש נושאים ספציפיים (דוגמאות לאוכלוסיות רגישות הן: אנשי מערכות מידע ורשתות, הנהלה, אנשי כספים, עוזרות אישיות, עובדי קבלן, עובדים חדשים או עובדים ששינו תפקיד בארגון, וכו').
- כחלק מהתכנית, יש לבדוק האם ניתן דגש להגברת המודעות לדרכי הדיווח של העובדים בנוגע לחשד להתקפה. דיווח מיידי הוא קריטי לעצירת ההתקפה ולהפחתת הנזק.



נושאי בדיקה נוספים מופיעים בתדריך שפרסם ה-NIST. מומלץ לעיין בו בהרחבה.

סיכונים פורצים
סיכונים מורכבים - משולבים
סיכונים אסטרטגיים

מאת **בועז ענר**, רו"ח, MA, CIA

תורת ניהול הסיכונים ותרומתה

אחד החידושים בתורת ניהול והערכת הסיכונים הוא נטישת שיטת הבקרות (CONTROL) המצומצמת, שהתמקדה רובה ככולה בנעשה בארגון עצמו ובנוהלי הבקרה הפנימיים בו, לטובת הצבעה על **סיכונים**, חלקם בעלי עוצמה רבה **שמעבר לגבולות הארגון**: סיכוני רגולציה, סיכוני סחר, סיכוני מטבע, סיכונים טכנולוגיים, סיכוני תדמית ותקשורת, סיכוני סייבר ורבים אחרים. יצירת קטגוריות הסיכונים אפשרה וחייבה לקבוע מיהו הגורם הארגוני האחראי לסיכון בתחום זה או אחר וסייעה בהערכה וניהול הסיכונים, לפי סוגיהם.

בנוסף, תורת הסיכונים אפשרה את ההבנה שניהול והערכת הסיכונים אינם רק בתחום תפקידם ואחריותם של גורמי בקרה, גורמי מקצוע וגורמי ניהול בארגון, אלא שהאחריות הכוללת היא עניינה של ההנהלה הבכירה ביותר ושל הדירקטוריון, במיוחד באשר להתמודדות עם הסיכונים החיצוניים המשפיעים על הארגון ומחייבים מענה מורכב-אסטרטגי.

בחלוף הזמן גם הובן שיש השפעות לוואי ואינטראקציה בין הסיכונים: סיכון תפעולי עלול להפוך לסיכון תדמיתי, רגולטורי ומשפטי, עד להתהוות סיכון אסטרטגי שיפגע בהשגת יעדי הארגון ולעתים אף בעצם קיומו. האירוע בחברת "רמדיה" יצרנית מזון לתינוקות (שנחשף בנובמבר 2003) הוא דוגמה מוחשית להתממשות "חזון גוג ומגוג" מעין זה.

סיכונים מורכבים | סיכונים משולבים

השפעות הלוואי בין סיכונים והגברת העוצמה של סיכון אחד על משנהו, יצרה עולם מונחים של "סיכונים מורכבים" - "סיכונים משולבים". המשמעות התפעולית והניהולית היא שאין לבחון סיכונים רק בקטגוריה המצומצמת שלהם (כסיכונים תפעוליים; סיכונים פיננסיים ועוד), אלא נדרש לראותם בפרספקטיבה מורכבת וכוללת ויש להתערב בזמן כדי למנוע העצמת תוצאות הלוואי העלולות להיווצר מסיכון אחד על משנהו. ניתן לדמות תופעה לקוביות דומינו הנופלות בזו אחר זו. התופעה מחייבת חיזוי, הערכת ההסתברות והנזק של הסיכון המשולב, והתערבות בטרם יהפכו הסיכונים לסיכונים אסטרטגיים.

סיכונים פורצים

תחום חדשני נוסף של תורת הערכה וניהול הסיכונים הוא תחום "הסיכונים הפורצים" - סיכונים חדשים המפתיעים ארגונים שאינם ערוכים אליהם "EMERGING RISKS". תופעת "הסיכונים הפורצים" הועצמה מאוד בשלהי המאה ה-20, ובמיוחד במאה ה-21 בעידן "הכפר הגלובלי". לדוגמה, משבר הסאב-פריים שפרץ בארה"ב (ביולי 2007) הפתיע את הממשלות ואת העולם העסקי, נמשך שנים רבות, והשלכותיו ניכרות עד היום; המשבר הפיננסי באיחוד האירופאי שעדיין עמנו; ירידה בצמיחה בסין נתנה אותותיה לא רק בסין אלא במיטב הכלכלות, הבורסות ועולם העסקים; ירידת מחיר הנפט פגעה בכלכלות ובתעשיות (כמו תעשיית הנפט) אך מינפה כלכלות ותעשיות אחרות (כמו תעשיית התעופה); שינויים גיאופוליטיים (כמו עליית האסלאם הרדיקלי ועמו הגירת תושבים) מובילים לתוצאות כבדות משקל; שינויים חברתיים המוליכים לשינויים כלכליים רגולטוריים וצרכניים, למשל בישראל - מחאת הקוטג' ועמה מסקנות ועדת טרכטנברג, ועדת שישינסקי, רגולציה ענפה כנגד ריכוזיות, מאבק ב"פירמידות" והגברת התחרותיות. יש להביא בחשבון גם שינויים דמוגרפיים-חברתיים-כלכליים רבים שהואצו במאה ה-21 (כמו עליית תוחלת החיים ומשבר הפנסיה). הכפר הגלובלי אף מעצים ומשנע בין היבשות תופעות ביולוגיות-רפואיות על מכלול השפעותיהן הרפואיות והכלכליות, כמו נגיף האבולה, נגיף הזיקה, שפעת החזירים והעופות - שהפכו מאירוע מקומי לאירוע גלובלי; התפתחויות טכנולוגיות (הסלולר, האינטרנט, פייסבוק, טוויטר, אינסטגרם), אפשרו פיתוח כלכלי-

תקשורתי אך גם הביאו לתופעות כמו ה"שיימינג". תופעה זו יוצרת היום סיכון אסטרטגי חדש-לא רק לפרט אלא גם לארגונים. התפתחויות טכנולוגיות אלו יצרו גם סיכון חדש - סיכון הסייבר, שהוא בגדר סיכון פורץ המשנה במהירות את תכונותיו ואת שיטות התקיפה שלו, ומבחינת עוצמתו הוא סיכון אסטרטגי.

הנה כי כן, ארגונים עסקיים ולא עסקים מהירים שמייצרים חדשות לבקרים סיכון חדש - סיכון פורץ ההופך לסיכון אסטרטגי, על מכלול תופעותיו.

מכאן, שמועצות מנהלים והנהלות, גורמי בקרה וניהול חייבים לעסוק בחיזוי, בהערכה ובניתוח שוטפים-תקופתיים כדי להיערך למצבים העלולים לייצר סיכונים פורצים - סיכונים אסטרטגיים עבור הארגון.

ניתן לדמות זאת לפעולת מודיעין והערכה של צה"ל, שבו מיטב גורמי המודיעין עוסקים באיסוף, ניתוח והערכת מידע, ממגוון רחב של מקורות מידע. גורמים אלה מייצרים לצה"ל הערכה מודיעינית על הסיכונים-האיומים הצפויים שעמם יש להתמודד, וממנה צה"ל גוזר תכניות עבודה כדי לתת מענה אסטרטגי ותפעולי לסיכונים (איומים בעגה הצבאית).

כך גם מועצות מנהלים, הנהלות בכירות וזוטרות, גורמי הערכה וניהול של סיכונים וגורמי בקרה. כל אלה חייבים ליזום, לייצר ולהפעיל מערכי חיזוי והערכה של סיכונים, ובמיוחד סיכונים מורכבים, פורצים, וסיכונים אסטרטגיים, ולהיערך מראש לתת להם מענה.

