



עיונים בביקורת הפנימית

צעד אחד קדימה

חידושים בתקנים המקצועיים הבינלאומיים

בקורת ברשויות מקומיות - להבין, לשנות, להשפיע

אירועי "קו פרשת המים" - המחייבים חשיבה מחודשת
על תפיסות מסורתיות בביקורת הפנימית

אפריל
2017

CIA, CRMA, רו"ח, שרון ויטקובסקי טביב	עורכת כתב העת
CIA, CISA, MBA, רו"ח, אורן שחר	סגן העורכת
LLM, CIA, CISA, CRMA, CRISC, רו"ח, דרור בר משה	חברי המערכת
CIA, CRMA, CFE, רו"ח, יוסי גינוסר	
MA, רו"ח, נאוה חלמיש	
רו"ח, ד"ר יוסי נטוביץ	
MBA, רו"ח, עו"ד, ליאור סגל	
D.E.A, ד"ר גבי סייג	
CIA, MA, רו"ח, בועז ענר	
CIA, MBA, עו"ד, ערן שחף	
MBA, CIA, רו"ח, מרגלית שפרבר	
אינה גולדרייטר	מזכירת האיגוד
סטודיו דגה	עיצוב ועריכה גרפית
אודי לוינגר	עריכה לשונית והגהה
IIA ישראל - איגוד מבקרים פנימיים בישראל בע"מ	מו"ל

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

המובע במאמרים מבטא את דעת הכותבים בלבד. אין האיגוד נושא באחריות כלשהי בגין הנכתב בהם.

כל הזכויות שמורות ל- IIA ישראל - איגוד מבקרים פנימיים בישראל. ט.ל.ח.

דברים	2
2 דבר הנשיא	
3 דבר העורכת	
4 משולחן האיגוד	
עדכונים	8
8 חידושים בתקנים המקצועיים הבינלאומיים	
14 מדור מחקרים אקדמיים בתחומי הביקורת הפנימית	
טכניקות וכלים בביקורת הפנימית	18
18 התרומה הנסתרת במעבר מביקורת מסורתית לביקורת מתמשכת	
ממשל תאגידי	24
24 בחזרה ליסודות - תרגולת שריפה	
28 עולם של חיבורים	
34 האם יש קשר בין גודל מחלקת הביקורת לרמת הבשלות שלה?	
מערכות מידע	38
38 להיות חכם, ולא רק צודק: היערכות ארגונים למתקפת סייבר	
44 מדור טכנולוגיות מידע	
ניהול סיכונים	46
46 ניהול סיכונים ארגוני - סדק בתודעה	
ביקורת במגזרי פעילות יחודיים	50
50 ביקורת ברשות המקומית - להבין, לשנות, להשפיע	
54 הפקת תובנות ממקבץ דוחות ביקורת פנימית	
56 מדור ביקורת במגזר השלטוני	
מעילות והונאות	58
58 אירועי "קו פרשת המים" המחייבים חשיבה מחודשת על תפיסות מסורתיות בביקורת הפנימית	
62 הפולیגרף ככלי מסייע בעבודת המבקר הפנימי הלכה למעשה	
דעות ובלוגים	66
66 מיומנה של מבקרת פנימית - טור מס' 3	
70 ביקורת על ספרים - כשהמנכ"ל חוצה קווים אדומים	
Notes	74
Editor's Note	74
President's Note	75



דבר הנשיא

דורון כהן, רו"ח

נשיא IIA ישראל - איגוד המבקרים הפנימיים

בכנס הביקורת הפנימית שהתקיים בחודש ינואר השנה נבחרתי לכהונה שנייה כנשיא האיגוד. אני רואה בזאת זכות גדולה ומודה לחברי האיגוד על האמון. במהלך כהונתי הראשונה ביסס האיגוד את מעמדו כגוף המקצועי הגדול ביותר של מבקרים פנימיים בישראל.

מספר החברים שולש והוא עומד כיום על כ-800 חברים. ההשתלמויות, ימי העיון, וההסמכות המגוונות שמארגן האיגוד הן המובילות והמוערכות ביותר. חוזקו הקשרים עם לשכות מקצועיות ברחבי העולם, והאיגוד זכה להכרה כאיגוד מוביל. בשנת 2016 זכינו לארח מבקרים פנימיים מקניה שבאו להשתלם פה, ומבקרים ממדינות אחרות השתתפו בהשתלמויות שקיימנו בארץ. גם הקשר עם הרגולטורים וגופי השלטון בארץ חוזק בצורה משמעותית.

האיגוד מפרסם כתב עת מקצועי המתפרסם בקביעות וזוכה להערכה רבה, משיא תרומה נכבדה למבקרים הפנימיים ולעוסקים בתחומים משיקים ומעלה את קרנו של המקצוע. על כל אלה, אני מוצא חובה נעימה להודות, בכל לב, לעמיתי להנהלת האיגוד ולדירקטוריון שלו, המשקיעים ממיטב זמנם ומרצם ועושים לילות כימים לקידום המקצוע.

בתקופה הקרובה ימשיך האיגוד לפעול לחיזוק מעמדו של המבקרים הפנימיים באמצעות קידום והשפעה של יוזמות חקיקה, ובראשן תיקון חוק הביקורת הפנימית שמלאו 25 שנה לחקיקתו.

אנו שוקדים על שדרוג משמעותי של אתר האינטרנט של האיגוד. האתר יהווה בית למבקרים הפנימיים בישראל, יגבש קהילה מקצועית ויתרום להעשרת הידע של כל אחת ואחד מאתנו.

חג שמח וכשר לכל החברים, לבני משפחותיהם ולכל בית ישראל.



דבר העורכת

שרון ויטקובסקי טביב, רו"ח
CIA, CRMA

נושאו של גיליון זה של כתב העת "עיונים בביקורת פנימית", החמישי במספר, הינו "צעד אחד קדימה", ובמסגרתו תוכלו לקבל סקירה מאנשי המקצוע המובילים בתחומם אודות עיסוקי "המבקר הפנימי של המחר", שעבורנו זה כבר היום.

בנוסף, בגיליון זה תוכלו להתרשם ממחקרים אקדמיים חדשים בתחום הביקורת הפנימית, מתהליכי ניהול סיכונים המשולבים בעבודת הביקורת הפנימית באופן חדשני ומנושאי ניהול ידע, וזאת לצד מיומנויות וכלים שימושיים, ובהם התקנים המקצועיים של ה-IIA ובחינת השימוש בפוליקרף לצרכים שוטפים.

מאתגר - כבר אמרנו?

בגיליון הבא נעשה עוד צעד קדימה, ונדון בנושא "המבקר כשותף עסקי?". אין ספק שזו שאלה מעניינת ומאתגרת מאוד.

תודה ענקית מוקדשת לחברי המערכת, שלא התפשרו במהלך הכנת הגיליון והוצאתו לאור. אני חבה חובה נעימה להודות למרגלית שפרבר על תרומתה המשמעותית לשדרוג הגיליון למתכונתו החדשה, ולכם הקוראים שלנו שמתעניינים, מאירים ומגיבים - זה חשוב לנו.

אתם מוזמנים להצטרף אלינו, לקחת חלק פעיל בעשייה המקצועית של כתב העת, להתבטא ולהשפיע.

בהתקרב חג פסח מאחלת לכם ולבני משפחותיכם חג פסח שמח.

עד לא מזמן נושאי הביקורת הפנימית היו מקובעים למדי, ובכל שנה כללו פחות או יותר את אותם נושאים ואת אותן שיטות לביצוע הביקורות.

ובכן, נגמר!

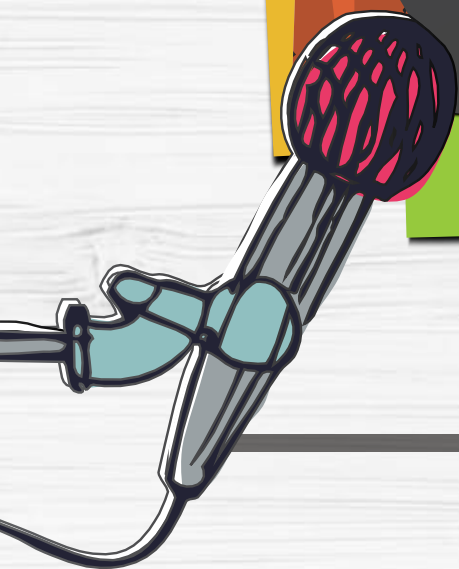
הפעילות העסקית היא דינמית ומשתנה כל העת, דבר המחייב אותנו כמבקרים פנימיים להשתנות בהתאם. היריעה קצרה מלהכיל את כל הדוגמאות מהשנים האחרונות, אבל אפשר להזכיר את הביקורות לגבי פעילות מדיה, דיגיטל, IoT, FinTech, סייבר ועוד.

המגמות הבולטות שבהן המבקר נדרש לספק ערך כבר היום או בעתיד הלא רחוק, כוללות תחומים כמו שיטות דיווח חדשות של ממצאי הביקורת הפנימית, כדוגמת "ביקורת מתמשכת" המוצגת בגיליון זה, כמו גם שימוש רחב בכלים מתקדמים כדוגמת "אנליטיקס" שהוצג בגיליון הקודם. כלים אלו מאפשרים לערוך ביקורת יעילה ואיכותית בכל נקודת זמן ולהגיע לממצאים החשובים במינימום משאבים.

מגמה נוספת שאליה נדרש המבקר הפנימי לשים לב היא התרבות הארגונית, המהווה סיכון מובנה בפעילויות הארגון, נמצאת בלבו של תהליך קבלת ההחלטות בארגון, ומתגלה כסיכון קריטי בארגונים שבהם התרבות הארגונית היא חזקה. דוגמה מובהקת לכך היא "אירוע פולקסווגן" המתואר בגיליון זה.

עדכונים

משולחן האיגוד



לחברות פיננסיות סיכוי של 50% לקבלת קנס

כשיש להן יותר מ-2,000 תלונות של צרכנים
לועד ההגנה הכלכלית של הצרכן בארה"ב
(CFPB)

לחברות סיכוי של 41% לקבלת קנס

כאשר הן אינן מצליחות לתת מענה ליותר
מ-100 תלונות צרכנים בטווח של 15 ימים

"הדו"ח הזה מדגיש את הסינרגיות בין
רמה גבוהה של תלונות צרכנים על
החברה לבין היתכנות של פעולת CFPB
נגד החברה", אומר אלכס בידין, מנכ"ל
PerformLine

Source: Performline, Risk Signals
From the CFPB's Consumer
complaint Database

פוליסת ביטוח לחשיפת סייבר

יותר חברות פונות לביטוח סייבר

מספר הארגונים הרוכשים ביטוח סייבר עלה בכ-30% ב-2016,
לפי מחקר שנערך לאחרונה על ידי החברה לניהול סיכונים
וביטוח (RIMS). תוצאות סקר הסייבר של RIMS ב-2016
מראות ש-80% מהחברות שנסקרו קנו פוליסת סייבר
עצמאית, בהשוואה למעט למעלה ממחצית החברות ב-2015.

RIMS סקרה 272 מומחי סיכונים ממגוון רחב של תעשיות.
כ-70% מצביעים על כך שהם מעבירים את סיכון הסייבר
לצד ג', עלייה של למעלה מ-10% ביחס לשנה הקודמת.
יתרה מכך, 24% אומרים שהם יוציאו יותר ממיליון דולר
השנה להגנות אבטחת סייבר, כולל פוליסת הביטוח שלהם,
ניטור אקטיבי וניתוח של אבטחת מידע, הדרכת עובדים
ואמצעי סריקה. 23% משלמים יותר מ-500 אלף דולר בגין
פרמיית הביטוח לבדה.

המשיבים ציינו נזק תדמיתי (82%), עלויות הכרוכות בהתרעות
(76%) והפרעות לעסקים בעקבות השבתות רשת (76%)
כדאגות מרכזיות שלהם בתחום אבטחת הסייבר - ד. סליירנו.

בעלי מניות מדברים

דירקטוריונים מרגישים לחץ גובר מצד משקיעים פעילים

כיום המשקיעים מפעילים יותר השפעה על דירקטוריונים מאי פעם, לפי סקר שנתי של דירקטורים בתאגידים שבוצע ע"י PwC ב-2016. הסקר, בו השתתפו 884 דירקטורים בחברות ציבוריות, מצביע על כך שדירקטורים מושפעים יותר מלחץ המשקיעים במספר רב של נושאים הקשורים לממשל התאגידי, לרבות הצעת דירקטורים חדשים, שינוי הרכב הדירקטוריון ומתן עדיפות גבוהה יותר לגיוון הדירקטוריון.

"המודל המתרכז בדירקטוריון, אשר התחזק בשנות ה-90 בעקבות מספר שערוריות תאגידיות, ממשיך לפנות את מקומו לטובת מודל המתרכז במשקיע", אומרת פאולה לופ, ראש מרכז תובנות הממשל של PwC.

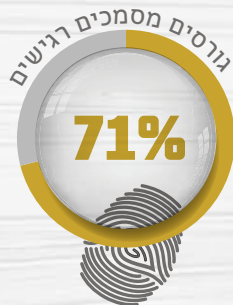
"כתוצאה מכך, קולם של המשקיעים ממשיך להתגבר, ודירקטוריונים אינם יכולים להתעלם מהם יותר. המשקיעים רוצים אחריות מוגברת ודגש חזק יותר על שקיפות בקבלת החלטות וביצוען".

על אף שחיפוש דירקטורים חדשים אינו מתרחק מגבולות חדרו של הדירקטוריון, ניתן לחוש במגמה של שינוי. 18% מהדירקטורים שהשתתפו בסדר פונים להמלצות המשקיעים בחיפוש אחר חבר דירקטוריון חדש - עלייה מ-11% ב-2012 - בעוד ש-87% יבקשו המלצות מעמיתיהם בדירקטוריון. 61% העידו כי צירפו דירקטור עם כישורים ספציפיים עקב לחץ מצד המשקיעים ו-46% צירפו חברי דירקטוריון מגוונים יותר.



האם מבוגרים אמריקאיים מוגנים בפני גניבת זהות?

רבים ממחזיקי (כרטיסי) אשראי מגנים על זהותם, אך עדיין יש כמה פגיעים



הרבה מה לעשות לטובת הגנת המידע

העסקים אינם ערוכים לציית לכללי הפרטיות האירופיים החדשים

יותר מ-80% ממומחי מערכות מידע ועסקים שהשתתפו בסקר אומרים שהם יודעים מעט או לא יודעים דבר על החקיקה החדשה בנושא הגנה כללית על המידע (GDPR) של האיחוד האירופי, אשר אומצה ע"י המועצה האירופית באפריל, כך עולה מסקר הרגולציה להגנה הכללית של המידע אשר נערך על ידי חברת "דל". Dimensional Research סקרו יותר מ-800 משיבים שאחראיים על פרטיות מידע בארגונים המבוססים באזור אסיה פסיפיק, אירופה וארה"ב.

עם כניסתה לתוקפה במאי 2018, החקיקה בנושא הגנה כללית על המידע (GDPR) נועדת לחזק ולאחד את ההגנה על מידע בעבור פרטים באיחוד האירופי, תוך שהיא מפשטת את הכללים לעסקים. עסקים אשר אינם מצייתים לחקיקה עלולים להסתכן בעבירות, קנסות משמעותיים ונזק מוניטין.

כמעט 70% מהמשיבים לסקר אומרים שארגונים אינו ערוך, או שהם אינם יודעים האם הוא ערוך, לעמוד בחקיקה החדשה היום. רק ל-3% מארגוני המשיבים יש תכנית היערכות קיימת. יותר משלושת רבעי מהנשאלים הלא ארופאיים אינם ערוכים לכניסתה של GDPR לתוקף. ארגונים משיבים בגרמניה (44%) הינם הערוכים ביותר לקראת ה-GDPR, בעוד שהארגונים באומות הבנלוקס (בלגיה, הולנד ולוקסמבורג - 26%) הכי פחות ערוכים.

עסקים עדיין נמצאים בחוסר וודאות ביחס לחומרת הקנסות שינבעו מאי-ציות וביחס להיקף השינוי שיידרש להשפיע על העסק שלהם, מצוין הדו"ח. הוא ממליץ לארגונים להתחיל בצעדים הנחוצים כבר עכשיו, לרבות "עיבוי הפתרונות של הארגון לנושא ממשל הרשאות למידע, גישה ניידת מאובטחת, אבטחת דוא"ל ואבטחת היקף הרשתות שלהם" - ניקול ליקורט.

המשקיעים מנצלים את השפעתם בעניין החלטות על הקצאת ההון, נירמול התקשורת בין דירקטורים ומשקיעים, חידוד ביצוע הדירקטוריון, אימוץ מנגנון להעלאת הצעות להצבעה על ידי המשקיעים, הגברת הגילוי במסגרת מנגנון ההצבעה, קידום אופקים אסטרטגיים ארוכי טווח והשפעה על מדיניות תגמול בכירים.

80% מהדירקטורים הסכימו במידה כזו או אחרת כי אקטיביזם של בעלי המניות אילץ אותם להעריך אסטרטגיה, ביצועים והקצאת הון באופן יעיל יותר. "בעלי מניות מחפשים מקום בשולחן הדירקטוריון, תוך שהם שמים את הדירקטורים באור הזרקורים ומובילים לשינוי בנוף הממשל התאגידי", אומרת לופ. - ס.ס.ספי.



Global Council 2/2017

אחת לשנה יש ישיבת Global Council של ה- IIA. הנושאים שעלו בישיבה ב 2/2017 (בה השתתפו דורון רוזנבלום ודורון רונן):

- רישוי
- בדיקת אפקטיביות של הביקורת הפנימית - תקן 1312
- גיוס ושימור חברים
- שדלנות (Advocacy)
- סקר על הנושאים בבחינות CIA

חידושים בתקנים המקצועיים הבינלאומיים

דורון רונן, ר"ח, MA, LLM, CIA, CRMA, QAR, CRISC, CFE

תא

מטרות התקנים הן: לסייע בעמידה בדרישות החובה של מסגרת הכללים המקצועיים, לספק מסגרת לביצוע ולקידום היקף רחב של שירותי ביקורת פנימית מוסיפי ערך, לייסד בסיס להערכת ביצועי הביקורת הפנימית, ולטפח פעולות ותהליכים ארגוניים משופרים.

מקצוע הביקורת הפנימית אינו קופא על שמריו, ולכן גם התקנים המקצועיים מתעדכנים בהתאם להתפתחות המקצוע ולציפיות המשתמשים בתוצריו. העדכון האחרון לתקנים חל בינואר 2017. מאמר זה יסקור את תמצית השינויים והעדכונים שנערכו לאחרונה בתקנים.

התקנים המקצועיים עד יולי 2015

עד יולי 2015, מבנה התקנים המקצועיים כלל את: הגדרת מקצוע הביקורת הפנימית, הקוד האתי, והתקנים המקצועיים (תקני תכונות 1000, ותקני ביצוע 2000). נוסף על התקנים המחייבים כאמור, היו קיימות הנחיות מקצועיות מומלצות מאוד (לא מחייבות): נוהלי ייעוץ (Practice Advisories), הנחיות לפרקטיקה (Practice Guides) וניירות עמדה (Position Papers).

התקנים המקצועיים הבינלאומיים של לשכת המבקרים הפנימיים העולמית (IIA) משמשים בעבודתם כ-193 אלף מבקרים פנימיים חברי ה-IIA, בכ-180 מדינות. תקנים אלה אומצו גם על ידי האו"ם, ה-OECD ו-IFAC (שבהם מדינת ישראל חברה), על ידי ה-EU (שאליו מדינת ישראל נספחת), ועל ידי ה-INTOSAI - איגוד מבקרי המדינה בעולם (שבו חבר משרד מבקר המדינה הישראלי). התקנים נמצאים בשימוש ארגונים בינלאומיים גדולים רבים, כגון הבנק העולמי, וככל שמתרחבת הפעילות הכלכלית הגלובלית, כך גדל מספר המשתמשים. התקנים תורגמו ליותר מ-20 שפות (ובהן עברית), והם יוצרים אחדות מושגית ומקצועית, התורמת רבות לשחקנים בשווקים הבינלאומיים בהערכת האפקטיביות של הביקורת הפנימית בגוף מבוקר.



2015

תמצית השינויים בתקנים המקצועיים החל מיולי

משלימות" (Supplemental Guidance) בהתאמה, כדי לבטא מה כל שכבה כזו אמורה להשיג - סיוע ביישום של התקנים או השלמת המסגרת בדוגמאות ספציפיות. הנחיות היישום וההנחיות המשלימות הן מומלצות (Recommended), להבדיל מ-"Strongly Recommended" לפני השינוי.

• הוצאת ניירות העמדה ממסגרת הכללים (PP) - בראש ובראשונה ניירות עמדה אלו כללו מידע בדבר תפקיד הביקורת הפנימית בארגון. למרות חשיבותם, הם אינם צריכים להיות חלק מהמסגרת המכוונת להנחות את העוסקים במקצוע בהוצאה לפועל של האחריות שלהם.

השינויים העיקריים שבוצעו בתוכן ובמבנה התקנים הם:

- הצגת משימת הביקורת הפנימית המהווה בסיס למסגרת ותומכת בה, כדי לתאר באופן ברור ותמציתי את מטרת העל של הביקורת הפנימית בארגונים שבהם היא פועלת.
- הצגת עקרונות ליבה של הביקורת הפנימית, כדי לבטא את האלמנטים העיקריים המתארים את אפקטיביות הביקורת הפנימית.
- שינוי מינוח ההנחיות - "הנחיות לפרקטיקה" (Practice Guide) ו"נוהלי ייעוץ" (Practice Advisory) ל"הנחיות יישום" (Implementation Guidance) ו"הנחיות

אחרי

The new IPPF 2015

לפני

IPPF (2007-2014)



בגופים רבים המבוקרים על ידי מבקר המדינה, מוטלת על המבקר הפנימי המשימה להוות איש הקשר עם משרד מבקר המדינה, ולעתים אף להיות מעורב בצוות תיקון הליקויים, במיוחד לגבי המעקב אחר תיקון הליקויים. נושא זה, שנמצא שבמחלוקת, נדון בימים אלה בוועדה לענייני ביקורת המדינה בכנסת ישראל.

כידוע, חברי כנסת מגישים הצהרת הון ליו"ר הכנסת, והצהרות אלו חסויות ומופקדות בכספת של יו"ר הכנסת. ברוח עניין זה, לאחרונה נחקק חוק הצהרת הון של בעלי תפקידים בכירים בשירות המדינה, שמכוחו הוטל על מבקרים פנימיים במשרדי ממשלה מסוימים להיות "גורם מפקח" שאצלו יופקדו הצהרות ההון של בעלי התפקידים כאמור, והוא יודא עדכון ועניינים נוספים.

התרחבות מורכבות הארגונים והפיכתם לבינלאומיים, בד בבד עם הגברת הציפיות ממקצוע הביקורת הפנימית והעומדים בראשו, תרמו לכך שמבקרים פנימיים נדרשים לתת ערך מוסף אמיתי לארגון, שמשמעותו היא ייעוץ. חלק מהמבקרים הפנימיים סבורים שאסור למבקר לעסוק ב"יעוץ" לארגון, אולם גם אותם מבקרים פנימיים כוללים בדוחותיהם המלצות, המהוות למעשה סוג של ייעוץ. בשל כך, תוקנו התקנים המקצועיים הבינלאומיים כך שבמקום המילה "ייעוץ" (Consulting), יופיע "מתן עצה" (Advice). לדעתי, בין אם אנו כמבקרים פנימיים מסכימים לכך ובין אם לאו, הציפייה מאיתנו היא להתקדם עם העולם ולדאוג למתן ביקורת בונה עם ערך מוסף לארגון; ביקורת שמלבד הצגת הממצאים, תביא גם המלצות אופרטיביות ותיתן עצה (Advice) ותובנה (Insight).

משימת הביקורת הפנימית Mission Statement

משימת הביקורת הפנימית נועדה לתמוך במקצוע הביקורת הפנימית. היא נועדה לבטא את מה שהביקורת הפנימית שואפת להשיג בארגון.

מיקומה של הצהרת המשימה ב-IPPF מכוון להבהיר כיצד ראוי שהעוסקים בביקורת פנימית ימנפו את המסגרת בכללותה כדי לסייע ליכולת שלהם בהשגת המשימה.

משימת הביקורת הפנימית הוגדרה כדלהלן: לחזק ולהגן על ערך הארגון על ידי מתן הבטחה (Assurance), עצה (Advice) ותובנה (Insight) אובייקטיביים מבוססי סיכון.

השגת המשימה נתמכת באמצעות המסגרת הכוללת - עקרונות הליבה של הביקורת הפנימית, הגדרת מקצוע הביקורת הפנימית, הקוד האתי, התקנים המקצועיים, וההנחיות המקצועיות.

זה המקום להזכיר את הוויכוח עתיק היומין באשר לתפקידיו של המבקר הפנימי: אין חולק כי תפקידו העיקרי (ויש האומרים היחיד) של המבקר הפנימי הוא ביצוע ביקורת פנימית.

חוק הביקורת הפנימית, המיוחד למדינת ישראל, מאפשר למבקר הפנימי, בנוסף על תפקידו ככזה, להיות גם הממונה על תלונות הציבור או הממונה על תלונות העובדים (אם מילוי תפקיד נוסף כאמור לא יהיה בו כדי לפגוע במילוי תפקידו העיקרי).



תוקנו התקנים המקצועיים הבינלאומיים כך שבמקום המילה

לדעתי, בין אם אנו כמבקרים פנימיים מסכימים לכך ובין אם לאו, הציפייה מאיתנו היא להתקדם עם העולם ולדאוג למתן ביקורת בונה עם ערך מוסף לארגון; ביקורת שמלבד הצגת הממצאים, תביא גם המלצות אופרטיביות ותיתן עצה (Advice) ותובנה (Insight).

עקרונות הליבה של הביקורת הפנימית (Core Principles)

הצגת עקרונות הליבה של הביקורת הפנימית באה לבטא את האלמנטים העיקריים המתארים את אפקטיביות הביקורת הפנימית. עקרונות הליבה, בכללותם, מבטאים את מועילות (אפקטיביות) הביקורת הפנימית. כדי שפונקציית ביקורת פנימית תיחשב אפקטיבית, ראוי שכל העקרונות יתקיימו ויפעלו באפקטיביות. יישום עקרונות הליבה על ידי מבקר פנימי או יחידת ביקורת פנימית, יכול להיות שונה מארגון לארגון, אך מִכְשָׁל ביישום עיקרון כלשהו עלול להשתמע כי פעילות הביקורת הפנימית אינה אפקטיבית כפי שיכלה להיות בהשגת משימת הביקורת הפנימית.

העקרונות אינם מסודרים לפי סדר חשיבותם, אלא מסודרים בקבוצות כדי לספק פילוח הגיוני:

הצגת עקרונות אלו תקל על העוסקים במקצוע להבין ולהתמקד בנושאים החשובים. העקרונות אמורים גם לייעל את התקשורת עם בעלי עניין, כולל רגולטורים, באשר לעדיפויות המגדירות ביקורת פנימית אפקטיבית.



עקרונות המתייחסים לתוצרים של פעילות הביקורת הפנימית:

8. מספקת הבטחה מבוססת סיכונים.
9. בעלת תובנה, פרואקטיבית (נוקטת יוזמה) וממוקדת בעתיד.
10. מקדמת שיפור ארגוני.

עקרונות המתייחסים לפעילות הביקורת הפנימית ותהליכיה:

4. תואמת את האסטרטגיות, את היעדים ואת הסיכונים של הארגון.
5. ממוקמת באופן הולם בארגון ובעלת משאבים מספקים.
6. מפגינה איכות ושיפור מתמשך.
7. מתקשרת באופן אפקטיבי.

עקרונות המתייחסים למבקר הפנימי כפרט ולפעילות הביקורת הפנימית בכלל:

1. מפגינה יושרה.
2. מפגינה כשירות וזהירות מקצועית ראויה.
3. אובייקטיבית ומשוחררת מהשפעה בלתי הולמת (בלתי תלויה).



לסיכום - לאחר
השינויים (יולי 2015)

2017

תמצית השינויים
בתקנים המקצועיים
החל מינואר

אפשריים אלה, ויכולים לכלול פעילויות כמו הערכה תקופתית של קווי הדיווח והאחריות וכן פיתוח תהליכים חלופיים להשגת הבטחה הקשורה לתחומי אחריות נוספת.

נוסף תת-תקן חדש A3.1130

"תפקידי המבקר הפנימי הראשי מעביר לביקורת פנימית"

פעילות הביקורת הפנימית יכולה לספק שירותי הבטחה במקום שבו קודם לכן ביצעה שירותי ייעוץ, בתנאי שאופי הייעוץ לא פגם באובייקטיביות ובתנאי שהאובייקטיביות של המבקרים המעורבים מנוהלת כאשר מקצים משאבים למטלת ההבטחה.

בביאורים לתקן 1300 | "תוכנית שיפור והבטחת איכות"

נוסף משפט: המבקר הפנימי הראשי צריך לעודד פיקוח מצד הדירקטוריון באשר לתוכנית להבטחת איכות ושיפור.

בביאור לתקן 1312 | "הערכות חיצוניות" נוספו שני משפטים

- המעריך החיצוני חייב להסיק לגבי עמידה בקוד האתי ובתקנים; ההערכה החיצונית יכולה גם לכלול הערות תפעוליות או אסטרטגיות.

תקן 1110 | "אי תלות ארגונית"

"הביקורת הפנימית חייבת להיות חופשית מהתערבות בקביעת היקף הביקורת הפנימית, ביצוע העבודה, ודיווח התוצאות". נוסף משפט: המבקר הפנימי הראשי חייב בגילוי התערבות כזו לדירקטוריון ולדון בהשלכות הנובעות מכך.

נוסף תקן חדש 1112

"תפקידי המבקר הפנימי הראשי מעביר לביקורת פנימית"

כאשר למבקר הפנימי הראשי יש תפקידים או מצופה ממנו לבצע תפקידים ואז אחריות מחוץ לביקורת פנימית, חייבים לנקוט אמצעי זהירות כדי להגביל פגיעות באי התלות או באובייקטיביות.

ביאור - המבקר הפנימי הראשי עשוי להתבקש לקבל תפקידים נוספים ואחריות מחוץ לביקורת פנימית, כגון אחריות על פעילויות ציות או ניהול סיכונים. תפקידים כאלה עשויים לפגום, או להיראות כפוגמים, באי התלות הארגונית של פעילות הביקורת הפנימית או באובייקטיביות של המבקר הפנימי. אמצעי זהירות הם פעילויות פיקוח, שבדרך כלל הדירקטוריון נוטל על עצמו, כדי לטפל בפגמים

- המבקר הפנימי הראשי צריך לעודד פיקוח מצד הדירקטוריון באשר להערכה החיצונית, כדי להפחית ניגוד עניינים נתפס או אפשרי.
- **בתקן 1320 | "דיווח על תוכנית הבטחת האיכות והשיפור"**
- המבקר הפנימי הראשי חייב לדווח להנהלה הבכירה ולדירקטוריון על תוצאות התוכנית להבטחת איכות ושיפור. "לכן נוסף פירוט: הגילוי יכלול:
 - ההיקף והתדירות של ההערכות הפנימיות והחיצוניות.
 - הכשירות ואי התלות של המעריך/ים או צוות המעריכים, לרבות ניגוד עניינים אפשרי.
 - מסקנות המעריכים.
 - תוכניות לתיקון.

תקן 2050 | "תיאום" הפך ל"תיאום והסתמכות"

הנוסח החדש: ראוי שהמבקר הפנימי הראשי יחלוק מידע, יתאם פעילויות, וישקול הסתמכות על עבודתם של נותני שירותי הבטחה וייעוץ פנימיים וחיצוניים אחרים על מנת להבטיח כיסוי נאות וצמצום כפל מאמצים.