סקר סיכונים אסטרטגיים בראייה עולמית

סקר שנערך בשנת 2013 בקרב 300 מנהלים ברחבי העולם העלה כדלקמן:

- הגדרה רחבה של הסיכון האסטרטגי: "כל דבר, כל מכשלה, כל נושא שעלול לפגוע, באופן מהותי, בהשגת היעדים האסטרטגיים".
- נושא הסיכונים האסטרטגיים קיבל מעמד מועדף מקרב כלל סוגי הסיכונים שעמם מתמודדים הארגונים.
- **23%** מהמשתתפים בסקר השיבו שהנושא של הסיכון האסטרטגי וההתמודדות עמו הוא באחריות המנהל הכללי (CEO) **19%** - של הדירקטוריון; **25%** - של ועדת סיכונים מיוחדת מטעם הדירקטוריון. יתר האחריות, לדברי המשתתפים בסקר שלעיל, מוטלת על ועדה ארגונית בתוך הארגון או באחריות של גורמים אחרים בארגון.
- מתוצאות הסקר עולה שסיכוני תדמית-תקשורת (רשתות חברתיות) צוינו כגבוהים מבין הסיכונים האסטרטגיים.
- **94%** מהמשתתפים בסקר ציינו שבשלוש השנים הקודמות לסקר, הסיכונים האסטרטגיים כבר חייבו שינויים ארגוניים קונספטואליים בגישה להתמודדות עמם.
- **תוצאות תפעוליות-ניהוליות - פעולות שכבר ננקטו על ידי המשיבים בסקר בהקשר של סיכונים אסטרטגיים:**

» ההתייחסות לסיכונים האסטרטגיים והערכת תוצאותיהם הפכה לחלק בלתי נפרד מהליך התכנון והאישור של התכניות האסטרטגיות-עסקיות, שבאות למעשה גם לתת מענה לסיכונים אלה.

» בהתאם - חל שינוי באסטרטגיה העסקית של 91% מהארגונים עקב סיכונים הנובעים מהאצת השימוש בכלים טכנולוגיים: סיכוני רשתות חברתיות, סיכוני מערכות סלולאריות, סיכוני "התפוצצות המידע וזמינותו" (BIG DATA).

» גברה חשיבות האיסוף, הניתוח והערכת המידע בעולם העסקי ממגוון מקורות המדיה הזמינים ולא רק מקרב לקוחות הארגון. מידע זה אמנם קל לאיסוף אך מורכב לנתח ולהעריך.

» ירדה חשיבותו של הניתוח הפיננסי - ההסתמכות על נתונים כספיים-חשבונאיים המספקים מידע על ביצועי העבר ועל העמידה בתכניות העבודה, אך אינם מספקים מידע על הסיכונים בעתיד. לשון אחר - לדעת משתתפי הסקר, הכלים הכספיים-חשבונאיים חשובים לשימור ערך (VALUE) ארגוני-כלכלי ולאו דווקא לפיתוח ערך חדשני.

» מהסקר עולה שהארגונים השקיעו משאבים ויצרו כלים חדשים ושיטות להתמודדות עם הסיכונים האסטרטגיים, ובהם: חלק מהארגונים הקצו משאבים והגבירו את תכיפות הערכת הסיכונים (52%); חלקם דאגו לאיסוף מתמיד ומתמשך של מידע בנדון (43%); חלקם הרחיבו את מספר המנהלים שתפקידם לעסוק בסיכונים (38%).

- כלי נוסף להתמודדות עם העולם המשתנה במהירות, על הסיכונים הכרוכים בו, אינו מוזכר בסקר אך עולה בניירות עמדה ומחקרים אחרים.

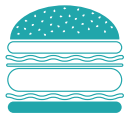
כלי זה עוסק בהרכב הדירקטוריון:

» הגישה החדשנית טוענת כי דירקטוריון המורכב רובו ככולו ללא איזון מגדרי ומההיבט המקצועי מאנשי כספים, רואי חשבון ומשפטנים אינו המענה הנכון-המאוזן, ויש לשלב בו מגוון חברים מדיסציפלינות שונות (שיווק, מדיה, חברה, גורמים מגזריים).

» טענה אחרת מתייחסת למשך הכהונה הארוך מדי של דירקטורים, וכי ההתמודדות עם העולם המשתנה במהירות מחייבת ריענון שורות לאחר כהונה אחת בת כמה שנים ספורות.

חיזוי והערכות לסיכונים אסטרטגיים דוגמאות והמחשות מתחום המזון

חברת מקדונלד'ס



דוגמה טובה להמחשת תהליכים וכלים של חיזוי, הערכות מראש ומתן מענה אסטרטגי, תפעולי ושיווקי לסיכונים אסטרטגיים היא חברת מקדונלד'ס הבינלאומית - מתחום המסעדנות. נכון ל-2016, החברה מעסיקה 420,000 עובדים במשרה מלאה, העובדים ביותר מ-36,000 מסעדות ברחבי העולם.

תחום המזון רווי סיכוני תפעול, סיכוני בריאות ואיכות מזון, יחד עם סיכונים רגולטוריים, ולא פחות - סיכוני תקשורת ותדמית. מדובר ב"סיכונים פורצים" לתודעת הציבור, "סיכונים מורכבים" המשלבים סיכון מתחום הייצור ובקרת איכות המזון עם סיכוני תדמית, דרך חשיפה תקשורתית, ועמם סיכון רגולטורי. כל אלה יחד מהווים "סיכון אסטרטגי" לחוסנו ולשרידותו של הארגון, שבמונחים ציוריים נמצא במוקד הרעש - ב"רעידת אדמה" ארגונית.

חברת מקדונלד'ס צלחה סיכונים כאלה וערכה עלה במהלך השנים: בסוף 2006 ערך המניה עמד על 42 דולר, ובסוף אוגוסט 2016 עמד על כ-115 דולר. מדובר במגמה, סדורה ונמשכת של עליות בעשור של טלטלות כלכליות, פיננסיות, חברתיות ורגולטוריות רבות עוצמה.

זו דוגמה להפקת לקחים למתמודדים עם סיכונים אסטרטגיים, במיוחד בתחום המזון: כיצד צלחה חברת מקדונלד'ס תקופה ארוכה של סיכונים אלה? וכיצד "מגמות המזון הבריא" בתקשורת, ברשתות החברתיות ואצל הרגולטורים, שייצרו סיכון מהותי בתחום המזון, לא פגעו משמעותית בהישגי החברה?

הכרת מגמות השוק בראשית התהוותם, לימוד והכרת הסיכונים האסטרטגיים - הסיכונים הפורצים, הערכות ארגונית בתחומי המחקר ותכנון, שימת דגש על יצירתיות, חדשנות ושיווק. כל אלה עשויים ליצר אסטרטגיה נכונה כמענה לסיכונים העומדים בפני החברה

התשובה היא בחיזוי - במודיעין עסקי, תכנית אסטרטגית, היערכות מול סיכונים ופעולות שיווק שהחברה עשתה:

- מאז הקמתה בשנת 1940 פעלה חברת מקדונלד'ס באמצעות אסטרטגיות שיווקיות: מזון זמין-מהיר להגשה וצריכה, מגוון מוצרים לא גדול, מחיר זול, הפצה באמצעות זכיינים, שילוב נערים ונערות במכירה. דרכה של מקדונלד'ס לא הייתה סוגה בשושנים: כנגד החברה עלו במהלך השנים טענות כבדות משקל ובהן: פגיעה בבעלי חיים, זיהום הסביבה, ניצול כוח עבודה זול בשכר לא נאות, וטענות למזון משמין הפוגע בבריאות החברה אף הסתבכה במשפטי דיבה, כשהיא תובעת גורמים שלכאורה פגעו בשמה. פגיעה תקשורתית תדמית ניכרת בחברה חלה בשנת 2004, כשהופק סרט על תרומתה לתופעת השמנת היתר -OBESITY - סרט שפגע קשה בתדמיתה.
- הסיכונים האחרונים שלעיל: הטענות בדבר פגיעה של החברה בבריאות הציבור ובדבר איכות המזון שהיא מציעה - המחישו לחברה באופן ברור וחד את הסיכונים האסטרטגיים שעליה להתמודד עמם. ניתן לומר שבכך הוצב בפני החברה "קו פרשת המים". כתשובה אסטרטגית לסיכונים מהותיים-מוחשיים אלה הציבה החברה, החל משנת 2004 ואילך, מענה מהותי: החברה הייתה הראשונה - "חלוץ לפני המחנה" - בתחום המזון הבריא. מקדונלד'ס השקיעה משאבים, שילבה מחקר ופיתוח ופעלה לייצר ולשווק מזון איכותי יותר.

להלן כמה מהשינויים שהחברה יישמה ומיישמת: הפחתה ניכרת בקלוריות ובשיעור השומנים, הוספת ירקות טריים בשיעור ניכר, השבחת הלחמניות ללחם מלא, הפחתת סוכרים, הפחתת נתרן (מלח), החלפת השמן לטיגון, שימוש בבשר ללא חומרים משמרים וללא אנטיביוטיקה, פרסום של קלוריות לכל רכיב ורכיב, מסע פרסום - "מקדונלד'ס, לא מה שחשבתם" המשווה בין מוצרי מזון הנחשבים כדלי קלוריות (כמו פריכיות, דגני בוקר) לעומת ערכי הקלוריות של מוצרי

החברה, כמו גם שינוי אריזות וצבעים תוך שימוש בצבע ירוק ולבן. כל אלה יצרו מסר ברור ובולט - מוצרי החברה עומדים באופן נאות בתחרות על בריאות הציבור ואיכות המזון.

אין כוונה לשווק במאמר את החברה, אלא את "מרשם הקסם" להצלחתה, את הגישה הניהולית ואת האסטרטגיה שצלחה ושיש ללמוד ממנה: הכרת מגמות השוק בראשית התהוותם, לימוד והכרת הסיכונים האסטרטגיים - הסיכונים הפורצים, הערכות ארגונית בתחומי המחקר ותכנון, שימת דגש על יצירתיות, חדשנות ושיווק. כל אלה עשויים ליצר אסטרטגיה נכונה כמענה לסיכונים העומדים בפני החברה.

חברת פרוטארום

מהזווית המקומית, ניתן להציג גם דוגמה ישראלית מצליחה - חברת פרוטארום העוסקת בייצור ושיווק חומרי-גלם לתעשיית הטעם והריח ותערובות טעם וריח לתעשיות המזון והקוסמטיקה. פרוטארום היא אחת מ-10 החברות הגדולות בעולם בתחום זה. ערך מניותיה בבורסה עלו מסוף 2011 לסוף 2016 בשיעור של פי 5.8. האסטרטגיה של החברה: רכש חברות בעולם בעלות יתרון של מוצרים טבעיים-בריאים יותר, ודגש על פיתוח מוצרים בעלי רכיבים טבעיים ובעלי ערך בריאותי גדול יותר. בדוח הכספי של החברה לסוף 2015, בפרק העוסק על התפתחותה ועל האסטרטגיה של החברה, מופיעה המילה "טבעי-טבעיים" 28 פעמים; והמילה "בריאות -בריא" מופיעה 12 פעמים. יש כאן המחשה ברורה ומוצלחת של גילוי מוקדם של המגמות ושל הסיכונים האסטרטגיים למפעל.

חברת החלב "טרה"

זאת דוגמה ישראלית נוספת: החברה הפכה סיכון לסיכוי; החברה קבעה תכנית אסטרטגית שמיצבה את עצמה ואפשרה לה להתמודד מול ענקיות החלב, זאת בין היתר באמצעות אסטרטגיה של "מזון בריא" שהיא אימצה: מוצרי גבינה ללא חומרים משמרים (לדוגמה, גבינת נעם). אסטרטגיה זאת יחד עם תכנון, מחקר, ייצור ושיווק נתנה מענה לציבורים רחבים בחברה הישראלית ואפשרו לטרה לנגוס בנתח השוק על חשבון המתחרות ולבסס את עצמה כמותג מוכר ומוביל.

מול החלוציות ומול הרף המצליח BENCHMARK שממנו ראוי היה ללמוד, ניתן להציב שורה ארוכה (ועצובה) של חברות שלא היו ערות למגמות ולסיכונים ושנפגעו באופן מהותי.

בישראל למשל ניתן להציב את חברות הבשר המעובד, חברות הפסטרמה, ש"לא ראו את הכתובת על הקיר" - כתובת המזון הבריא נטול חומרים משמרים. תעשיות אלה לא נערכו כראוי ונפגעו קשות במכירותיהן. הן חוו ירידה של כ-30% במכירות בשנה האחרונה. חוסר ערנות, חוסר חיזוי וחוסר היערכות גרמו לשגיאות אסטרטגיות, כשהאחראים להן הם הדרג המפקח והמנהל הבכיר בחברות אלה, כולל הדירקטוריונים וההנהלות.

סיכונים אסטרטגיים | סיכונים פורצים | הקונספציה והכלים של המבקר הפנימי לבדיקה והערכה

בביקורת "מקובלת" שעיקרה ביקורת ציות, עומדים בפני המבקרים הפנימיים כלים וסרגלים ברורים הנמצאים "בשדות החרושים היטב" של הביקורת המסורתית: מגוון נהלים והחלטות. לעומת זאת, בבדיקות "מתקדמות", כאשר בדיקת נושא הסיכונים האסטרטגיים והפורצים היא בוודאי בתחום חדשני ומתקדם, עומד המבקר הפנימי נבוך מעט. הכלים המקובלים, הנהלים וההנחיות הארגוניות בתחום הסיכונים האסטרטגיים והסיכונים הפורצים אינם קיימים, או שהחלו בהקמתם, ביסוסם ויישומם רק לאחרונה, כך שהמבקר חסר סרגלים וחסר ממד של זמן להעריך את תקפותם ואת תרומתם של הנחיות ונהלים שזה עתה מיושמים.

מכאן שתפקידו של המבקר הפנימי בנושא זה אינו במישור ביקורת הציות. תפקידו נמצא במישור הסקירה, ההערכה ובמישור ההמלצה. בהעדר סרגלים, הנחיות ונהלים ברורים, בתחום הסיכונים האסטרטגיים והפורצים, כמו גם בתחומים חדשניים אחרים, תפקידו של המבקר הוא ללמוד, לסקור, לנתח, ובעיקר להשוות - לייצר BENCHMARKS - לארגונים אחרים, למחקרים ומאמרים; לראיין ולשאול מקבלי החלטות בארגון: דירקטורים, מנכ"ל, הנהלה בכירה, מנהל הסיכונים ועוד רבים אחרים, וכך ליצור, בזהירות הראויה, תובנות מסתמנות המחייבות דיון והתלבטות, סוגיות רלוונטיות, כיווני מחשבה, כיווני פעולה, לקחים שהופקו או יש להפיק, להצביע על "חללים" - "לאקונות", שיש בארגון מי שסובר שקיימות, ועוד.

זהו תפקידו של המבקר הפנימי בשלב הראשוני של הערכת הסיכונים האסטרטגיים, כמענה לסיכונים הפורצים. המבקר אמור לתרום בשאלותיו לסוגיות המחייבות מחשבה ובחינה, לרבות באשר לשאלות שאף כי לובנו ייתכן שטרם מוצו.

לשון אחר - מהותה של הבדיקה של המבקר הפנימי אינה בהצבעה מקובלת על ממצאים-ליקויים, אלא דווקא במישור ההערכה, התובנות, ההכוונה, ההמלצות והייעוץ - דרך השאלות וההמלצות. אכן, מדובר בשיטה שונה של בדיקה ושל דיווח!

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."

Best Practice - ניהול סיכונים

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.