ונוסף ביאור: בתיאום פעילויות, המבקר הפנימי הראשי יכול להסתמך על עבודתם של נותני שירותי הבטחה וייעוץ אחרים. יש לייסד תהליך עקבי לביסוס הסתמכות זו, והמבקר הפנימי הראשי יתייחס לכשירות, לאובייקטיביות, ולזהירות המקצועית הראויה של נותני שירותי הבטחה והייעוץ. למבקר הפנימי הראשי צריכה להיות הבנה ברורה של ההיקף, היעדים, ותוצאות העבודה שבוצעה ע"י נותני שירותי הבטחה וייעוץ אחרים. היכן שקיימת הסתמכות על עבודתם של אחרים, המבקר הפנימי הראשי עדיין אחראי ונושא באחריות לוודא שיש תימוכין מספקים למסקנות ודעות אליהן הגיעה פעילות הביקורת הפנימית.

בתקן 2060 | "דיווח להנהלה הבכירה ולדירקטוריון"

- עודכן (בין היתר) הביאור, **ונוסף בו פירוט:** הדיווח והתקשורת של המבקר הפנימי הראשי להנהלה הבכירה והדירקטוריון חייבים לכלול מידע על:
- כתב האמנה של הביקורת הפנימית.
 - אי תלות פעילות הביקורת הפנימית.
 - תוכנית העבודה של הביקורת הפנימית וההתקדמות לעומת התוכנית.

תקן 2100 | "אופי העבודה"

הנוסח החדש: הביקורת הפנימית חייבת להעריך ולתרום לשיפור תהליכי הממשל התאגידי, ניהול הסיכונים ותהליכי הבקרה של הארגון, באמצעות שימוש בגישה שיטתית, ממוסדת ומבוססת סיכונים. אמינות וערך הביקורת הפנימית מתגברים כאשר המבקרים פרואקטיביים, והערכותיהם מציעות תובנות חדשות ומתייחסות להשפעה עתידית.

הערה: התוספת היא לשם התאמה לעקרון ליבה מספר 9.

תקן 2200 | "תכנון מטלת ביקורת"

הנוסח הקיים: "מבקרים פנימיים חייבים לפתח ולתעד 'תוכנית ביקורת' לכל מטלת ביקורת, לרבות מטרות מטלת הביקורת, היקפה, מועדה והקצאת המשאבים". נוסף משפט: התוכנית חייבת להתייחס לאסטרטגיות, ליעדים ולסיכונים הארגון הרלוונטיים למטלת הביקורת.

הערה: התוספת היא לשם התאמה לעקרון ליבה מספר 4.

בתקן 2230 | "הקצאת משאבים למטלת ביקורת"

כתוב כך: "מבקרים פנימיים חייבים לקבוע משאבים הולמים ומספקים להשגת מטרות מטלת ביקורת, ואשר מתבססים על הערכת האופי והמורכבות של כל מטלה, אילוצי זמן וזמינות משאבים".

לכן נוסף ביאור: הביטוי "הולמים" מתייחס לתמהיל הידע, מיומנויות ויכולות אחרות הנדרשים לבצוע מטלת הביקורת. הביטוי "מספקים" מתייחס לכמות המשאבים הנדרשים להשלים מטלת ביקורת בזהירות מקצועית ראויה.

קיימים עדכונים נוספים, רובם טכניים. את התקנים המעודכנים בעברית אפשר למצוא באתר האיגוד (<http://www.theiia.org.il>) בלשונית: תקינה מקצועית.

סיכום

מבקרים פנימיים, עלינו לפעול לפי תקנים מקצועיים שמטרתם בין היתר לשמור עלינו. לכן חשוב להקפיד שעבודת הביקורת תהא לפי התקנים המקצועיים.

מדור מחקרים אקדמיים

בתחומי הביקורת הפנימית

ד"ר גבי סייג

תא

מטרת המדור היא להביא סקירה על מחקרים אקדמיים נבחרים בתחומי הביקורת הפנימית שפורסמו בכתבי עת חשובים על ידי דירוג אקדמי-מדעי (Impact Factor). חקר פונקציית הביקורת הפנימית הוא חשוב מאוד ומקדם את המקצוע באמצעות התובנות הנגזרות ממנו. מדור זה מביא תמצית של שלושה מחקרים: הראשון מציג סיכום על תובנות החקר האמפירי של אפקטיביות הביקורת הפנימית בספרות המקצועית ומציע כיווני מחקר חדשים; השני מתייחס לבדיקה אמפירית של השפעת הביקורת הפנימית על הדיווח הכספי; השלישי מציע מודל קונספטואלי לזיהוי הגורמים המביאים לשינוי ארגוני בסקטור הציבורי ומציג את תרומתה של הביקורת הפנימית לשינוי זה.

חקר פונקציית הביקורת הפנימית הוא חשוב מאוד

ומקדם את המקצוע באמצעות התובנות הנגזרות ממנו

אפקטיביות הביקורת הפנימית | כיווני מחקר חדשים

- הכללת הנושאים העיקריים במודל תוך התייחסות לגורמי מקרו ומיקרו.
- גזירת כיווני מחקר עתידיים העשויים להוסיף להבנה של תרומת הביקורת הפנימית.
- מבחינה פרקטית, מחקר זה יכול לעזור לעוסקים בביקורת פנימית במאמציהם למצב את פונקציית הביקורת בתוך הארגון כפונקציה בעלת זהות ייחודית. המעניין בעבודה זו הוא הסיכום של תוצאות חקר אפקטיביות הביקורת הפנימית עד עכשיו, והבאת כיוונים חדשים להמשך חקר האפקטיביות בעתיד. כמו כן, העבודה מצביעה על שאלות שבכוחן לקדם את ההבנה של פונקציית הביקורת הפנימית ואת יכולתה להביא לשיפור ולהעלאת הערך המוסף שלה.
- מחקר זה מרכז את תמצית תוצאות המחקרים האמפיריים על אפקטיביות הביקורת הפנימית ומצביע על כיווני מחקר חדשים. Rainer Lenz Ulrich Hahn, (2015). "A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities". Managerial Auditing Journal. Vol. 30 Iss 1 pp.5-33
- מחקר זה מציג סקירה של העבודות האמפיריות שהתבססו על ההערכות לגבי אפקטיביות הביקורת הפנימית שמקורן בעבודות המבקרים הפנימיים ("inside - out"), ואלה שיונקות מתוך הפרספקטיבה של בעלי עניין ("outside - in").
- ממצאי המחקר כוללים את הנקודות הבאות:
- זיהוי הנושאים המשותפים בספרות האמפירית בנושא אפקטיביות הביקורת הפנימית.



גורמי מקרו ומיקרו
המשפיעים על אפקטיביות
הביקורת הפנימית

השפעת איכות הביקורת הפנימית על הדוחות הכספיים

כולל לאיכות עבודתה של הביקורת הפנימית; נמדדו גם היבטים שונים לאיכות עבודתה של הביקורת הפנימית (יכולת וכישורים, אובייקטיביות, יסודיות והקפדה בעבודה בשדה); נמדדה גם אופייה של תרומת הביקורת הפנימית להשלמת הדוחות הכספיים (ביצוע עבודה באופן בלתי תלוי ולחלופין סיוע ישיר). תוצאות המחקר הראו שקיים קשר שלילי בין הזמן הנדרש להשלמת הדוחות הכספיים המבוקרים לבין איכות עבודתה של הביקורת הפנימית (IAF Quality).

ממצא מעניין (ראו תרשים) הוא שהצמצום בזמן (t) הנדרש להשלמת הדוחות, גדול יותר כשעבודת הביקורת הפנימית מתבצעת באופן בלתי תלוי מזו של רואה החשבון החיצוני (Independently Performed Work), ולא כסיוע ישיר (Direct Assistance) בכפיפות להנחיותיו של רואה החשבון החיצוני.



מחקר זה עוסק בהשפעת איכות עבודתה של הביקורת הפנימית ותורמתה להשלמה בזמן של הדוחות הכספיים.

Pizzini, M., Lin, S., & Ziegenfuss, D.E. (2015). "The impact of internal audit function quality and contribution on audit delay." Auditing: A journal of Practice and Theory, Vol.34 Iss 1 pp 25-58

עם יישום פרק 404 של חוק סרבנס-אוקסלי המתייחס לבקרה הפנימית, הזמן הנדרש להשלמת הדוחות הפיננסיים המבוקרים גדל באופן משמעותי. פונקציית הביקורת הפנימית (IAF) יכולה להשפיע על הדיווח הכספי ובהמשך על צמצום הזמן הנדרש להשלמתם של הדוחות הכספיים. הרעיון המסדר הוא שמבקרים פנימיים יכולים לסייע להנהלה בקיומן של בקורות פנימיות חזקות, ולסייע למבקרים החיצוניים בתהליך השלמתם של אותם דוחות. בהתאם לכך, מחקר זה בדק באיזה מידה איכות עבודתה של הביקורת הפנימית (IAF Quality) ותורמתה להשלמת הדוחות הכספיים משפיעה על הזמן הנדרש להשלמת אותם דוחות. הבדיקה נערכה באמצעות מדגם של 292 פירמות שלגביהן נאספו מידע ונתונים בשתי תקופות: לפני ואחרי יישום חוק סרבנס-אוקסלי.

בעזרת שימוש בנתוני סקר שנאספו במסגרת סקרי ה-IIA Gain Surveys שנערכו בשנים 2003 ו-2004, פותח מדד

הקשר בין עבודת הביקורת לשינוי ארגוני בסקטור הציבורי

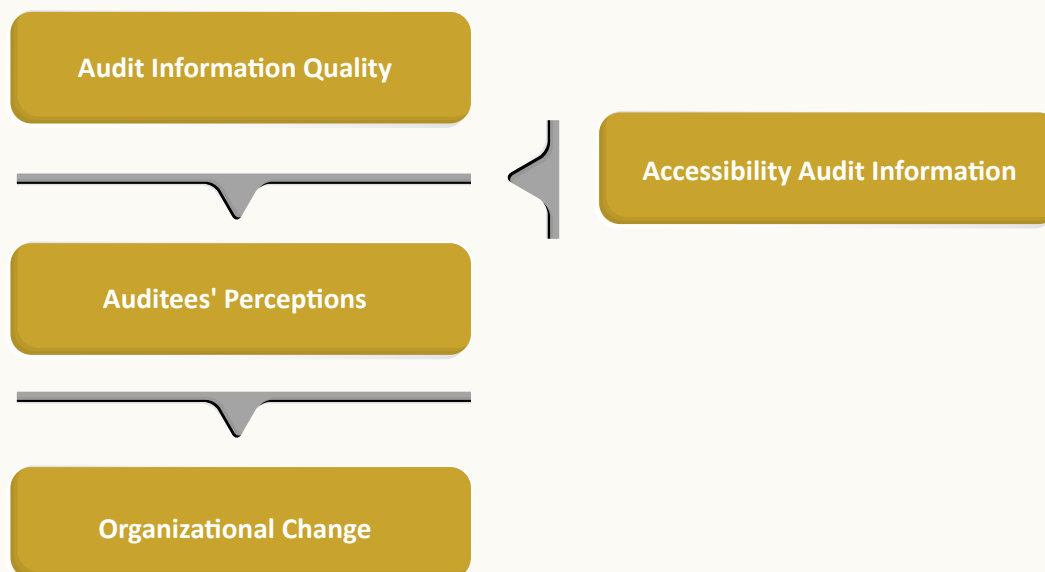
קונספטואלי חדשני יחסית, המתאר את הגורמים העיקריים לשינוי במוכנות המבוקרים כלפי תהליכי העבודה של הביקורת הפנימית וקבלת ממצאיה והמלצותיה. המשתנה הבלתי תלוי מיוצג על ידי איכות המידע שמקורו בביקורת (audit information quality) והמשתנה התלוי הוגדר כשינוי ארגוני (Organizational Change). כמו כן, תפיסות המבוקרים (auditees' perceptions) מהוות משתנה מתווך (מושפע מאיכות המידע שמקורו בביקורת ומשפיע על השינוי הארגוני), ונגישות למידע שמקורו בביקורת (accessibility to audit information) הוגדרה במודל כמשתנה ממתן (משפיע גם על המשתנה התלוי - שינוי ארגוני - ומיוצג על ידי האינטראקציה בינו לבין המשתנה הבלתי תלוי). באופן מעשי יש בכוחו של המודל וביחסים הקיימים בין משתני המודל לכוון את העוסקים בתחום איך לתמוך בניהול ביקורות אפקטיביות כאמצעי לשיפור הביצועים בארגון ולהשפעה על שינוי ארגוני. מודל המחקר מוצג להלן.

מחקר זה מציע מודל מושגי להבנת הגורמים המשפיעים על הקשר בין עבודת הביקורת הפנימית לשינוי ארגוני בסקטור הציבורי.

Aviv K., M., Yuval, O., & Hertzel, C. (2016). "New perspective on the black box of internal auditing and organizational change" Managerial auditing journal, Vol.31 Iss 8/9 pp 804-820

מחקר זה מתייחס למעבר מביקורת פנימית מסורתית לביקורת מתקדמת, השמה דגש על מועילות, יעילות וניתוח תהליכים. המעבר הזה מעיד על כך שהמבקרים הפנימיים במגזר הציבורי מתפקדים כ"סוכני שינוי" התומכים בשינויים בסיסיים של תהליכים בארגון. מטרת העבודה היא להציע מודל המזהה את הגורמים לשינוי ארגוני בסקטור הציבורי הנובעים מעבודתה של הביקורת הפנימית, ומסביר את הדרכים שבהן מבקרים פנימיים מסייעים ליצירת שינוי זה. מחברי המאמר פיתחו מודל

מודל המחקר



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.



התרומה הנסתרת במעבר מביקורת מסורתית לביקורת מתמשכת

דן נתניהו, BSc, MBA, CISA
תא

כמו שהיה נהוג בעבר. ניתוח נתוני כלל האוכלוסייה מחייב שימוש בכלים ממוחשבים. כלי ייעודי נפוץ לביצוע ביקורת באמצעות מחשב נקרא CAATTs - Computer Assisted Audit Techniques & Tools. תוכנות כגון IDEA ו-ACL הן תוכנות CAATT.

ננסה להסביר מדוע יש צורך בשינוי הפרדיגמה ולמעבר מביקורת מסורתית (שבה נעשה כבר שימוש בכלי CAATT) לביקורת מתמשכת, מה נדרש ברמות השונות בארגון כתנאי להצלחת המעבר, מהם רכיבי השיטה ומהן התרומות המרכזיות הנובעות מההליך ותוצריו.

בגיליון דצמבר 2016 של כתב העת "עיונים בביקורת פנימית", במסגרת המאמר "מהפכת המידע האנליטי בביקורת הפנימית בארגון", הוצגו המושגים ביקורת מתמשכת וניטור מתמשך, וצוין כי השילוב ביניהם מביא לארגון ערך מוסף בניתוח נתונים וניטור שוטף של בקורות, על ידי היחידות העסקיות ובמועדים שאינם תלויים במועדי הביקורת.