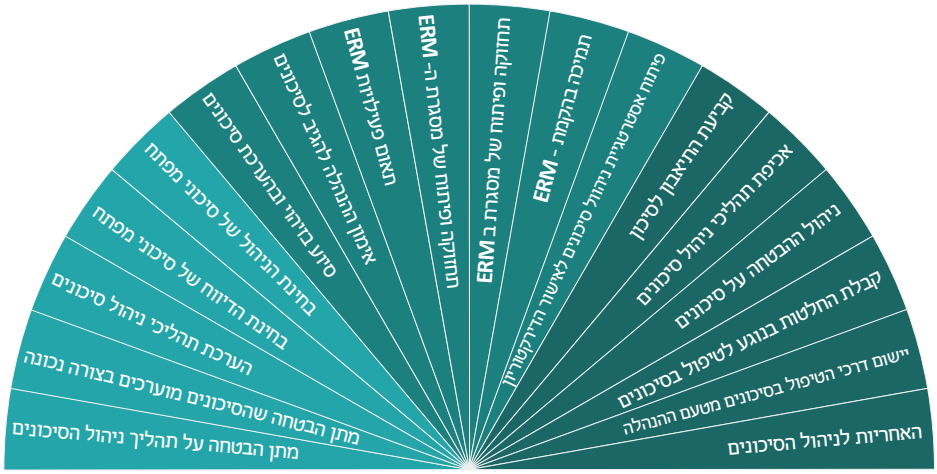
חוק הביקורת הפנימית קובע כי "המבקר הפנימי יערוך את הביקורת על פי תקנים מקצועיים מקובלים". מכיוון שתקנים אלו נקבעים ומעודכנים באופן שוטף על ידי ה-IIA, אשר מאפשר סיוע של המבקר הפנימי להנהלה בתחומים נוספים, חוק הביקורת הפנימית מאפשר סיוע של המבקר הפנימי לארגון בתחום ניהול הסיכונים.

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 שיאויש 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. אל למבקר הפנימי לבצע את הפעילויות המופיעות מימין, כיוון שהן כרוכות בנטילת אחריות ניהולית. עליו לבצע את הפעילויות המופיעות משמאל, כחלק מתפקידו כמבקר פנימי. הפעילויות שבמרכז מסייעות להנהלה בהיבט ניהול סיכונים, הן לגיטימיות לביצוע על ידי המבקר הפנימי בתנאי עמידה בכלל אי התלות ובהינתן שיש בידיו את הכישורים המקצועיים לבצען.



תפקידים שעל הביקורת הפנימית להימנע מלעסוק בהם

תפקידים לגיטימיים של הביקורת הפנימית, אם נוקטים אמצעי ביטחון

תפקידי ליבה של הביקורת הפנימית בנוגע - ERM

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 בארגון. 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 שפונקציית 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.

המבקר הפנימי בין הנהלה ודירקטוריון בחברה ממשלתית

מאת **לילי אילון**, רו"ח, MBA

לחברות הממשלתיות בישראל משקל ניכר במשק הישראלי. מהמאזן של ממשלת ישראל עולה כי היקף נכסיהן מהווה כשליש מנכסי המדינה והן אמונות על היבטים משמעותיים וחיוניים ביותר לקיומם ולאיכות חייהם של אזרחי ישראל. על רקע זה נמצאות החברות הממשלתיות במוקד הדיון הציבורי במדינה, ונשמעת ביקורת ציבורית לא מעטה באשר לכשלים בפעילותן ובהתנהלותן. במקרים מסוימים בשנים האחרונות, הגיעו הכשלים עד הביקורת הפנימית בחברות עצמן, כך למשל בחברת נתיבי ישראל, חברת החשמל וחברת נמל אשדוד.

עוד טרם הוגדר המונח "ממשל תאגידי", הבינה רשות החברות הממשלתיות כי ריחוקו של בעל השליטה (המדינה) ממנהליו יוצר סיכון של זליגת משאבים, של פעילות לא יעילה או לא אפקטיבית, ואף יש חשש לפגיעה בטוהר המידות

לאורך השנים היוותה הביקורת הפנימית בחברות הממשלתיות את אחד הנדבכים העיקריים בפעילותה של רשות החברות הממשלתיות (להלן הרשות או רשות החברות), והמבקרים הפנימיים נתפסו כשומרי הסף העיקריים בחברות וכזרועה הארוכה של רשות החברות.

הסיבה העיקרית לכך היא שהרשות, כנציגת המדינה שהיא בעלת השליטה בחברות, הבינה כי לאור היעדרו של בעל שליטה פעיל בחברות, ולאור הפער הקיים בינה כנציגת המדינה, כלומר "נציגת הבעלים", לבין החברות, נוצר סיכון מהותי כי החברות לא ישיגו את מטרותיהן. עוד טרם הוגדר המונח "ממשל תאגידי", הבינה רשות החברות הממשלתיות כי ריחוקו של בעל השליטה (המדינה) ממנהליו יוצר סיכון של זליגת משאבים, של פעילות לא יעילה או לא אפקטיבית, ואף יש חשש לפגיעה בטוהר המידות. לפיכך, מבראשית ניתן לראות כי רשות החברות הממשלתיות תפסה את הביקורת הפנימית כאורגן הכרחי ומשמעותי בחברות.

חוק החברות הממשלתיות 1975 תשל"ה

היה החוק הראשון במדינת ישראל שבו קבעה המדינה את חובת קיומה של ביקורת פנימית בגוף כלשהו. בהתאם, החוק קובע כי:

סעיף 48: "הדירקטוריון של חברה ממשלתית ימנה לחברה מבקר פנימי, זולת אם אישרה הרשות שהיקף פעולות החברה או אופיין אינו מחייב מינוי של מבקר פנימי"

סעיף 49: "(א) הדירקטוריון יקבע את סמכויותיו ותפקידיו של המבקר הפנימי. (ב) המבקר הפנימי יהיה כפוף ליושב ראש הדירקטוריון ולמנכ"ל ויגיש את דו"חותיו והצעותיו לדירקטוריון."

בהמשך, כבר בשנת 1992, פרסמה רשות החברות הממשלתיות חוזר לחברות בשם "נוהל ביקורת פנימית בחברות ממשלתיות ובת ממשלתיות". שוב הייתה זו רשות החברות הממשלתיות חלוצת הרגולטורים בהתייחסות לנושא ומתוך שאיפה להתמודד עם נושא הביקורת הפנימית בצורה רחבה וכוללת.

החוזר ("הנוהל") קובע מסמרות באשר לאופן קיום הביקורת הפנימית: הנוהל מגדיר ומרחיב מהי ביקורת פנימית. הוא קובע את אופן מינויו של המבקר, ובין היתר קובע כי המבקר הפנימי ימונה על ידי הדירקטוריון בהמלצת ועדת הביקורת ובהתייעצות עם המנכ"ל, ומתווה את הליך מינוי המבקר. הנוהל קובע כי יהיו למבקר ההשכלה, הניסיון והכישורים המתאימים לתפקיד זה והוא יוגדר כפקיד בכיר. הדירקטוריון הוא זה שקובע את היקף העסקתו של המבקר ואת אופן סיום עבודתו. את תכנית העבודה של המבקר הפנימי תאשר ועדת הביקורת והדירקטוריון. יישמרו אי תלותו של המבקר הפנימי ועובדיו. בנוסף, מפרט הנוהל את תפקידיו וסמכויותיו של המבקר הפנימי.

הנוהל אף עוסק בוועדת הביקורת: מגדיר את הרכב הוועדה, קובע את היחסים בינה לבין דירקטוריון החברה והנהלת החברה, קובע את תפקידיה וסמכויותיה של ועדת הביקורת, מפרט את עבודת הדירקטוריון בעניין הביקורת הפנימית ומסיים בחובת הדיווח לרשות החברות הממשלתיות. הנה כי כן, בחוזר זה התמודדה רשות החברות בצורה מוצלחת עם מרבית היבטי הממשל התאגידי בקשר עם הביקורת הפנימית. זאת, מספר עשורים לפני שהוגדר במדינת ישראל מושג "הממשל התאגידי" ועוגנה בחוק ובתקנות.

מקצוע הביקורת הפנימית בעולם התקדם בצעדי ענק והוסדר בתקנים מקצועיים. הביקורת הפנימית בחברות הממשלתיות בישראל לא נותרה מאחור: כך למשל, בשנת 2010 פרסמה רשות החוזר בנושא מינוי המבקר הפנימי ובדיקת איכות הביקורת הפנימית בחברות הממשלתיות "מינוי מבקר פנימי ובדיקת איכות הביקורת הפנימית בחברות הממשלתיות". חוזר זה נכתב לאורו של תקן 1312 של ה-IIA.

מטרת החוזר הייתה לחזק את עצמאותו ואי-תלותו של המבקר הפנימי, ולשפר שיפור מתמיד את איכות הביקורת הפנימית בחברות הממשלתיות.

החוזר מרענן את נוהל מינוי המבקר הפנימי ואופן העסקתו. וחשוב לא פחות, הוא מחדש בכך שהוא קובע את חובת ביצועו של הליך בדיקת איכות הביקורת הפנימית: הליך זה הינו מערכת בדיקות הנעשות על ידי גורם חיצוני במטרה לבחון האם מטרות הביקורת הפנימית הושגו ובאיזו מידה, האם היא פעלה באופן אפקטיבי וביעילות, והאם מערך הביקורת הפנימית בחברה תִפקד באופן מיטבי. ככל שהתשובה לשאלות אלו או חלקן היא לא, יש לבדוק ולברר מהן הסיבות והגורמים לכך ומהן ההמלצות לצורך שיפור הביקורת הפנימית בחברה.

על פי החוזר, ההליך כולל שני נדבכים:

הנדבך הראשון - מתייחס למערך הביקורת הפנימית בחברה. על פיו יש לבדוק את הממשק בין ועדת הביקורת למבקר הפנימי ובין אורגנים נוספים בחברה לבין המבקר הפנימי. כמו כן, יש לבחון את הממשק בין הנהלת החברה והדירקטוריון למבקר הפנימי ואת טיפולם בסוגיות שהועלו על ידי המבקר הפנימי וועדת הביקורת.

הנדבך השני - בדיקת איכות הביקורת הפנימית. נדבך זה מתייחס לשאלת עבודתו ותפקודו של המבקר הפנימי וצוותו. על פיו יש לבחון שאלות בנוגע ליחידת הביקורת ולעובדי הביקורת - מידת הכשרתם והתאמתם למטלות הנדרשות, אופן הטיפול בניגודי עניינים; המתודולוגיה ואופן הביצוע של הביקורת הפנימית - האם נעשים בהתאם לתקנים מקצועיים מקובלים ולחוזרי הרשות.

בשנת 2011 פרסמה רשות החברות הממשלתיות את "חוזר חברות ממשלתיות - דוחות" (2011). החוזר מאגד את חובות הדיווח של החברות הממשלתיות ומבטא את התייחסותה של הרשות לחובות הביצוע שהוחלו על החברות בהיותו אחד מכלי האכיפה שבידי הרשות. שהתווה ועיגן את חובות הדיווח של החברות הממשלתיות. בחוזר זה הוקדשו מספר פרקים גם לביקורת הפנימית, ובהם הובעה מדיניות הרשות באשר למכלול ההיבטים הקשורים בביקורת הפנימית בחברות הממשלתיות, וכן חוזקו הקביעות וההוראות בשני חוזרי הביקורת הפנימית שסקרתי לעיל.

בחוזר זה מקבעת הרשות, כמי שנושאת בשם המדינה בכובע הבעלים בחברות הממשלתיות, את מעמד הביקורת הפנימית בחברות ואת החשיבות שהיא מייחסת לביקורת הפנימית. הדבר נעשה בדרך של הוראה על דיווח לרשות בקשר עם התנהלות הביקורת הפנימית בחברה הממשלתית. החוזר שואף להגברת השקיפות באשר לתפקוד המבקר, כמו גם לתפקוד הדירקטוריון וההנהלה, בכל הנוגע לביקורת הפנימית: מעמד, משאבים, שיטות עבודה ועוד. יצוין כי הדרישות הללו גם מגבירות את חובת הנשיאה באחריות (ACCOUNTABILITY) של המבקר הפנימי, ולא פחות של ההנהלה והדירקטוריון, בכל הקשור לביקורת הפנימית. להלן אפרט את עיקרי הדברים שאליהם מתייחס החוזר.

על פי חוזר זה, יש לדווח על אופן העסקתו של המבקר הפנימי כפקיד בכיר (חוק החברות הממשלתיות (החוק) מגדיר נושאי משרה בחברה שהינם "פקידים בכירים" - באשר אליהם קובע החוק כי הדירקטוריון יאשר את מינוים ויקבע את תנאי העסקתם).

בחוזרים שהוציאה רשות החברות הממשלתיות היא מביעה את עמדתה באשר לחשיבות הביקורת ולמעמדו של המבקר, תוך שהיא פועלת לחיזוק מעמדו של המבקר. מעטים הם הרגולטורים האמונים על חוק הביקורת הפנימית המייחסים חשיבות כה רבה לביקורת הפנימית.

על קשרים אחרים שיש לו (ככל שישנם) עם החברה הממשלתית על מנת לשלול זיקות שיביאו למצב של ניגוד עניינים, היקף העסקתו של המבקר הפנימי, ואם צומצם - פירוט הסיבות לכך על מנת להביא לכך כי המבקר הפנימי יזכה לזמן הנדרש לו לביצוע עבודתו כנדרש. יש לפרט את התקנים המקצועיים המקובלים שעל פיהם עורך המבקר הפנימי את תכנית הביקורת, ואם יש אי עמידה בתקנים יש לפרט את הסיבות לכך, יש לציין את המועדים שבהם הוגשו ממצאי הביקורת ליו"ר הדירקטוריון, ליו"ר ועדת הביקורת ולמנהל הכללי, את המועדים שבהם התקיים דיון בוועדת הביקורת או בדירקטוריון, ואם לא התקיימו יש לפרט את הסיבות לכך. נדרשת התייחסות פוזיטיבית של הדירקטוריון לשאלה האם היקף, אופי ורציפות פעילות המבקר הפנימי ותכנית עבודתו סבירים בנסיבות העניין, ויש בהם כדי להגשים את מטרות הביקורת הפנימית בחברה. בנוסף, יש לצרף לדוח על עבודת הדירקטוריון גם דוח של המבקר הפנימי על ביצוע תכנית עבודה שנתית. בדוח זה יפורטו המסקנות וההמלצות של המבקר הפנימי הנובעות מעבודת הביקורת שביצע בחברה, יפורט המעקב שמבצע הדירקטוריון אחרי עבודת תיקון הליקויים שהועלו על ידי המבקר הפנימי, ועדת הביקורת, דירקטוריון החברה וועדות אחרות של הדירקטוריון, והמעקב שמבצע הדירקטוריון אחר תיקון ליקויים שהועלו על ידי מבקר המדינה, רשות החברות הממשלתיות, רואה החשבון המבקר וגורמי ביקורת מוסמכים אחרים. כמו כן יפורטו ממצאי דוח מעקב של המבקר הפנימי לגבי נושאים שלא נבדקו ולא טופלו כנדרש בתכנית העבודה התלת שנתית של המבקר הפנימי ובחוזרי הרשות, או שהתגלו בהם ליקויים שטרם תוקנו לדעתו או לדעת ועדת הביקורת או הדירקטוריון. יובא תיאור מתוך דוח המבקר הפנימי לגבי עבודות שביצע ושלא נכללו בתכנית העבודה השנתית או בדוחות המעקב האמורים או סטייה מהם. בתיאור יפורטו מהות השינויים והסיבה לשינויים, יצורפו תכנית הביקורת הפנימית המעודכנת ונוהל הביקורת הפנימית בחברה.

יודגש כי רשות החברות הממשלתיות מביעה בחוזר זה (שכאמור הוא חוזר דיווח ועניינו בגילוי ושקיפות) את עמדתה באשר לחשיבות שהיא רואה בביקורת הפנימית. פירוט העניינים שעל החברה בכלל ועל הדירקטוריון וועדת הביקורת בפרט לדווח עליהם הוא נרחב ביותר ומקיף את מכלול עבודת המבקר הפנימי ומערך הביקורת הפנימית. מעטים הם הרגולטורים האמונים על חוק הביקורת הפנימית המייחסים חשיבות כה רבה לביקורת הפנימית.