במאמר נידון בנוסף המושג Data Analytics, שמשמעותו ניתוח נתוני כלל האוכלוסייה להערכת אפקטיביות הבקורות הפנימיות, ולא הערכה של האפקטיביות על סמך דגימה,

ניתוח נתוני כלל האוכלוסייה מחייב שימוש בכלים ממוחשבים. כלי ייעודי נפוץ

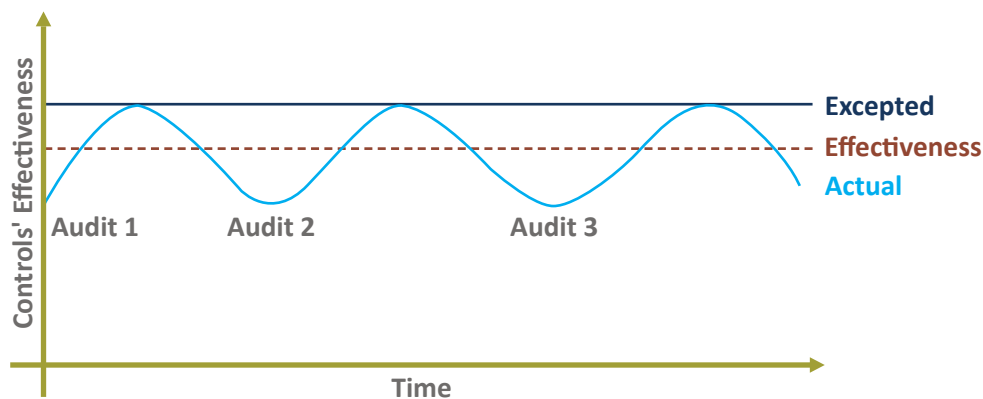
לביצוע ביקורת באמצעות מחשב נקרא CAATT - Computer Aided Audit

Technique & Tools. תוכנות כגון IDEA ו-ACL הן תוכנות CAATT

הצורך בשינוי

במרבית יחידות הביקורת הפנימית בארץ ובעולם, הביקורת מגבשת תכנית עבודה שנתית, הנגזרת מניתוח סיכונים שגובש בביקורת הפנימית או ניהול הסיכונים של הארגון, והנחיות ההנהלה וועדת הביקורת. הפועל היוצא הוא תכנית הבדוקת נושא אחת למספר שנים בהתאם לסיכונים המוכלים בו Ad-Hoc Analysis.

נמצא כי אפקטיביות הבקורות לאורך זמן בשיטת עבודה זו, נמוכה מהאפקטיביות לה אנו מצפים. האפקטיביות עולה מיד לאחר הביקורת אך שוקעת לערך המקורי עד לעריכת הביקורת הבאה:



נייר עמדה של חברת CaseWare Analytics העוסק בביקורת מתמשכת, Continuous Auditing: A Strategic Approach to Implementation, מסביר כי מלבד הבעיות הנסקרות במסמך GTAG, ארגונים מתמודדים גם עם קצב הולך וגובר של יצירת נתונים, תוך יצירת סביבה שבה המשתמשים במידע הפיננסי דורשים ודאות לדיוק, שלמות ורלוונטיות הנתונים בדוחות.

מאחר שקצב גידול הנתונים מתגבר, פונקציות הניהול הופכות ליותר ויותר תלויות במערכות המידע התפעוליות ובכלי קבלת החלטות מבוססי המחשה חזותית. ביקורת מסורתית המבוצעת במחזוריות שנתית/חמש שנתית, אינה מסוגלת להבטיח להנהלה את רמת הוודאות הנדרשת בתחומים אלה.

ביקורת מתמשכת אינה אפליקציית תוכנה או כלי המסייע למבקרים פנימיים לעמוד באתגר שלעיל תוך הישרדות במחסור המתמשך בכוח אדם מקצועי, אלא תהליך המשלב שיטות עבודה בסיסיות שמבצע המבקר הפנימי, לרבות תכנון והערכה מתמשכת של הסיכונים והבקורות, יחד עם פרדיגמת ביקורת חדשה של מעבר מביקורת תקופתית מבוססת מדגמים אל ביקורת המתאפיינת בהערכה מתמדת המתבססת על ניתוח כלל התנועות.

מהי ביקורת מתמשכת ?Continuous Auditing

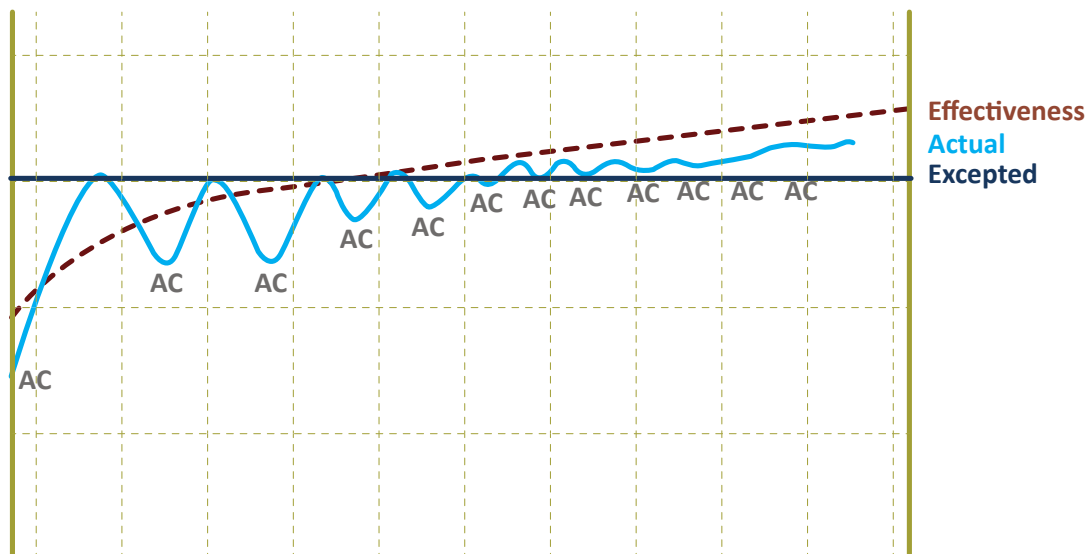
מסמך IIA (GTAG - Global Technology Audit guide), משנת 2015, שכותרתו Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, מתאר כי סביבת רגולציה משתנה, גלובליזציה גוברת, לחצי השוק לתוצאות עסקיות משופרות, וסביבה עסקית שבה התהליכים משתנים בקצב גבוה, יוצרים את הצורך בארגונים

- לפיתוח תכנית לביקורת מתמשכת
- המכוונת לנתונים פיננסיים ותפעוליים. תכנית כזו תומכת ביכולת הביקורת הפנימית לספק ביטחון מתמשך בניהול סיכונים יעיל ובבקרה לממונים על הממשל התאגידי.

מאפייני הביקורת המתמשכת כוללים עקרונות למעבר לביקורת מתמשכת

- גישה רב-פעמית לנתונים, כלומר הורדת נתונים בשיטתיות ממערכות ERP והמרה שוטפת של הנתונים למידע.
- אוטומציה, באמצעות פרוצדורות אוטומטיות, לייבוא נתונים, לניתוח תנועות, לרבות תנועות שהתווספו (Incremental Analysis), ולייצוא חריגים.
- הגדרת תזמון ותדירות של שליפה וניתוח הנתונים, בהתאם לניתוח הסיכונים.
- בדיקת הבקורות הממוחשבות להצפת חריגים וניהולם (Management by Exceptions) לרבות הרמת דגלים אדומים:
 - « זיהוי בזמן ודיווח של חריגים, שלמות ותקפות הנתונים.
 - « ניתוח תנועות מפורט.
 - « בחינת הבקורות.
 - « ניתוח תבניות ומגמות.
 - « ניתוח השוואתי בין יחידות, במטרה ליצור אחידות בשיטות עבודה.
 - « חיזוי ביצועים סטטיסטי למספר תקופות קדימה.

ממסמך GTAG עולה כי המעבר לביקורת מתמשכת מאפשר גידול משמעותי באפקטיביות הבקורות לאורך זמן, כמוצג בתרשים להלן:



מצד מספר גורמים בארגון. זהו שינוי שימצב את הביקורת הפנימית כגורם התורם ערך מוסף גבוה יותר לארגון. השינוי כולל בניית תשתית ארגונית להצלחת המעבר, מחויבות המבקר הפנימי, מחויבות יחידת הביקורת ומחויבות מבקר ה-IT.

שינוי הפרדיגמה אינו שינוי טריוויאלי. קבלת החלטה שמתאריך נתון משלבים ביקורת מתמשכת יחד עם עריכת ביקורת מסורתית לא תביא לשינוי הדרוש.

שינוי תפיסת עריכת הביקורת מביקורת מסורתית למערך המשלב ביקורות תקופתיות כמקובל, יחד עם ביקורת מתמשכת, מחייבת תשתית הכוללת היערכות מוקדמת ומחויבות לתהליך

תשתית להצלחה

מהספרות (GTAG, 6 Simple steps to a more effective internal audit, IIA) עולה כי לגורמים הבאים אחריות למימוש ולהבטחת ביקורת מתמשכת: ועדת הביקורת, ההנהלה הבכירה בארגון, המבקר הפנימי והביקורת הפנימית, כמפורט בטבלה להלן.

תפקיד	אחריות
ועדת הביקורת	• הכרה בצורך לשינוי. • אישור להצטיידות בכלי תחקור אנליטי (CAATT), להכשרת יחידת הביקורת הפנימית לעבודה בו, עד להטמעה אפקטיבית (קבלת ההחלטה בוועדת הביקורת/בהנהלת הארגון). • הבנה כי ייתכן שתפוקות הביקורת עד להטמעה אפקטיבית יקטנו.
הנהלת הארגון	• תכנון וביצוע ניטור מתמשך על מנת להעריך את ההתאמה והאפקטיביות של הבקרה וניהול הסיכונים. • פיתוח ויישום פתרונות ניהוליים לבעיות יסוד. • קיצור משך הזמן לתגובה.
המבקר הפנימי	• פעולות המדגימות היצמדות לסטנדרטים המקצועיים. • בניית צוות ביקורת רב-תחומי, בעל יכולות מקצועיות מוכחות. • מיסוד אמינות לפעילות ביקורת מתמשכת על ידי הוכחת יכולות צוות הביקורת, באמצעות הכלים הטכנולוגיים, הסדרי אבטחת נתונים ותקציב היחידה. • הצגה ברורה ליחידת הביקורת, להנהלה הבכירה ולמועצת המנהלים, של התפקידים והאחריות של הביקורת הפנימית לעומת תחומי האחריות של ההנהלה. • התחייבות לאסטרטגיה רב-שנתית להגדלת התמיכה של בעלי עניין. • שיתוף ההנהלה ומועצת המנהלים בתוצאות הערכות הביקורת הפנימית לאפקטיביות הניטור המתמשך המבוצע על ידי ההנהלה.
יחידת הביקורת	• תכנון ביקורת מתמשכת יחד עם היחידות העסקיות בהנהלה. • ביצוע ביקורת מתמשכת: « קשירת הניתוח האנליטי להנחות ולמטרות העסקיות. « הוספת ערך כיועץ על ידי הערכת סיכונים תאגידיים מתהווים. « יצירת זיקה בין גורמי הסיכון לבין פעילויות הבקרה. • ביצוע ביקורת על אופן ביצוע הניטור המתמשך. • אספקת הבטחה מתמדת בהקשר של מטרות הביקורת, כגון שלמות, דיוק ואבטחה. • שמירה על הסדרי אבטחת מידע אפקטיביים.

— ★ —
**מחויבות
המבקר
הפנימי**

- השקעת שעות הדרכה לצוות הביקורת הפנימית בהכשרה פרונטלית בכלי ה-CAATT שנבחר, והתמחות סגל העובדים לרמה המאפשרת עבודת ניתוח ותחקור עצמאית.
- מיסוד פעילות On the Job Training (OJT) מתמשכת, לשם הטמעת הידע התיאורטי של ה"איך" הנלמד בהשתלמות לנושאים המבוקרים.
- עדכון נוהלי עריכת ביקורת.
- יישום סביבת שליפה לנתונים מהמערכות התפעוליות ב-ODBC (Open Data Base Connectivity) ממערכת ERP.
- תקנון שיטת עבודה להשגת חיסכון במשך ביצוע ביקורת, התייעלות וחסכון כספי ע"י
- « התקנת כלי ה-CAATT הנבחר במחשבי עובדי הביקורת.
- « בחירת משרדי מיקור חוץ העובדים בכלי ה-CAATT שנבחר.
- « עידוד המבקרים לנתח ולתחקר נתונים באמצעות כלי ה-CAATT הנבחר בלבד ולא רק בכלים מסורתיים (גיליון אלקטרוני, Access ואחרים).
- בחירת נושאי ביקורת כמותיים שבהם קיים ערך מוסף לביקורת מתמשכת, על פי תוצאות ניהול סקר הסיכונים וצורכי ההנהלה.
- בחירת נושאים המשלבים ניתוח מסמכים יחד עם תחקור נתונים כמותי.

— ★ —
**מחויבות
יחידת
הביקורת**

- התגברות על ההתנגדות הטבעית לשינוי.
- הבנה שנדרש להשקיע זמן לימוד פרונטלי וזמן לימוד באמצעות הכשרה בפרויקט מעשי ביחידת הביקורת On the Job Training - OJT.
- ניתוח ותחקור נתונים באמצעות כלי ה-CAATT שנבחר.

— ★ —
**מחויבות
מבקר ה-IT
ביחידת
הביקורת**

- בארגונים רבים, מבקר ה-IT עוסק בעיקר בסיוע למבקרים האחרים בהגדרת הנתונים הנדרשים, בהורדתם לסביבת ה-PC ובתחקורם. גם בעידן הביקורת המסורתית, למבקר IT יש מטלות ביקורת IT כגון היערכות לחירום (DRP), אבטחת מידע ובדיקות חדירה, סייבר, וניהול ובקרה של חוות השרתים.
- כפועל יוצא משינוי עיסוקו המסורתי של מבקר ה-IT, והמעבר מסיוע לאחרים לפעילות ביקורת IT ממוקדת, יש לו אחריות מרכזית להקמת התשתית לדוחות בקרה, כחלק מהביקורת המתמשכת שנועדה לזהות חריגים ביחס לנורמה ולאפשר הרמת דגלים אדומים.

בניית דוחות בקרה של התהליכים העסקיים על בסיס תכנית הביקורת השנתית

- בסיום הקמת התשתית הנדרשת לשינוי הפרדיגמה והתמקדות בנושאי ביקורת המשלבים ניתוח כמותי, ניתן להתחיל בבניית דוחות בקרה הכוללים את השלבים הבאים:
- ביצוע ניתוח להערכת חוזק הבקורות הפנימיות:
 - « שימוש ביכולות המובנות בכלי ה-CAATT לייבוא, ניתוח ושליפת ליקויים בתהליך שוטף ועקבי לבדיקת אמינות הנתונים, חישובים פנימיים, הפרדת תפקידים ועוד.
 - « זיהוי הבקורות שאינן מתפקדות או מתפקדות באופן בלתי מספק בתהליך המבוקר.
 - « תיעוד תהליכי העבודה והממצאים.
- יצירת פרוצדורה חזותית אוטומטית של כל התהליך שנבדק, ללא קוד, ובדיקתו על הנתונים המקוריים.
- קיבוע פרוצדורה לאחר בדיקות והעברתה לבקרה העסקית, להרצה בשוטף לשליפת חריגים מהנורמה ולהרמת דגלים אדומים, סמוך ככל האפשר למועד התרחשות האירוע.
- גיבוש תפריטי עבודה מובנים ותהליכים אוטומטיים המאפשרים חזרה בנקודות זמן על פעילות בדיקת הבקורות, במטרה לוודא תיקון ליקויים וזיהוי בעיות חדשות.

תרומות הנובעות משינוי הפרדיגמה והערך המוסף הסמוי

- תרומות שינוי הפרדיגמה בנושא אפקטיביות הבקורות בתהליכים העסקיים מתוארות במסמך GTAG.
- אם כן, מהו הערך המוסף הנובע משינוי שיטת העבודה שאינו מוצג ב-GTAG?
- הפקה של דוחות בקרה אוטומטיים ללא עלות (הדוחות נוצרים ללא כתיבת קוד בעת ביצוע הביקורת ומכאן שאין להם עלות), לשם איתור כשלים הפוגמים באיכות הנתונים וזמינותם, בכל נקודת זמן שבה תחליט יחידת הבקרה להריץ את הדוח. חשוב להדגיש כי לאחר בדיקת הביקורת להרצה ראשונה תקינה של הדוח, נדרשת העברת האחריות להפקת דוחות הבקרה בשוטף ליחידת הבקרה העסקית ולא ליחידת הביקורת הפנימית.
- מניעת זליגה כספית - פתרון ותיקון הליקויים במערכות המידע הארגוניות, תהליך הדורש בדרך כלל מסגרת זמן והשקעת משאבים משמעותיים. שינוי שיטת העבודה להרצת דוחות בקרה לפני ביצוע תהליכי הוצאת כספים מהחברה, ימנע זליגת כספים ויאפשר סגירת פרצות מידית, עד לתיקון התהליכים וחזוק הבקורות.
- ביצוע מעקב תיקון ליקויים שוטף באמצעות הרצת הדוחות, ימנע את הצורך בביקורת חוזרת ויאפשר השגת חיסכון כספי ניכר.
- הקטנת תלות הביקורת הפנימית בעובדים ייחודיים על ידי הכשרת המבקרים לניתוח אנליטי.