על חשיבות הביקורת הפנימית בכלל ועל בקרת איכות הביקורת הפנימית בפרט בעיני רשות החברות, ניתן ללמוד גם מהחוזר שפורסם בשנת 2014. עיקר חשיבותו של החוזר הוא בכך שהוא קובע כי רשות החברות עצמה תקיים בדיקת איכות לביקורת הפנימית במספר חברות ממשלתיות בכל שנה. חוזר זה נועד לתת מענה לצורך בשיפור הביקורת הפנימית במקום שבו רשות החברות סבורה כי הדירקטוריון לא יקיים את הבדיקה כהלכתה.

השינוי ההכרחי הבא שיש לעשות בנוגע לביקורת הפנימית הוא בכפיפותו של המבקר הפנימי. התפישה העומדת בבסיס חוק החברות הממשלתיות כי ניתן לנהל ביקורת פנימית תוך כדי כפיפות כפולה של המבקר הפנימי אינה מתיישבת עם המציאות.

בחוזר זה לוקחת הרשות אחריות נוספת על קיומה של ביקורת פנימית אפקטיבית בחברות. היא אינה מסתפקת עוד באכיפה פסיבית אלא עושה צעד אל עבר האכיפה האקטיבית. הרשות מחילה חוזר שלה על עצמה וקובעת כי חלה עליה החובה להיות ערנית, ובמקום שבו התהליכים אינם מתקיימים כשורה עליה לנקוט צעד פעיל לשיפורם. אציין כי רשות החברות לא פרסמה מידע באשר לתוצאות בדיקותיה עד כה.

ניתן לסכם בכך כי לאורך השנים פעלה רשות החברות באופן שיטתי ומהותי לחיזוק הביקורת הפנימית ומעמד המבקר הפנימי. ניכר, כפי שפורט לעיל, כי הלכה למעשה התקדמה והתפתחה הביקורת הפנימית בחברות הממשלתיות באופן עקבי ומתמיד ובצורה המשקפת הבנה עמוקה של רשות החברות באשר למקצועיותו ולתפקידו של המבקר הפנימי כשחקן מרכזי בעולם החברות הממשלתיות.

בחוזרים שהוציאה רשות החברות הממשלתיות היא מביעה את עמדתה באשר לחשיבות הביקורת ולמעמדו של המבקר, תוך שהיא פועלת לחיזוק מעמדו של המבקר. מעטים הם הרגולטורים האמונים על חוק הביקורת הפנימית המייחסים חשיבות כה רבה לביקורת הפנימית.

טרם תמה המלאכה:

המלאכה לא הושלמה. השינוי ההכרחי הבא שיש לעשות בנוגע לביקורת הפנימית הוא בכפיפותו של המבקר הפנימי. חוק החברות הממשלתיות קובע כי המבקר הפנימי יהיה כפוף למנכ"ל וליו"ר הדירקטוריון. זו תקלה. התפישה העומדת בבסיס חוק החברות הממשלתיות כי ניתן לנהל ביקורת פנימית תוך כדי כפיפות כפולה של המבקר הפנימי אינה מתיישבת עם המציאות. בעיקר במקום שבו "מאבק השליטה", המוכר מעולמן של החברות הציבוריות, לובש בחברות הממשלתיות צורה של מאבק בין המנכ"ל לבין יו"ר הדירקטוריון. במצבים כאלה הופך המבקר הפנימי במקרים מסוימים לכלי בידי השניים המנסים לעשות בו שימוש זה כנגד זה. תוך כדי כך הם מטילים עליו מטלות לא ענייניות, הופכים אותו לשק חבטות, פוגעים בקיומה של תכנית הביקורת ופוגעים במעמדו של המבקר.

הפתרון בעיניי הוא הכפפתו המקצועית של המבקר ישירות ליו"ר הדירקטוריון ולוועדת הביקורת בלבד. בעניין זה יש ללכת בעקבות חוק החברות הקובע בסעיף 49 כי: "המבקר הפנימי יגיש לאישור הדירקטוריון או לאישור ועדת הביקורת, כפי שייקבע בתקנון, או בהעדר הוראה בתקנון, כפי שיקבע הדירקטוריון, הצעה לתכנית עבודה שנתית או תקופתית, והדירקטוריון או ועדת הביקורת, לפי העניין, יאשרו אותה בשינויים הנראים להם". כלומר, הכפיפות המקצועית של המבקר היא לוועדת הביקורת ולדירקטוריון, ובכך מדיר החוק את הנהלת החברות מהתערבות בעבודת המבקר הפנימי.

לדעתי, זהו הדבר הנכון והנדרש, על מנת להביא הן להפעלה מיטבית של המבקר על ידי ועדת הביקורת והן למצב של תפקוד אפקטיבי שלו כשומר סף בחברות הממשלתיות.

מדור המגזר השלטוני - דיון על השחיתות השלטונית בישראל

מאת **בועז ענר**, רו"ח, MA, CIA

מבוא

מרכז המידע והמחקר של הכנסת הגדיר שחיתות ציבורית כ"שימוש בלתי הולם במשרה ציבורית במטרה לקדם אינטרסים פרטיים" ("גופים להתמודדות עם שחיתות ציבורית במדינות שונות", מרכז המידע והמחקר, 16.11.15). בפברואר 2016 ערכה הוועדה לענייני ביקורת המדינה של הכנסת דיון שכותרתו: "בקשה לחות דעת מבקר המדינה בנושא: השחיתות השלטונית בישראל וטיפול רשויות החוק בסוגיה".

עיקרי הדיון:

בהלך הדיון עלה הצורך בגוף מתכלל, ובלשון יו"ר הוועדה - ח"כ אלהרר: "משרדים ממשלתיים בגדול לא יודעים לדבר אחד עם השני... נניח שקיבלתם תלונה, איך המשרדים הממשלתיים משלבים כוחות ביניהם... הגיע הזמן לעשות ניתוח מקיף ולהסדיר את הסוגיה".

נציגת הפרקליטות הסתייגה והציעה חלופה: "לחשוב האם נכון לעשות איזשהו הליך של כמו ועדה מתמדת כזאת (גוף או הליך), שיתכלל ויסתכל באופן רוחבי יותר ובאופן יותר רשמי על מה שנעשה היום ובאופן יותר סדור ושיטתי".

במהלך הדיון עלתה הצעה חלופית: למסד "שולחן עגול", שבו ייפגשו מעת לעת היועץ המשפטי לממשלה ונציגי משרד המשפטים עם נציגי מבקר המדינה, מבקרים פנימיים במגזר השלטוני, חשבים וגזברים בשלטון המקומי, גורמי מודיעין וחקירה משטרתיים ועוד. מפגשים אלה יאפשרו לאפיין מגמות בשחיתות הציבורית ופרצות שיש למנען, להחליף מידע, ולהגביר שיתוף פעולה בין-ארגוני במאבק.

במהלך הדיון שנערך בפברואר 2016 בוועדה לענייני ביקורת המדינה של הכנסת עלה הצורך בגוף מתכלל: ובלשון יו"ר הוועדה, ח"כ אלהרר: "משרדים ממשלתיים בגדול לא יודעים לדבר אחד עם השני... נניח שקיבלתם תלונה, איך המשרדים הממשלתיים משלבים כוחות ביניהם... הגיע הזמן לעשות ניתוח מקיף ולהסדיר את הסוגיה"

"לא עכברא גנב אלא חורא גנב"

באשר לשחיתות שלטונית, במיוחד בשלטון המקומי, בדיון הומחשה הטענה שחסרה ראייה מערכתית: כבר היו חקירות רבות ובמשך השנים כבר נצברו פסקי דין רבים המרשיעים ראשי ערים וסגניהם בשחיתות שלטונית. יש בכך הישג אבל המאפיין של ההליכים הללו הוא מרוץ אחר מי ש"גנב" - אחרי "העכבר", ולמיטב ידיעת עורך המדור, באותן שנים לא מומש הליך מקיף-חקיקתי שהוליך לסגירת הפרצות באמצעות חוק או בתקנות, מלשון מניעת "הפרצה הקוראת לגנב".

סוף דבר...

סיום הדיון קראה הוועדה לחשיבה מחודשת על הדרך הנכונה למלחמה בשחיתות.