סיכום

ש ינוי תפיסת שיטת העבודה הוא תהליך לטווח ארוך. ראשיתו בהבנה בצורך בשינוי, והמשכו בשכנוע הנהלת הארגון ומועצת המנהלים בתרומת השינוי לארגון, ובהכרה כי משך הזמן מהתנעתו ועד למימוש אפקטיבי הוא ארוך. לגורמים רבים בארגון יש השפעה על התהליך, ובראשם למבקר הפנימי וליחידת הביקורת המחויבים לשינוי שיטת העבודה. פועל יוצא של תהליך העבודה המוצע, הן ביחידת הביקורת הפנימית והן ביחידות הבקרה הכספית בארגון, הם התוצרים הארגוניים הבאים:

- מאגר דוחות בקרה אוטומטיים זמין לזיהוי חריגים וכשלים בתהליכים השונים.
- יכולת להשוות ביצועים ועלויות ביחידות השונות בחברה באופן שוטף ומתמיד.

בחזרה ליסודות- תרגולת שריפה

מאמר זה הוא תרגום של המאמר The fire drill שהתפרסם בגיליון יוני 2016 של כתב העת Internal Auditor IA
מייקל מרקוצ'י

תא

ב יומו השני של מפגש צוות ראשי הביקורת של חברת GE קפיטל בניו יורק, החלה פתאום לפעול אזעקת החירום של הבניין בעוד הכרוז מודיע ברמקול: "תרגיל, תרגיל, תרגיל, שריפה פרצה בבניין". בהתאם לנוהל, הנוכחים עזבו את חדר הישיבות בזה אחר זה והתרכזו במבואה. בזמן שהמתנו להרצאה הרגילה על בטיחות אש, הנוכחים החלו לפזול לכיוון הטלפונים הסלולריים שלהם. בשלב זה נכנס למבואה קצין האש, ביל, והחל לדבר. הביטחון, האינטנסיביות והמומחיות המעמיקה שלו משכו מיד את תשומת לבם של ראשי הביקורת. בעשר הדקות הבאות למדנו יותר על בטיחות אש מאשר כל מה שלמדנו אי פעם בנושא זה. הבחנו גם ברמת ריכוז ובהירות מחשבה שניתן ליישם בעבודתנו כמבקרים. ההרצאה הבלתי נשכחת של ביל הזכירה לנו כי חמישה תחומי מפתח - תכנון, כשירות, כישורי מכירות, התמקדות בתמונה הגדולה והנעה לפעולה - מהווים את חותמת האיכות של מבקר מצליח.



תכנן את עבודתך, עבוד לפי תכניתך

תרגולת השריפה החלה מספר ימים או אף שבועות לפני שהופעלה האזעקה. מישהו היה צריך להודיע להנהלת הבניין, לתאם עם רשויות כיבוי האש והמשטרה המקומיות, לבדוק את הציוד, להקצות סדרנים לניהול זרימת האנשים בזמן התרגיל, להתריע בפני המאבטחים ולקבוע סוגיות לבדיקה לצורך איסוף נתונים שימשמשו להערכת תוצאות התרגיל לאחר סיומו. אמנם ביל היה זה שדיבר, אך ניכר שמספר גדול של אנשים עבדו כצוות על מנת להבטיח שהתרגולת תעבור באופן חלק.

מורכבות הפונקציות שאנו מבקרים בשילוב הציפיות הגבוהות ביחס לעבודתנו, הופכים את התכנון האפקטיבי למהותי, במיוחד עבור מנהלים. למעשה, תכנון הוא התחום שבו השפעתם של המנהלים על תוצרי העבודה היא הרבה ביותר. בדומה לביקורת, ההצלחה של האירוע עצמו תלויה באופן משמעותי בהשקעה בתכנון. בהכשרה למתודולוגיית הביקורת של GE קפיטל, מעודדים את מנהלי הביקורת להשקיע עד 40% מזמנם בשלב התכנון של הביקורת, מכיוון שזו הנקודה שבה ניתן למנף את הניסיון שנצבר בביקורות קודמות לטובת הנחיית צוות הביקורת. משמעות הדבר היא הסתכלות קדימה ושימוש בניסיון זה לצורך הנחיית הצוות באמצעות תכנית שנבנתה במיומנות.

לפצות באמצעות כשירות

ברגע שביל הצליח לקבץ ולהשקיט אותנו, הוא אמר שהוא יודע שאנחנו עסוקים ושיגזול רק עשר דקות מזמננו. הוא התקדם בזריזות ברשימת הנקודות שלו וסיים את ההרצאה בזמן. ביל הגיע מוכן לעבודה, הכיר את החומר וניצל היטב את הזמן שעמד לרשותו. התוכן היה יבש והוא ידע שהקשב שלנו יהיה מוגבל, ולכן פיצה על כך באמצעות כשירות. ביל היה רוטט, בקיא ותכליתי. ניכר היה שהתכנון היטב לנאום שנשא, והוא משך את תשומת הלב שלנו באמצעות נתונים מדויקים שהתבססו על הניסיון והתובנות שלו.

במהלך ביקורת לא תמיד קל להצליח לקבל מזמנם ותשומת לבם של מנהלים. כאשר אנו מציגים ממצאים בפני בעלי העניין, אנו יודעים שהם היו מעדיפים להיות בכל מקום אחר באותו הרגע, ולכן עלינו לדמיין את עצמנו כסוכני מכירות שמרוכלתם היא שירותי הבטחה, ואנו עושים זאת באמצעות בקיאות, עצמאות וכשירות, ובאמצעות גיבוי תובנותינו בנתונים ובניסיון. גישה כזאת חיונית לערך שהמבקרים מספקים לארגונים.

למכור עם תשוקה של אלוף

במהלך הפרזנטציה שלו, ביל לא הזכיר מדיניות או רגולציה ולו פעם אחת. הוא מעולם לא התייחס לצד שלישי או לגורמים בכירים ממנו כדי להצדיק את פעילותו באותו היום, והוא גם לא התנצל עליה. הוא מנה את הסיכונים המרכזיים, הסביר מדוע עלינו לעבוד ביחד וסיפק לנו מידע בעל ערך. הוא עשה זאת עם כזו תשוקה ואנרגיה עד שאחרי כמה דקות בודדות קבוצה של מנהלי ביקורת הפכה לחסידה של בטיחות אש. במובן זה הוא הפך את תפקידו לכוזה של איש מכירות. הוא מכר בטיחות אש, ואנחנו קנינו את נאום המכירות שלו. הוא לא היה קורבן של המדיניות, אלא אלוף של בטיחות.

כאשר ההנהלה לוחצת להבין מדוע ראוי להקדיש זמן ומשאבים לתיקון בעיה שנמצאה בתהליך הביקורת, המוצא הקל והנוח הוא לצטט מדיניות או רגולציה. אך אלו אינן הצדקות מספקות להשקעת משאבי החברה, ומהוות משענת רעועה עבור המבקרים. למעשה, ההצדקה הטובה ביותר להשקעת משאבי החברה הוא תיקון חולשה בבקורות היוצרת סיכון שלא ניתן להשלים עמו. בעוד שאנו אוהבים לחשוב שהתואר "מבקר" הוא תואר מספק עבורנו בביצוע עבודתנו, ראוי היה שנהיה יותר כמו ביל ונמכור את התובנות שלנו למנהלים מתוך תשוקה ומומחיות. לעתים רבות אנו נשאלים לדעתנו, דבר שמהווה חלק מתפקידנו, אך דעתנו טובה רק ככל שהיא נתמכת בעובדות ובניתוח של הסוגיה. אחרת דעתנו אינה אלא ספקולציה.

לתקשר סיכונים מהותיים באופן ברור

ביל התמקד בתמונה הגדולה. המשמעות של בטיחות אש עבור בניין במנהטן היא מוכנות, קיומה של תכנית ועזיבה את הבניין בבטחה. אך קיימים רכיבים נוספים מעבר לכך, כגון ירידה במדרגות, הימנעות מהשימוש במעלית, לקיחת חפצים אישיים, שמירה על רוגע, הכרת היציאות מהבניין ואבטחת שולחן העבודה. בכך שהוא מיקד אותנו בתמונה הגדולה, ביל הצליח לשמר את הקשב שלנו והשאיר אותנו עם מידע שנוכל לזכור. למעשה, הוא עשה עבודה טובה כל כך עד שחודשים אחר כך אני עדיין זוכר את הרעיונות הכלליים שעליהם הוא דיבר: הֲיָה מוכן, הכן תכנית, הבט מסביב ואל תילחץ בזמן העזיבה את הבניין.

ביקורות עלולות להיות מעיקות ועבודת השטח יכולה לכלול שבועות או חודשים של שחזורים, התאמות, ראינות ובדיקות אחרות. עבודה זו מהווה בסיס לתובנות שלנו, אך אין צורך לסקור את הקושי והמאמץ שבעבודה זו במסגרת הגשת הדוח הסופי שלנו וחווה דעתנו להנהלה. על מנת לספק ערך מוסף, עלינו להמיר את כמויות הנתונים שאספנו

במהלך הביקורת לכדי מידע שימושי, ולמסגר מידע זה לכדי סיכוני המפתח של הארגון. ניתן לתפוס את הקשב של כל מנהל כשיר דרך שימוש במילים כגון "היעדר בקורות בתהליך זה מהווה עבור הארגון סיכון שלא ניתן להשלים איתו". לעומת זאת, המנהלים יפזלו מיד לסמארטפונים שלהם אם נשתמש במקום זאת במילים "לאורך שלושה שבועות ביצענו התאמות ב-42 חשבונות בספרים של החברה".

אז מה?

זוהי דרך תכליתית לשאול, "מדוע אתה מספר לי את זה ומה אתה מצפה שאעשה?". ביל היה מאוד ממוקד ב"אז מה". הוא לימד אותנו מדוע תרגיל אש הוא חשוב וכיצד להתכונן למאורע האמיתי. לא פעם אנחנו מוצאים את עצמנו בביקורת, בפרזנטציה בפני ההנהלה או בכל פגישה אחרת עם הבנה של העובדות והסיכונים אך ללא תכנית פעולה. לאחר ששומעים את השאלה "אז מה" מספיק פעמים, לומדים לפתוח פרזנטציות המתייחסות לשאלה זו במקום להכריח אנשים לחכות ובלתי נמנע. על ידי התייחסות לנקודה המרכזית בתחילת הפרזנטציה, ובאמצעות חזרה על הדברים מבעוד מועד על מנת להעביר מסר חד וממוקד, אפשר לגרום להנהלה לפעול באופן מיידי בעניין חולשות מהותיות בבקרה.

כמבקרים פנימיים, אנו מבצעים מסה של עבודה תחת לוח זמנים צפוף, ובסופו של דבר מאמצנו מתומצתים לכדי מְקטע קצר או מספר משפטים בפרזנטציה. אך כפי שהמחיש ביל, ברגעים המעטים שבהם אנו זוכים לתשומת הלב של בעלי העניין, תפקידנו הוא להעביר מסר ממוקד שמוביל לפעולה מצד ההנהלה. בסופו של דבר, אנו המבקרים לא מספקים כל ערך מוסף אם אנו לא משמשים זרזים לשינוי בארגונים שלנו.

זהו אינו תרגיל

This article was reprinted with permission from the June 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



קמפוס השפלה בשיתוף א"י ישראל-איגוד מבקרים פנימיים בישראל ובשיתוף איגוד מבקרי הרשויות המקומיות

מזמין אתכם להירשם לקורס הכנה לבחינות ה - CIA חלקים 1+2+3

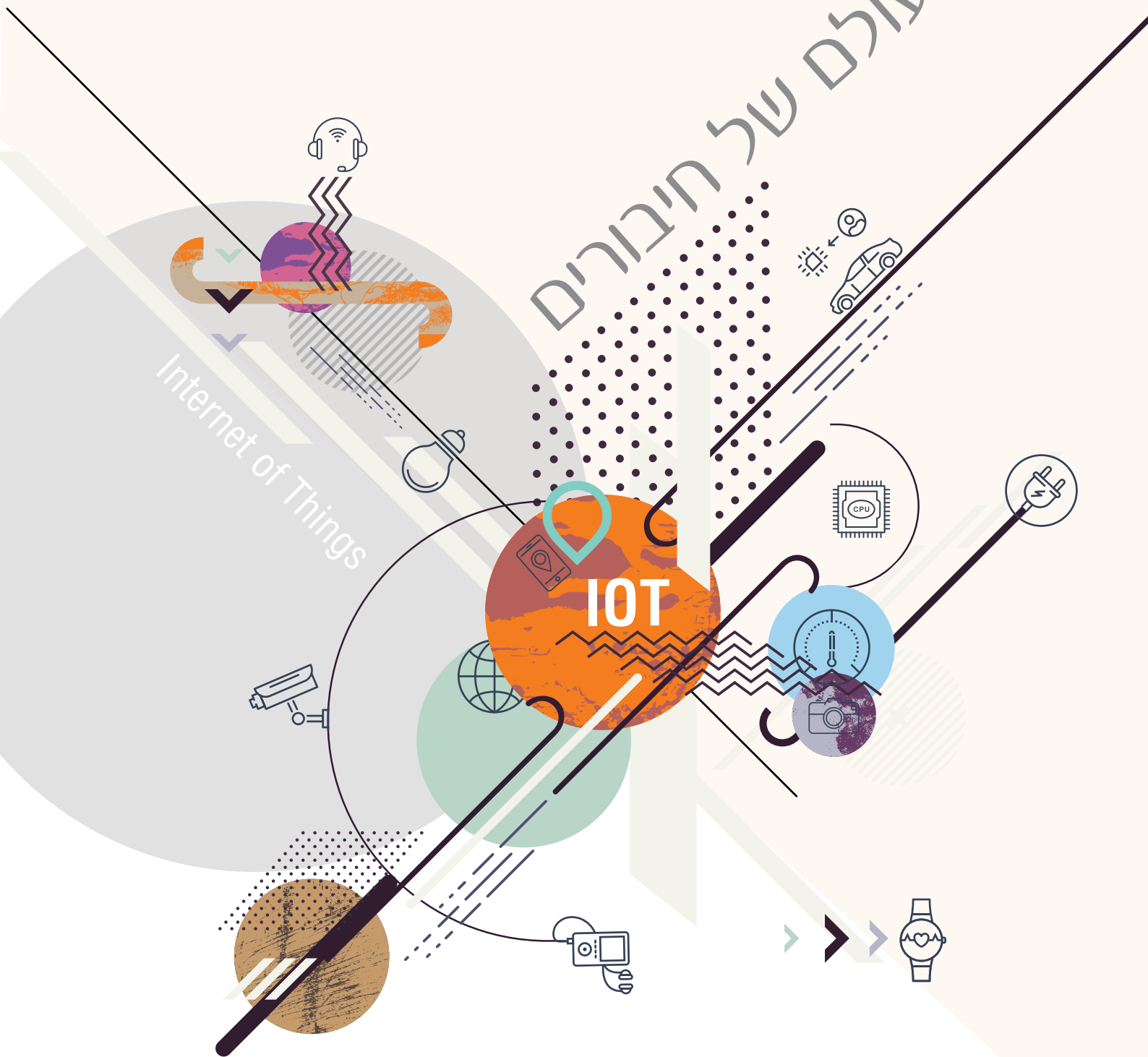
קורס ההכנה לבחינות CIA כולל תכנים בתחומי תקני הביקורת הפנימית, עולם הסיכונים, ניהול הביקורת הפנימית, דיני ביקורת, אתיקה ונורמות בניהול, ביקורת טכנולוגית המידע והסייבר, חשבונאות ניהולית וחשבונאות פיננסית, ביקורת מעילות והונאות ועוד.
בנוסף לחומר התיאורטי, הקורס יכלול גם תרגול מעשי.

מועד פתיחה התכנית מאי 2017		מתכונת חד-שבועית
חלק 1 נושא א' ציות לתקני IIA והנחיות נושא ב' בקרה פנימית וסיכונים נושא ג' עריכת עבודת השטח - כלי ביקורת וטכניקות	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 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 גלובלית
תכנית בהיקף של 200 שעות אקדמיות בהתאם לדרישות הנרשמים יוחלט על מתכונת הקורס		שכר לימוד 6900 ₪ + 2000 ₪ בגין ערכת לימוד CIA שרכישה היא חובה
מתכונת חד שבועית יום שלם 09:00-16:00 / בוקר 09:00-13:00 / ערב 15:00-19:00		*שכ"ל אינו כולל דמי רישום למבחני ההסמכה **מחיר למבקרים ברשויות המקומיות

הבטיחו את מקומכם, מספר המקומות מוגבל

לפרטים ורישום | 1-800-200-667
קמפוס השפלה, רח" הזית 4 רמלה





המאמר הוא תרגום של המדור A world of connections שהתפרסם בגיליון אוגוסט 2016 של כתב העת
Internal Auditor IA
Jane Seaqo, כותבת מקצועית.

ה"אינטרנט של הדברים" מעמיד את המבקרים הפנימיים בפני סיכונים שלא ניתן להכיל בקלות

עם זאת, יש שמכירים בכך שלהשלכות של מיליארדי החיבורים הללו ויתרונותיהם, רבים ככל שיהיו, יש צד אפל: סיכוני אבטחה, אובדן הפרטיות ואובדן היכולת של אנשים לשלוט בחייהם. קנת' מורי, מנהל חברת Stronghold Solutions International והמבקר לשעבר של העיר אוסטיין, טקסס, טוען כי "הסיכונים העתידיים שגלומים ב-IoT הם משמעותיים הרבה יותר מהסיכונים הקיימים כיום. לרגישויות החדשנות האלו יש השלכות קשות בתחומים של אבטחת מידע ואבטחת סייבר".

למבקרים פנימיים יש סיבות אחרות לתהות לגבי המשמעות של ה-IoT עבור הארגונים שלהם. ייתכן כי יידרשו להעניק ייעוץ להנהלה לגבי התועלת והיתרונות התחרותיים שה-IoT יכול לספק להם. עם זאת, עליהם גם לפקח על הסיכונים החדשים שנובעים מכך והבקורות המפצות הנדרשות. הם אינם יכולים להרשות לעצמם להסתמך על ההנחה כי הגורמים הקבועים יישארו קבועים. בדיוק כפי שגאות עולה מגביהה את כל הסירות, כך ההתפתחות המהירה של ה-IoT מובילה לאבולוציה מהירה של הסיכונים. על המבקרים הפנימיים להיות קשובים לשינויים אלה ולהיערך בהתאם על מנת שיוכלו לוודא שהארגונים שלהם מעודכנים.

מעריך של סיכונים

התחרותי (מתקפות מכל סוג שהוא על ידי מתחרה עסקי), מהפכות או אי-סדר שלטוני (תעמולה או "האקטיביזם"), ואף אובדן חיים (נזק לקוצבי לב או לצידוד חדרי ניתוח בבתי חולים). מורי מצביע על סיכון אחר, אובדן של נתח שוק, שמתרחש כתוצאה מ"כישלון של הארגון לאמץ את ה-IoT ולנצל את ההזדמנויות והתועלת שיכולות לצמוח ממנו".

מורי מתייחס לסיכון החיובי של ה-IoT, נקודת מבט שלעתים מתעלמים ממנה במסגרת החשש המוצדק מפני סיכוני האבטחה והפרטיות. אך יש סיבה לכך ששוק ה-IoT מתרחב במהירות, על אף הסיכונים המובנים: הוא מספק תועלות, שלטעמם של פרטים ועסקים רבים, גוברים על הסיכונים הכרוכים בו. לקוחות מעריכים את האופן שבו מכשירי IoT הופכים את חייהם לקלים יותר על ידי צפייה מראש והתייחסות לצרכים ולהעדפות שלהם (לדוגמה, התאמה אוטומטית של טמפרטורת הבית בהתבסס על התנאים בבית ולוחות הזמנים של המתגוררים בו; הכנת

לפי מקורות שונים, עד שנת 2020 הכמות הכלל עולמית של מכשירים בעלי יכולת להתחבר לאינטרנט תנוע בין 26 מיליארד (גארטנר) ל-50 מיליארד (סיסקו). בשני הקצוות של הטווח הזה, המספר הוא מדהים. ניכר כי כוחות השוק, ובהם זמינות גוברת של האינטרנט, עלויות חיבור נמוכות, שימוש נרחב בענן, מספר עולה של מכשירים בעלי יכולת חיבור לרשת והעלות הפוחתת של הטכנולוגיה, יצרו יחד את הסביבה האידיאלית ל"אינטרנט של הדברים" (the Internet of Things - IoT).

ההשפעה של ה-IoT כבר ניכרת. מגמה טכנולוגית רווחת זו, שמוגדרת על ידי ג'ים טאלי, מנהל המחקר בנושא IoT בחברת המחקר והייעוץ גארטנר בלונדון, "כרשת של חפצים פיזיים שמשוּבצת בהם טכנולוגיה המאפשרת להם לזהות ולהתקשר עם סביבתם כדי לייצר תועלת עסקית", היא חלק בלתי נפרד מחיינו (ראה להלן "דוגמאות ל-IoT"). חסידי ה-IoT משבחים את הנוחות, המהירות, ההתאמה לפרט ופשטות השימוש הגלומות בו. עסקים מהללים את ה-IoT בשל ההזדמנויות שגלומות בו בהיבטים של חיסכון בעלויות, בטיחות, יצירת הכנסות ואיסוף מידע.

מעטים חולקים על כך כי קישוריות היתר של ה-IoT כרוכה בחשיפה לסיכונים. עם זאת, קיימים חילוקי דעות ביחס לאופי הסיכונים האלה.

יש שמתייחסים לסיכונים האלה במונחים אפוקליפטיים. הם מאמינים כי כאשר פעילויות יומיומיות מנוטרות ואנשים מייצרים מידע באופן רציף, היכולת ליצור פרופילים ולכוון למטרות ספציפיות תגדל ותוביל לקשיים גוברים בהיבטים חברתיים, כלכליים ופוליטיים. הם טוענים כי ישנו צורך לייצר עבור האנשים דרכים להתנתק מהרשת, להפסיק לשלוח ולקבל מידע. טאלי מביע סקפטיות לגבי היכולת להתנתק מהרשת: "ה-IoT נמצא בכל מקום", הוא טוען, "אין דרך להתחמק ממנו לגמרי".

עם זאת, קיימות דעות אחרות, פרגמטיות יותר, ביחס לסיכונים הגלומים ב-IoT: הפסדים כספיים המשפיעים על הרווחיות (האקר מצליח לפרוץ למד חשמלי וגונב אנרגיה), הפרעות לעסקים (בעקבות מתקפות מונעות שירות), אובדן היתרון

לספקים". דל-קרלו מוסיף כי סביר להניח שספקים אינם מייצרים לבדם את המכשירים שהם מספקים. הוא מטיל ספק בכך שספקים יודעים מי הם הגורמים שמייצרים את החלקים שנרכשים כחלק משרשרת האספקה שלהם. "האם הם בודקים את החלקים האלה על מנת לוודא שהם עומדים בדרישות האבטחה שלנו?" הוא שואל.

פיטר רייס ג'נקינס, ארכיטקט פלטפורמת Watson IoT ב-IBM, מחזק את הצורך באבטחה לאורך כל תהליך הייצור. "אני רוצה שהמקרה שלי יהיה מאובטח באותה המידה שמכשיר ממשלתי מאובטח", הוא אומר.

ארגונים שעושים שימוש במכשירי IoT צריכים שתהיה להם אסטרטגיה להטמעתם בחברה. מ. ג'. וידיה, מנהל ב-EY באטלנטה, מציין כי למרות שפונקציית הביקורת הפנימית אינה לוקחת חלק בהגדרת האסטרטגיה הזו, "רכיב זה מהותי לכך שניתן יהיה לוודא כי האסטרטגיה מוטמעת בצורה טובה, מנקודת מבט של ניהול סיכונים".

צעד ראשון פרודוקטיבי עבור מבקרים פנימיים בהתייחסותם ל-IoT הוא הערכת הסיכונים שנובעים מהשימוש ב-IoT בארגונים שלהם. הסיכונים שונים בין חברה לחברה, כתלות במערכות ה-IoT הקיימות בעסק והתהליכים העסקיים שבהם הן תומכות. לאחר שזיהוי הסיכונים הושלם, הביקורת הפנימית יכולה לוודא כי קיימות בקורות ממגרות-סיכונים מתאימות, הפועלות ביעילות ולוקחות בחשבון את ההקשר שבו פועלות מערכות ה-IoT.

בבחינת ההקשר כאמור, חשוב לזכור שדבר אינו מתקיים בריק. דל-קרלו מספר על מקרה שאירע בשנת 2015 בכנס "הכובע השחור" בארה"ב (העוסק באבטחת מידע), במסגרתו האקרים קיבלו על עצמם אתגר להשתלט מרחוק על רכב שהיה מחובר לאינטרנט. הגישה שלהם הייתה פשוטה יחסית. יצרן הרכב לא הטמיע הגנה באמצעות סיסמה על הרכיבים במערכת השמע של הרכב שהיו מחוברים לאינטרנט. "המעצבים חשבו שמערכת השמע של הרכב אינה כרוכה במידע רגיש, ולכן לא ראו צורך באבטחתו", מסביר דל-קרלו. "הם צדקו לגבי מערכת השמע עצמה, אך נקודת הגישה שבמערכת זו אפשרה חדירה לשאר חלקי הרכב". ההקשר הוא הכול.

תחומי פעילות

התמודדות עם האתגרים הקשורים ל-IoT היא אתגר עצום שדורש עבודת צוות כלל-ארגונית. עם זאת, אפילו המסעות הארוכים ביותר מתחילים בצעד ראשון, וברוח זו - קיימות מספר פעולות ראשוניות שדרךן הביקורת הפנימית יכולה לגשת לנושא.

כוס קפה בהתאם לטעמו המדויק של הפרט, והיכולת לנטר את סטטוס ההכנה מרחוק). עסקים שמשתמשים במכשירי IoT במסגרת התהליכים הפנימיים שלהם, או שעובדיהם משתמשים במכשירים כאלה, יכולים ליהנות מיתרון תחרותי על פני מתחרים בעלי זיקה נמוכה יותר לטכנולוגיה, מחיסכון בעלויות באמצעות ייעול וניטור בזמן אמת, קשר אישי ומיידי יותר עם לקוחות, והחזר גבוה יותר על ההשקעה שלהם בשיווק באמצעות מסרים שיווקיים מדויקים יותר המכוונים לקהלים ספציפיים. חברות שמייצרות מכשירי IoT צפויות לראות עלייה בהכנסות כתוצאה מעלייה בדרישה, ואף עשויות לאתר הזדמנויות ליצירת קווים עסקיים חדשים. כולם, פרטים ועסקים כאחד, ירוויחו מההתמקדות הגוברת באבטחת סייבר (וכן, כפועל יוצא מכך, מהאימוץ של סטנדרטים מקובלים ומאמצים עסקיים לזכות באמון הלקוח) שמכשירי ה-IoT ייצרו.

בין אם הסיכון הוא חיובי או שלילי, מדובר בסוגיה מעשית שהביקורת הפנימית צריכה להיות פעילה בזיהוי, הערכה ושיכון הסיכונים. סטיבן באב, דירקטור ויועץ עצמאי בפירמת Newton Leys Consulting Lts שבאנגליה, טוען כי ייתכן שההנהלה אינה מודעת באופן מלא לסיכון, אולי משום שהוא אינו מוסבר במונחים עסקיים, וכי המדיניות עוד לא כוללת הגדרה של השימוש ב-IoT. "באופן טיפוסי, ה-IoT נכלל כחלק מאבטחת הסייבר, נושא שזוכה לחשיפה ניהולית גוברת, אך ניתן לעשות יותר בעניין", לדבריו. "כמו כן, ה-IoT מכסה נושאים שבאופן טיפוסי אינם נופלים בתחומם של מחלקות אבטחת המידע".

קורבין דל-קרלו, דירקטור ביקורת פנימית, אבטחת IT ותשתיות בחברת Discover שבאילינוי, מצביע על קבוצה מקצועית נוספת שעליה להתעסק בניהול סיכוני IoT: מפתחי תוכנה (מתכנתים). "הרבה מתכנתים מתמודדים באופן קבוע עם מערכות סגורות", הוא אומר. "ייתכן שהם אינם מודעים למשמעות של הקישוריות. כקו הגנה שלישי, מבקרים צריכים לשוחח איתם ולהביא לתשומת לבם את הסיכון".

לשפוך אור על הסיכונים

בעבור באב, תפקידה של הביקורת הפנימית ביחס ל-IoT "קשור כולו לנראות וסיכון - לסייע לצוותי ניהול סיכונים להדגיש כי הסיכון הוא אמיתי, לכמת את החשיפה ולהביא לתשומת הלב של ההנהלה", הוא אומר.

גם דל-קרלו טוען טיעונים דומים. "עלינו לקרוא תיגר על נשאים של איומים", הוא מסביר. "עלינו להיות ערוכים להמליץ על פעולות שיכולות להביא לשיפור האבטחה. עלינו להיות מוכנים לשאול שאלות על איומים שקשורים

זיהוי מדיניות

כאשר מתייחסים לנושאים הקשורים באבטחה בארגון, אחד הצעדים הראשונים הוא לקבוע האם קיימת מדיניות והאם היא עדכנית. אין הרבה ארגונים שיש להם מדיניות ספציפית בנושא IoT, אך רבים מתייחסים לנושא במסגרת מדיניות ה-BYOD ("Bring your own device") - "הבא את המכשיר האישי שלך" שלהם. באב מסביר שלרוב, מדיניות BYOD מכסה רק כמות מצומצמת של מכשירים שנכנסים בקטגוריית ה-IoT. הוא מוסיף כי "הרבה מהמכשירים מגיעים דרך העובדים, אך כמות לא פחותה של מכשירים נרכשו על ידי הארגון. מתוכם, רבים ייפלו מחוץ לגבולות הגזרה של מערכות המידע והאבטחה בארגון, כך שהסיכונים הגלומים בהם עלולים להישאר חבויים".

מורי מוסיף כי למעסיקה הקודמת שלו (העיר אוסטין שבטקסס) לא הייתה מדיניות-על שבמסגרתה ניתן להתייחס ל-IoT, אבל הייתה מדיניות שהתייחסה לשימוש בכוננים ניידים, החסנים ניידים (מכשירי דיסק און קי) ומכשירים ניידים אחרים כגון טלפונים ומחשבים ניידים.

מגבלות האבטחה של ה-IoT מציבות בפני הביקורת הפנימית הזדמנות לשחק תפקיד משמעותי באמצעות עבודה עם צוות אבטחת הסייבר ופונקציות ה-IT, הייעוץ המשפטי והשמירה על סודיות ומתן ייעוץ בעניין פיתוח מדיניות IoT. יהיה צורך לבחון ולעדכן נהלים קיימים ביחס לשימוש בסיסמאות, בטלאי תוכנות ובניטור מערכות כך שניתן יהיה לשבץ את סוגיית ה-IoT במסגרתם. עוד ייתכן שיהיה צורך בנהלים חדשים או עדכניים בעניין סגמנטציה והרשאות גישה. יש צורך להבהיר מהם המכשירים והשימושים המותרים, ולזהות בבירור את ההשלכות לא רק עבור העובדים אלא גם עבור שותפים עסקיים, ספקים ולקוחות בעלי חיבור לרשת של החברה.