עוד סוכם, שהוועדה תֻפנה בבקשה לראש הממשלה ולשרת המשפטים כדי לקבל בתוך חודש (עד ליום 22 במארס 2016) את התייחסותם לנושא הקמת הגוף המתכלל.

האם בעקבות הדיון יתחיל שינוי מחשבתי-תהליכי? האם יוקם גוף מתכלל או לפחות יחל מיסודו של "שולחן עגול" בין-ארגוני? האם יואצו הליכים לאיתור הפרצות ותואץ הרגולציה להסדרה? ימים יגידו...

מדור היתולי

מיומנה של מבקרת פנימית

מאת: רונית שורצל, MA - בנק הפועלים

מבקרים פנימיים
חובת ההוכחה מוטלת עלינו

אנו נדרשים להוכיח ללא הפסקה שאנחנו בקיאים, מעודכנים, שולטים בנושאים הרלוונטיים, עוסקים רק בעיקר, ובאופן כללי "מבינים עניין".

כדי שיתייחסו במלוא הרצינות לדברינו, כלומר כדי שנהיה אפקטיביים, עלינו לעמוד על המשמר ללא הרף. להכיר את ההיסטוריה, להיות מעודכנים בנעשה כעת, ולצפות את פני העתיד. הארגון מעריך ביקורת רק אם עומדים מולו אנשי ביקורת מצוינים. כלומר - "אפס סובלנות" לטעויות.

ועדיין, גם אם עשינו את כל זה - למדנו, שיננו, חקרנו, בדקנו, קראנו, שאלנו, חפרנו, מצאנו והמלצנו - יש סיכוי סביר שנקבל מהמבוקרים כתף קרה. להלן התגובות השכיחות:

"נו טוב, לכם יש זמן..."

"אתם לא מבינים כלום!"

"אתם רק מסרבלים את התהליך!"

"שנתון לא יבוים לתצוגה כל מילה שיוצאת מהפה..."

"איך תבינו? אתם הרי לא מטפלים בלקוחות..."

וגם:

"אתם לא יחידה יקרת רוח. אתם רק מפריעים לנו לעבוד רווחים"

"לא צריך לשמור אוניברסיטה בשביל להמליץ על מתשלם הביקורת"

"אתם רק מייקרים לי את עבודה"

"לכם לקח חצי שנה לעשות ביקורת, ומעניין אתם מבקשים תצפות בתוך שבועיים..."

נשמע מוכר, נכון?

וכשהמבוקרים חושבים שאנחנו לא שומעים, הם יצירתיים אפילו יותר. לאחרונה הגיע אלינו מייל עם תגובה לטיוטת דוח ביקורת. בשרשור הפנימי בין המבוקרים כתב מבוקר אחד לאחר: *"בהבלאתה עם הרטלון בקריאת הדוח"*.

(בהיעדר בקרה על המייל היוצא, הורדנו למבוקר ציון בסעיף 'בקרות'...)

שאלת השאלות היא: כיצד רותמים את המבוקר? כיצד גורמים לו להגיע להכרה (בלי לערפל את הכרתו) שאולי יש משהו בהמלצות שלנו; ש"אורח לרגע רואה כל פגע"; שמטרתנו היא לשפר דברים בארגון, לטובת כולנו?

התשובה בעיני היא

ש"ש

כלומר:

אפשרות א' | **ש**עות **ש**נתיות.

מינימום שעות ביקורת שנתיות בהחלט ישפרו את שביעות רצון המבוקרים.

אפשרות ב' | **ש**ם **ש**מים (אם לא יעזור לא יזיק)

אפשרות ג' | **ש**קיפות ו**ש**ירות. כלומר: לא עוד מבקרים "שושואיסטים", השומרים על ריחוק, מגיעים בהפתעה חמושים במשקפי שמש כהים בסגנון האחים בלוז. להיפך - תכנית עבודה שנתית נשלחת מראש ליחידות המבוקרות, והמבקר מגיע חמוש בחיוך בלבד.

ועוד | ממצאים מתוקשרים באדיבות, אף פעם לא דוחים בקשה להיפגש, ולא פוסלים על הסף שינוי אדרת לאותה גברת (כלומר, ניתן לתאר ממצא בכמה דרכים).

האם כל זה יעזור לשיפור הממשק מבקר-מבוקר? לא בטוח. לפרקים נראה שכן, לעתים לא.

לפעמים נדמה שהכול רגוע, עד שמגיעה מעטפה שעליה כתוב: *"לכבוד רונית שוורץ, המחלקה לביקורת"...*

או מישהו שמציג אותי במילים אלו: *"תכירו, צוות רונית מהמחלקה ל..... אני נורא קשה לי להגיד את המילה..."*

במקרים כאלה אני נושמת עמוק, סופרת עד 5, מנצלת את התחמושת שהבאתי (החיוך, זוכרים?) וממשיכה לעשות את עבודתי בצורה הטובה ביותר. אה, ומתייקת לעצמי את האירוע בפנקס הקטן שבראש, על כל מקרה. אולי יהיה לזה שימוש פעם. הרי בינינו, מי מבקר את המבקר?

ועל כך בטור הבא.

היחידה ללימודי המשך ולימודי חוץ | אוניברסיטת חיפה | University of Haifa Division of Continuing Education & Extension studies

IIA ישראל
איגוד מבקרים פנימיים בישראל
Institute of Internal Auditors in Israel

לימודי הסמכה למקצוע הביקורת הפנימית CIA

תכנית הכנה לבחינות - CIA מבקר פנימי מוסמך

חלק 1 | חלק 2 | חלק 3

מועד פתיחה התכנית | 15/11/16

מנהל התכנית | ד"ר גבי סייג

תפקיד המבקר הפנימי הינו אחד מכלי הניהול העיקריים, המרכזיים והחשובים ביותר, בידי כל הנהלת ארגון, ובשנים האחרונות תלותה של ההנהלה בתוצריו ובאמירותיו הולכת וגוברת משנה לשנה.

יעוד ותפקידי הביקורת הפנימית עוברים מהפכה מהותית בשנים האחרונות. מ"ביקורת ציבורית" שהייתה נחלתה הבלעדית כמעט של מוסדות ממשלה ומדינה, הפכה זו להיות ל"ביקורת ניהולית" במשמעותה המקיפה והמלאה, לטובת כלל הארגונים והגופים העסקיים והציבוריים במשק. משכך גבר הצורך הממשי של ארגונים בכל הסקטורים - במבקרים פנימיים בעלי הכשרה מתאימה.

בישראל, קיימת חובה לקיים ביקורת פנימית על ידי מבקר פנימי בכל גוף ציבורי. חובה זו מעוגנת בחוק הביקורת הפנימית. בגופים פיננסיים כמו בנקים וחברות ביטוח וכן גם בגופים נוספים (רשויות מקומיות, חברות ממשלתיות ועוד) ישנה חובה למנות מבקר פנימי מכוח החוקים אשר מסדירים את פעילותם של גופים אלה.

ביוזמה משותפת של ד"ר גבי סייג ו-IIA ישראל - איגוד מבקרים פנימיים בישראל, מציעה היחידה ללימודי המשך ולימודי חוץ - אוניברסיטת חיפה - קורס הכנה לבחינות להסמכה בינלאומית למקצוע הביקורת הפנימית CIA שנותנת מענה לשינויים המהותיים במקצוע הביקורת הפנימית.

מטרת התכנית

הקורס יאפשר לתלמידים להירשם ולהיבחן לבחינות המסמיכות לשם קבלת הסמכת CIA. מבקר פנימי מוסמך (CIA) הינה ההסמכה הבינלאומית המוכרת היחידה אשר האוחזים בה יכולים להפגין את יכולתם המקצועית. הסמכת ה-CIA - הינה יתרון מקצועי בעל ערך למבקרים פנימיים בכל הדרגים, למנהלי סיכונים ולכל אלה העוסקים במקצוע ביקורת פנימית.

למי מיועדת התכנית

ההסמכה המתוכננת מיועדת לבוגרי תכנית מבקרים פנימיים של היחידה ולבוגרי תכניות מבקרים דומות ולאלה העוסקים במקצוע ביקורת פנימית (מבקרים פנימיים, עובדי ביקורת ורואי חשבון העוסקים בביקורת).