בדיקת מצאי

קשה לאכוף מדיניות IoT ללא הבנה ברורה של כמויות וסוגי מכשירי ה-IoT הקיימים בארגון. באב ומורי מסכימים כי סביר להניח שרשימות מצאים, אם קיימות כאלו, לא יציגו את התמונה המלאה. ייתכן שחלק מהרשימות מכסות מכשירים שהארגונים קנו, אך לא יכללו את המכשירים הצרכניים שמביאים איתם העובדים למקום העבודה.

לאחר שהושג המידע הנדרש ביחס למצאי, ניתן להטמיע בקורות מתאימות. החברה של דל-קרלו, "דיסקאבר", שמה בעדיפות גבוהה את ההגנה על הרשת שלה. "יש לנו איסור כללי נגד מכשירים שאינם מטעם החברה", הוא אומר. "אנו לא מאפשרים להם להתחבר לרשת שלנו. יש לנו רשת 'אורחים' שאליה אנשים יכולים לחבר את המכשירים

הפרטיים שלהם; כל שיוכלו להשיג באמצעות רשת זו הוא גישה לאינטרנט". דיסקאבר אף מתקינה תוכנות הדמיה בעלות מערכת הגנה היקפית קפדנית על המכשירים שהיא מספקת על מנת למדר מידע. מחשבים ניידים מוצפנים וניתן לבצע מחיקה של המידע עליהם בשליטה מרחוק. למרות זאת, מציין דל-קרלו, "מדי יום, בקרות אלו חוסמות מאות ניסיונות חדירה של תוקפים ברמות תחום שונות. ללא מוכנות מתמדת למתקפות, יש סבירות נמוכה שארגון יוכל לעצור כל אחד מניסיונות התקיפה האלה".

חינוך ההנהלה

בלי קשר למידת המודעות של ההנהלה לסיכוני IoT, נראה כי קיים קונצנזוס ביחס לעובדה שתוספת בהיבט החינוכי תועיל לארגונים. מורי טוען כי לעתים ההנהלה מודעת למונחים הכלליים שעומדים מאחורי ה-IoT, אך אין לה הבנה מעמיקה די הצורך של ההזדמנויות והאיומים הגלומים בנושא. לטעמו, לביקורת הפנימית יש תפקיד ברור והוא לסייע להנהלה להבין את הסיכונים ולנהל אותם. ויידה מסכים כי חינוך הוא חשוב, "החל מרמת הדירקטוריון ועד לרמה הטקטית, לא רק בתחום ה-IT, לא רק בקרב מנהלים, לא רק ברמת פיתוח המוצר ולא רק ברמת הייצור, אלא לכל רוחבו של הארגון".

בניית דוחות בקרה של התהליכים העסקיים על בסיס תכנית הביקורת השנתית

בחירת האבטחה

ג'נקינס מונה מספר שלבים בסיסיים אך הכרחיים שמבקרים יכולים לבחון. "ביחס להרשאות, כאשר מכשיר חדש מצטרף לענן בפעם הראשונה, יש לוודא שהמנגנון שבאמצעותו התבצע החיבור הוא מוצפן". הוא גם ממליץ לוודא כי הענן עצמו מאובטח, הסיסמאות המוצפנות שמורות הרחק מנתוני ההזדהות הקשורים אליהן, ושהנתונים שזורמים מהמכשירים ואליהם מוצפנים. ג'נקינס מוסיף: "עדכוני תוכנה ישירות דרך הרשת ('over-the-air') נחוצים על מנת לשמר את עדכוניות המכשיר. ודאו כי תהליך זה מתבצע באופן מאובטח".

השגת שליטה ב-IoT

נראה כי לא ניתן לדון ב-IoT בלי להזכיר את הסיכונים הכרוכים בנושא. אך טאלי מדגיש כי לא מעט מכשירי IoT משמשים לאבטחה. הם קיימים על מנת להפחית סיכונים. "ניקה לדוגמה סנסורים מבניים בגשרים", הוא מציין, "סנסורים אלה מזיהרים מפני משקלים גבוהים מדי ולחצים. הם מחוברים למערכות

המילה. עלינו להקפיד על רמת האבטחה הגבוהה ביותר".
אם כן, האינטרנט של הדברים מהווה עבור מבקרים פנימיים הזדמנות לקחת על עצמם תפקיד שבדרך אינו אופייני להם: סגוריה. הם יכולים לעמוד לצדם של משתמשים אישיים וארגוניים של מכשירי IoT. "הטמעת אבטחה בתוך מכשירי IoT היא משימה קשה ותובענית אך חיונית", אומר ג'נקינס. "החברות שמייצרות את המכשירים טוענות שהן עומדות במשימה בהצלחה. אך האם כך הדבר? תפקידם של המבקרים הפנימיים הוא לגרום להם להוכיח זאת".

בקרת תנועה שיעצרו את התנועה מלעלות על הגשר. חיישני פחמן חד-חמצני המחוברים לרשת פועלים באופן דומה. כל מטרת השימוש בהם היא הפחתת סיכונים".

אך מרבית העוסקים בתחומי הביקורת הפנימית ואבטחת המידע עשויים לטעון כי מטרת המכשיר אינה מדאיגה אותם, אלא החיבוריות שלה והיעדר האפשרות לאבטח באופן מוחלט את הארגון, את נכסיו או את האנשים המשתמשים במערכות שלו. דל-קרלו מסכים, אך אינו נותן לחשש זה לעצור אותו. "אנחנו לא יכולים פשוט לוותר. אני עובד עבור בנק. אנחנו נמצאים היכן שהכסף נמצא - במלוא מובן

דוגמאות ל-IoT

מכשירי IoT רבים מוטמעים באופן עמוק כל כך בחיים המודרניים היומיומיים עד כדי כך שאנחנו לא תופסים שהם שם. אך ה-IoT קיים בשפע, כפי שעולה מהמדגם המצומצם שהביא ג'ים טאלי, כמפורט להלן:

רכבים: מודולים שעוקבים אחר התנהגותו של הנהג - באיזה אופן הוא מאיץ, מבצע פנייה, לוחץ על הבלמים. מידע זה מאפשר לחברות ביטוח לקבוע את הפרמיה של כל נהג באופן אישי על פי רמת הסיכון שלו. הן יכולות אף להציע ביטוח שבמסגרתו התשלום נקבע על פי שימוש בפועל, כלומר הפרמיה נקבעת לפי כמות הזמן שבמסגרתו נעשה שימוש ברכב או המיקום שלו - בדרך בין-עירונית מרוחקת או בעיר גדולה בשעות העומס.



חניה: חיישנים שמנטרים רחובות עירוניים על מנת לקבוע את זמינותם של מקומות חניה. החיישנים מתחברים לאפליקציה סלולרית שמנתבת את הנהג למקום חניה פנוי.



תאורה: אמצעי תאורה מתקדמים יכולים לזהות באילו אזורים בבניין נמצאים אנשים, ובכך לתרום לבטיחותם (על ידי וידוא כי אזורים אלה מוארים) וכן לחיסכון בעלויות (כיבוי האורות באזורים שבהם לא נמצאים אנשים).



צעצועים: יש צעצועים שמאובזרים במצלמות שמסוגלות לזהות את תווי הפנים של ילדים שונים. הם יכולים "ללמוד" כל ילד ולהתאים את האינטראקציה שלהם לכל ילד באופן אישי.



חקלאות: חיישנים בשדות מנטרים רמות לחות ואור שמש, מספקים בהתאם לכך המלצות ביחס להשקיה יעילה, ואף אומדים את מועד הקצירה הצפוי.





BASEL 2017

ECIIA
CONFERENCE
21-22/09.2017

From Insight to Influence

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.

האם יש קשר בין גודל מחלקת הביקורת לרמת הבשלות שלה?

נאוה חלמיש, רו"ח, MA - בנק לאומי

תאג

איך ניתן לדעת מהי רמת הבשלות של מחלקת הביקורת שלך ביחס לארגונים אחרים, ואילו צעדים מומלץ לבצע על מנת לשפר את הבשלות?



המחקר מפרט את המאפיינים שנבדקו, ומציע המלצות לשיפור בשלות המחלקה בכל מאפיין:

הלימה לאסטרטגיה של הארגון

פעילות הביקורת צריכה להיות מותאמת לתכנית האסטרטגית של הארגון, ומאפשרת דינמיות על מנת להתאים את פעילות הביקורת לשינויים ביעדים האסטרטגיים של הארגון.

על מנת לשפר היבט זה, כדאי לבנות קשרי עבודה חזקים עם מקבלי ההחלטות ובאמצעותם להתעדכן באופן שוטף לגבי שינויים באסטרטגיה. עוד מומלץ להיות פתוחים ומסוגלים לבצע שינויים בתכנית הביקורת בהתאמה לשינויים מהותיים ביעדים האסטרטגיים של הארגון. גמישות וזמינות חשובות על מנת לשמר ולשפר את מידת הבשלות.

הערכת סיכונים הוליסטית

ביקורת פנימית בשלה אמורה לבצע הערכה הוליסטית של מכלול הסיכונים והשפעתם על הארגון, בנוסף על הערכת הסיכונים הבדידים. ביקורת בשלה גם חייבת להיות פרואקטיבית וצופה פני עתיד על מנת להעריך סיכונים מתעוררים. כלומר, הביקורת נדרשת להערכת סיכונים פרואקטיבית ברמת המאקרו וברמת המיקרו.

על מנת לשפר היבט זה, כדאי לפעול לחיזוק התקשורת בין הביקורת ושני קווי ההגנה האחרים, לוודא שהערכת הסיכון רחבה ככל האפשר על מנת למנוע חוסר זיהוי של נקודות "חשוכות", ולהגביר את מידת ההבנה העסקית של הביקורת את הארגון ברמת המיקרו וברמת המאקרו.

יכולות וכישורים מגוונים

המחלקה כוללת מבקרים בעלי יכולות "משולבות". במחלקה מועסקים מבקרים בעלי ידע בביקורת מסורתית, וכן בעלי ידע מקצועי הרלוונטי לארגון, יכולות עסקיות, כישורי מנהיגות ויכולות חשיבה, וכן קיימת תכנית הכשרה מובנית, מתועדת ומגוונת.

על מנת לשפר היבט זה, כדאי לבנות צוות עם רקע מגוון המשלב ביקורת מסורתית וידע מקצועי עסקי, הן בשלב גיוס העובדים והן בתהליכי ההכשרה שלהם. מומלץ לקיים תהליכי הכשרה מובנים, מתועדים, מתמשכים ומותאמים אישית הן לעובדים והן לצורכי המחלקה, ולפתח מיומנויות גם בתחומים נוספים כגון חשיבה ומנהיגות.

יימת חשיבות לאמידת רמת הבשלות של מחלקת הביקורת ביחס לארגונים אחרים, על מנת שניתן יהיה לבצע פעולות לשיפור ולצמצום הפערים.

מחקר שנערך על ידי לשכת המבקרים הפנימיים העולמית ופורסם בחודש יולי 2016, ("Benchmarking internal audit maturity: A high level-look at audit planning and processes worldwide", by Mohammad Abdolmohammadi, DBA, CPA, Giuseppe D'Onza, PhD, Gerrit Sarens, PhD, CIA, IIA, July 2016). בחן את מידת הבשלות (Maturity) של מחלקות ביקורת פנימית.

המחקר התבסס על סקר שנערך בקרב 2,500 מבקרים ראשיים בארגונים ממגוון תחומי פעילות, מ-166 מדינות בעולם. בנוסף, ערכו החוקרים ראיונות עם מדגם מבקרים, בין היתר על מנת לנסות להסביר את תוצאות הסקר.

הנחות המחקר הן שמחלקת ביקורת בשלה נבדלת במספר מאפיינים ממחלקת ביקורת שאינה בשלה. המאפיינים שנבחנו: מיקום גיאוגרפי, גיל מחלקת הביקורת, גודל מחלקת הביקורת, גודל הארגון, שונות בין הארגונים, סוג הארגון - פרטי או ציבורי, היקף הארגון, התעשייה, האם הביקורת בארגון היא מתוקף רגולטורי, האם מחלקת הביקורת משמשת רקע להכשרה ניהולית בארגון, עמידה בתקנים המקצועיים של ה-IIA).

מחלקת ביקורת בשלה נבדלת במספר

מאפיינים ממחלקת ביקורת שאינה בשלה

המחקר מציג, למשל, השפעה מובהקת של גיל המחלקה על הבשלות שלה, דבר הנובע כנראה מכך שאורך זמן להבין מהו תהליך טוב, לפתח אותו, להיות עקבי בציפיות וביעדים, ולחזק את היחסים עם בעלי העניין.

המחקר מציג ממצא מעניין שעלה בניתוח תוצאות הסקר, והוא היחס בצורת "U הפוכה" בין מספר מאפיינים של רמת הבשלות, לבין גודל מחלקת הביקורת. בניסיון למצוא הסבר ליחס הזה, נשאלו המרואיינים לדעתם. חלקם הציעו את הסברה שבמקרים רבים למחלקה קטנה אין מספיק משאבים לפיתוח מתודולוגיות ותהליכי עבודה מתקדמים, דבר שיוצר פער בין ציפיות בעלי העניין לתפקוד המחלקה, והיא נתפסת כ"לא בשלה מספיק". מנגד, מחלקות גדולות מאוד נמצאות גם הן ברף הנמוך של רמת הבשלות בגלל ריבוי בירוקרטיה ומורכבות פנימית המקשות על ניהול אפקטיבי של המחלקה. מרואיינים אחרים מתנגדים למסקנה העולה מהמחקר וטוענים שאין קשר בין גודל לבשלות.

מחלקות גדולות מאוד נמצאות גם הן ברף הנמוך של רמת הבשלות בגלל ריבוי בירוקרטיה ומורכבות פנימית המקשות על ניהול אפקטיבי של המחלקה

מומלץ להשתמש בטכניקות של ביקורת מתמשכת וביקורת בזמן אמת על מנת להעלות את האפקטיביות לרמה הגבוהה ביותר המתאפשרת על ידי סביבת הבקרה וסביבת ה-IT.

דוגמה מ"השטח" למאפיין זה הוצגה על ידי סאלי קלארק, המבקרת הראשית של בנק ברקליס, שרואה את המחלקה שלה כ- "Leader in Assurance". כפי שסיפרה בריאיון לכתב העת PROTIVITI (Internal auditing around the world, Perspectives from women in leadership roles- How technology is impacting internal audit function, Volume xii, July 2016), המחלקה משתמשת במגוון כלים חדשניים הן בביצוע הביקורת, כגון שיחות וידאו, DATA ANALYTICS, BI ו- WEBEX, והן בניהול פעילות המחלקה, הנתמכת באפליקציה של הדמיית נתונים באייפד, ומאפשרת ניהול ובקרה ברמת על של כל פעילויות הביקורת.

קיום תכנית הבטחת איכות ושיפור (QAIP), כולל הבטחת איכות חיצונית. תכניות אלו מעלות את רמת הבשלות והאיכות של מחלקת הביקורת.

על מנת לשפר היבט זה, כדאי לבנות תכנית הבטחת איכות ושיפור הכוללת מערכת לניהול ביצועים, בהתאם לתקנים מקצועיים ה- IIA. יש להטמיע את התכנית באסטרטגיית הביקורת וב- KPI's שהוגדרו, וליצור תרבות פנימית המבטאת את הבטחת האיכות והשיפור.