* נרשמים לתכנית יזומנו לראיון אישי

מבנה התוכנית

קורס ההכנה לבחינות CIA כולל תכנים בתחומי תקני הביקורת הפנימית, עולם הסיכונים, ניהול הביקורת הפנימית, דיני ביקורת, אתיקה ונורמות בניהול, ביקורת טכנולוגית המידע והסייבר, חשבונאות ניהולית וחשבונאות פיננסית, ביקורת מעילות והונאות ועוד.

לפרטים נוספים: טל': 04-8249111 אימייל: ext-studies@univ.haifa.co.il

חלק 1

6 מפגשים פעם בשבוע של 4 שעות כל אחד + **2 מפגשים** 4 שעות כל אחד לתרגול מבחן חלק 1

נושא א' - ציות לתקני IIA והנחיות

נושא ב' - בקרה פנימית וסיכונים

נושא ג' - עריכת עבודת השטח - כלי ביקורת וטכניקות

חלק 2

6 מפגשים פעם בשבוע של 4 שעות כל אחד + **2 מפגשים** 4 שעות כל אחד לתרגול מבחן חלק 2

נושא א' - עריכת מטלת ביקורת (עבודת שטח)

נושא ב' - עריכת מטלות ביקורת ספציפיות

נושא ג' - מעקב (ניטור) אחר תוצאות הביקורת

נושא ד' - הונאות ומעילות

נושא ה' - כלים שימושיים במהלך עריכת הביקורת

חלק 3

12 מפגשים פעם בשבוע של 4 שעות כל אחד + **4 מפגשים** 4 שעות כל אחד לתרגול מבחן חלק 3

נושא א' - אתיקה עסקית וממשל תאגידי

נושא ב' - ניהול סיכונים

נושא ג' - מבנה ארגוני, תהליכים עסקיים וסיכונים

נושא ד' - תקשורת

נושא ה' - עקרונות ניהול ומנהיגות

נושא ו' - מערכות מידע והמשכיות עסקית

נושא ז' - ניהול פיננסי

נושא ח' - סביבה עסקית גלובאלית

משך הלימודים

תכנית בהיקף של 124 שעות.

הלימודים יתקיימו בימי ג' בין השעות 16:30-19:45

בקמפוס הנמל (רח' הנמל 65, חיפה) * נתון לשינויים

תעודה

לעומדים בדרישות התכנית לרבות נוכחות והשתתפות פעילה במפגשים תוענק תעודה על השתתפות בתכנית הכנה למבחני ההסמכה של ה-CIA מטעם אוניברסיטת חיפה, לימודי המשך ולימודי חוץ.

שכר הלימוד

שכר לימוד לשנת 2016 עבור ההכנה לבחינות CIA

חלקים 1+2+3 כולל תרגול וערכת הלימוד הינו **15,280 ₪**

11 תשלומים ללא ריבית. שכר הלימוד כולל בתוכו ערכת

לימוד, שרכישתה היא חובה, בשווי **900 $**

* שכ"ל אינו כולל דמי רישום בסך **200 ₪**

*שכ"ל אינו כולל דמי רישום למבחני ההסמכה.

*בוגרי תואר אקדמי מאוניברסיטת חיפה/היחידה

ללימודי המשך ולימודי חוץ זכאים ל-10% הנחה בשכ"ל,

במימון פרטי בלבד. שכר הלימוד לבוגרים הינו 13,750 ₪

11 תשלומים ללא ריבית.

הטבות לנרשמים

רישום לקורס יקנה חברות (ללא עלות נוספת) לתקופת הלימודים ב-IIA ישראל- איגוד מבקרים פנימיים בישראל ובלשכת המבקרים הפנימיים העולמית (IIA), בשווי של מעל $200 (כולל מנוי אלקטרוני חינם למגזין Internal Auditor).

שכר הלימוד המשולם על ידי הנרשמים ללימודים כולל ערכת לימוד לבחינות ה-CIA בעלות של כ-$900. רכישת ערכת הלימוד הינה חובה.

ייתכנו שינויים בימי הלימוד | פתיחת התכנית מותנית במספר הנרשמים.

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
SYDNEY, AUSTRALIA / 23-26 JULY 2017

Join Us Down Under And L.I.V.E. The Global Experience!

The IIA's International Conference is returning to beautiful Sydney, Australia, in 2017.

Leadership. Innovation. Value. Effectiveness.

Join us as we host The IIA's 2017 International Conference, 23–26 July in Sydney, Australia. You'll embark on an educational journey, rich with insights for internal auditors at every level.

The theme for this year's International Conference is "L.I.V.E. the Global Experience: Leadership. Innovation. Value. Effectiveness." and we will deliver a program that delves into timely issues impacting the profession.

Mark your calendar now and complete the form to sign up to receive exciting conference developments.

Editor's Note

Sharon Witkowski Tabib, CPA

CIA, CRMA

The last few months of the year are the time in which internal auditors prepare the next year's audit plan. This also includes, on top of the audit topics, the audit resource planning, audit tools and techniques and more.

Several questions are raised in that regard: when did we last stop to examine our activities on a strategic level? Have we defined targets to measure our own success as auditors? Have we assessed our strengths and weaknesses?

While a risk-based annual audit plan guides the internal audit throughout the year, a strategic plan leads the way beyond the foreseeable future.

In the 4th issue of "The Internal Auditor journal " - we decided to focus on the continuous evolvement of the profession. A significant part of the current discourse on internal audit deals with the future trends of the profession - where will we be in the future and how we should prepare for it: how can we better meet various stakeholder expectations and be perceived as a "valued bussiness partner"? How can we leverage our bussiness knowledge to enhance compliance and effectiveness in the organizations within which we opreate? How can strategic thinking be developed among the audit team? How can the indistinct boundaries between auditing and consulting be blurred? How do we move ahead, hand in hand with technological changes, and train the internal audit teams for the future?

Today, more than ever, organizations are required to adapt themselves to a dynamic reality and to the unexpected changes that sometimes occur quite rapidly. In such a reality, expectations from the internal audit are gradually increased, and we must continually adjust ourselves to this new dynamic.

This issue addresses, inter alia, analytics innovation in internal audits, as compared to traditional audits. Further emphasis is laid on the indepth understanding of technological risks, cyber and cloud services. We will also focus on risk management and corporate governance, as well as the internal audior's partnership with other "line of defences" bodies within the organization.

I am confident that this issue will help us, the internal auditors, in gearing up for the challenges that lie ahead in the upcoming year.

I wish to express my thanks to the editorial board team members for their perseverance in compiling this issue, and at the time of writing these lines, they are already well into the task of preparing the next issue, entitled: "one step forward".

A special thank you to Margalit Sperber for her notable dedication and contribution to the production of the journal in this format.

At this opportunity, I respectfully wish to ask you, the readers, to join us in taking an active part in shaping our professional landscape.

President's Note

Doron Cohen, CPA

President IIA Israel - Institute of Internal Auditors

In a broad view of the internal audit world we can clearly identify emerging trends that internal auditors will have to face over the next five to ten years. These include volatile risk environment, growing regulatory scrutiny, rising stakeholder expectations, complex technology risks etc

The implication of the above is that the mixture of internal audit work will be changed with increased emphasis on evaluating corporate governance and risk management processes at the expense of traditional controls evaluation and compliance tests. Auditors will have to shift their focus toward evaluation of strategic risks - a topic many of them avoid due to its complexity.

The Internal auditor's desired competency is also undergoing significant changes. -Today, internal auditors are expected to have a versatile skill set, including skills such as high analytical capabilities, critical thinking and IT knowledge.

This issue contains fascinating and innovative articles from Israel and abroad. We hope it will assist you in acquiring a better understanding of the trends impacting the profession in order to adequately prepare yourself for them.

The challenges detailed above require top professional talents. Since the Israeli Internal Audit Law was enacted in 1992, several initiatives were taken to amend it, which are being pursued to this very day. IIA Israel is operating to influence government and regulatory bodies so the amendments to be enacted will help reinforce the internal audit profession, strengthen the status of internal auditors and enhance their professionality.