בראיונות שנערכו העלו המבקרים מאפיינים נוספים של מחלקת ביקורת בשלה, כגון מידת התמיכה וההערכה כלפי הביקורת הפנימית, מידת המעורבות של הביקורת בפרויקטים מהותיים ובנושאים עסקיים רגישים, והעלאת משקל דברי הביקורת הפנימית בדיווח לבעלי המניות.

ניתן לבחון מאפיינים אלה באמצעות אינדיקטורים שונים, כגון מספר הישיבות והאינטראקציות עם ההנהלה הבכירה והדירקטוריון, אופי הנושאים המבוקרים, התדירות שבה מתבקשת התייחסות המבקר בנושאים מהותיים, וכן האם המבקר הפנימי נתפס בארגון כ"סוכן שינוי".

עדכון בתדירות גבוהה של הערכת הסיכונים המשמשת בסיס לתכנית עבודת הביקורת

סביבה עסקית דינמית מצריכה עדכון תקופתי של הערכת הסיכונים על מנת שהביקורת תישאר רלוונטית. לפיכך, עדכון מתמשך או לפחות עדכון בתדירות שנתית של הערכת הסיכונים, הוא אחד המאפיינים של ביקורת פנימית בשלה. המחקר מתייחס לחשיבות עדכון תכנית העבודה בנקודות זמן קריטיות נוספות לארגון, למשל בהתאמה לשינויים ארגוניים מהותיים.

על מנת לשפר היבט זה, כדאי לבצע הערכת סיכונים עדכנית ודינמית בהתאמה לצורכי הארגון, לחזק את ההבנה העסקית בכל הרמות במחלקת הביקורת. מומלץ לקיים תקשורת שוטפת עם מקבלי ההחלטות בארגון על מנת לוודא קבלת מידע אודות שינויים משמעותיים בפרופיל הסיכון של הארגון ולעדכן את הערכת הסיכונים בהתאם. כמו כן, מומלץ לאפשר דינמיות וזריזות בתוך מחלקת הביקורת על מנת לתמוך בשינויים ארגוניים משמעותיים.

תיעוד וניטור רציף של תהליכי עבודת הביקורת תוך קיום בקורות, וכן קיום אסטרטגיה ברורה לביקורת

על מנת לשפר היבט זה, כדאי לבצע תיעוד וניטור שוטף של תהליכי עבודת הביקורת ונוהלי העבודה, ולבצע בהם שינויים במידת הצורך ובהתאם לשינויים בפרופיל הסיכון. יש לשלב את היבטי הניטור בתהליך הערכת האיכות ובתכנית השיפור. עוד מומלץ לגבש ולתקשר את אסטרטגיית הביקורת באופן ברור לרוחב הארגון, לתרגם את האסטרטגיה ל- KPI's (אינדיקטורים מרכזיים לביצועים), ולנטר באופן שוטף את העמידה בהם.

שימוש בטכנולוגיות מתקדמות לאורך כל תהליך הביקורת (לדוגמה: data mining, data analytics, data mining)

על מנת לשפר היבט זה, מומלץ להשתמש בכלים טכנולוגיים לאורך כל תהליך הביקורת על מנת לייעל את התהליכים, להגביר את האפקטיביות ולהגיע לכיסוי רחב יותר של הסיכונים.

סיכום

דאי לכל מחלקת ביקורת לבחון את המיקום שלה ביחס לכל אחד מהמאפיינים, לאתר את ההיבטים שחשוב לשפר, לקבוע יעדים, ולגבש את תכנית הפעולה על מנת להשיג את היעדים שנקבעו!

• בזכותכם •

שינויים ותמורות חלים כל הזמן בכל תחום -
וגם איגוד המבקרים הפנימיים מתחדש ומתרגען.

שנת 2017 היא שנת התחדשות של האיגוד.

ההתחדשות באה מתוך צמיחה והתחשבות בשינויים המתרחשים מסביבנו כל הזמן

ותבטא גם בריענון התדמית
ובבניית נוכחות דיגיטלית הולמת לאיגוד.

תודה שהייתם שותפים למהלך, תרמתם את דעתכם וסייעתם לתהליך קבלת ההחלטות

בקרוב מאד נוכל להציע לכם

מרכז מידע מקצועי



מגוון קורסים דיגיטליים לפי נושאים שאתם בחרתם



תשלום מקוון של דמי חבר



קבוצות דיון לפי נושא ולפי מגזר



TM



להיות חכם, ולא רק צודק: היערכות ארגונים למתקפת סייבר

תאריך
אלי זילברמן כספי

ולשפר את יכולת התגובה וההתאוששות שלהם. היערכות מוקדמת להתמודדות והתאוששות מאירוע סייבר עשויה לצמצם משמעותית נזקים פוטנציאליים.

מצד שני, אי הכנה ותגובה מהוססת או לא נכונה, עלולה להכניס את הארגון לסחרור מסוכן. עם זאת, ארגונים רבים נמנעים מלהכין את עצמם לניהול אירוע סייבר וההתאוששות ממנו, ומעדיפים להשאיר את הנושא על כתפיו (הרחבות אך לא מספיקות) של מנהל הגנת הסייבר והכוונתו להמשיך בבניית יכולות ההגנה. על כן, קיימת חשיבות מיוחדת שהביקורת הפנימית תעסוק גם בבחינת מוכנות הארגון להתמודד ולהתאושש מאירוע סייבר, ועל ידי כך לדחוף את הארגון לעסוק בנושא, להכין תכניות לניהול משבר סייבר, ולתרגל את התגובה וההתאוששות בפועל.

מות תקיפות הסייבר ומורכבותן הולכות וגדלות ובקצב גבוה. עד כמה המגמה הזו משמעותית? שימו לב לנתון הבא: בחלק ממדינות אירופה פשיעת סייבר עלתה על היקפי הפשיעה המסורתית (!) כך על פי דוח של האינטרפול מספטמבר 2016. לאור מגמות עולמיות אלו, יש לקחת בחשבון שיהיה קשה מאוד לזהות ולעצור חלק מתקיפות אלו, זאת על פי המלצות המדריך של NIST 800-184 העוסק בהתאוששות מאירוע סייבר (Guide for Cybersecurity Event Recovery), שפורסם בדצמבר 2016. על פי מדריך זה, התמקדות אך ורק במניעת תקיפות סייבר אינה מספקת, ולצד שיפור יכולות ההגנה ואימוץ טכנולוגיות חדשות, ארגונים צריכים להתכונן לקראת אירוע סייבר

בחלק ממדינות אירופה

פשיעת סייבר עלתה על היקפי הפשיעה המסורתית (!)

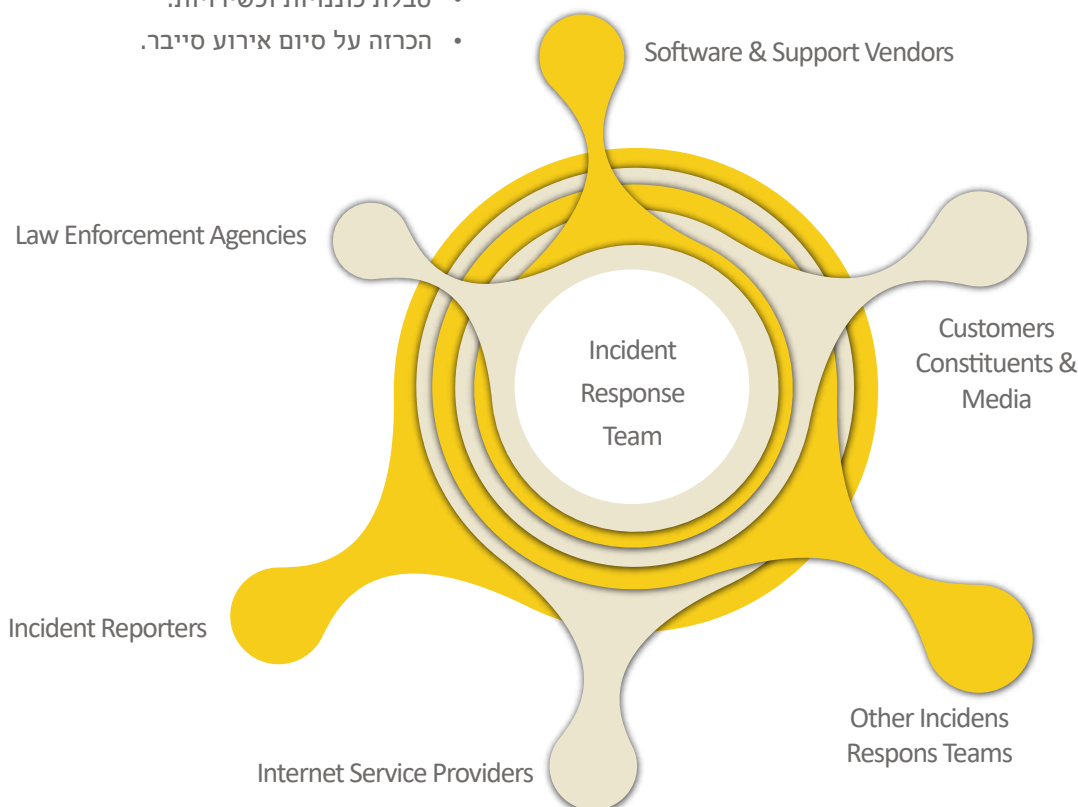
תכנית לניהול משבר סייבר מטרתה ותכולתה

תכנית ניהול משבר סייבר צריכה לשקף הסכמה של הארגון בנוגע לאופן שבו יפעל בזמן אירוע סייבר. מסגרת זו תגדיר חלוקת אחריות ברורה בין כלל הגורמים הרלוונטיים, כלומר מנהלים בכירים, מנהלי הסיכונים, היועצים המשפטיים, הצוותים הטכניים (רשת, תקשורת, אפליקציות, DBA, אבטחת מידע וכו'), אנשי יחסי הציבור והדוברות, יועצי ניהול משבר, מו"מ ועוד.

לאור סביבת חוסר הוודאות הרבה שתשרור בזמן אירוע ולאור ההבדלים (לפעמים אף גדולים) בגישות, הצרכים והאינטרסים של השותפים השונים בצוות ניהול האירוע, שיתוף הפעולה הנכון בין הגורמים הללו אינו טריוויאלי בכלל. לכן מעורבות כלל הגורמים בגיבוש התכנית הוא קריטי ליכולת שלהם לפעול בצורה נאותה בזמן אירוע. בסופו של תהליך, התכנית תשקף באופן פורמלי וממוקד את גישת הארגון לניהול אירועי סייבר.

על התכנית לספק מפת הדרכים ברורה לניהול האירוע, כאשר היא נותנת מענה לדרישות הייחודיות של הארגון, לוקחת בחשבון את האסטרטגיה העסקית, גודל הארגון, המבנה והפונקציות השונות. התכנית תכלול בין היתר התייחסות לנושאים הבאים:

- עקרונות הכוננות לאירוע סייבר, ההכרזה על אירוע סייבר והגדרת רמת האירוע.
- מבנה ואיוש חדרי מצב.
- דרכי תקשורת.
- גופים ותהליכי עבודה ייעודיים לניהול אירוע בסייבר (חדרי מצב).
- אופן ביצוע הערכת מצב ועקרונות הדיווח לבעלי עניין.
- הפעולות הנדרשות בשלבי ניהול האירוע (מזהי ועד להתאוששות) - טכנולוגי, עסקי, משפטי, מוניטני.
- עקרונות לניהול מו"מ במסגרת אירוע סייבר.
- הסתייעות בגורמים ממשלתיים ועבודה מול רגולטורים ורשויות החוק בארץ ובעולם.
- פעילות בתחום המוניטין והתקשורת.
- טבלת כוננויות וכשירויות.
- הכרזה על סיום אירוע סייבר.

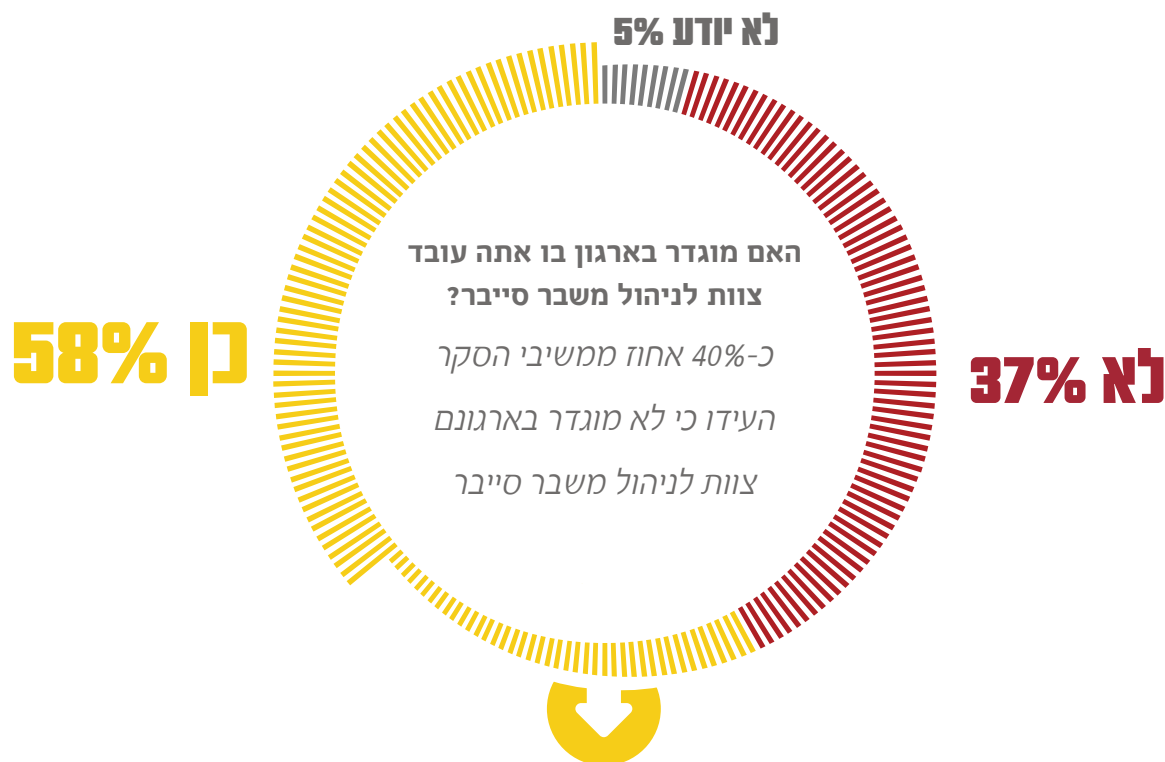


/להיות חכם ולא רק צודק: היערכות ארגונים למתקפת סייבר/

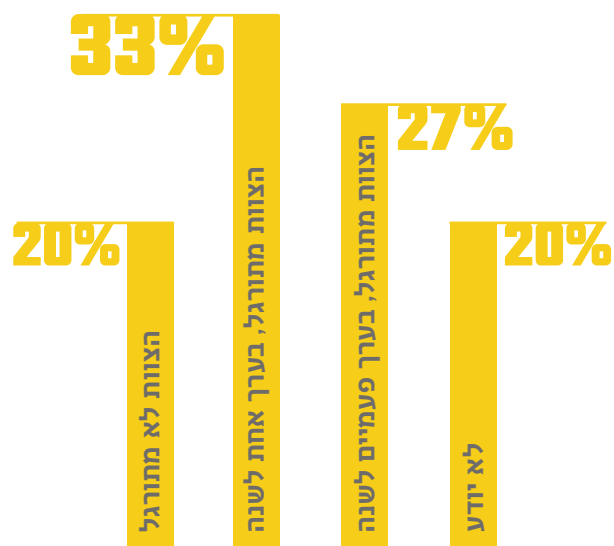
מערכות מידע ומנהלי סיכונים, רובם מהמגזר הפיננסי, מההיי-טק ומגופים ממשלתיים.

כ-40% אחוז ממשיבי הסקר העידו כי לא קיים בארגונם צוות לניהול משבר סייבר. יתר על כן, כ-20% מצוותי התגובה לא תורגלו מעולם.

להלן נתון שצריך לשים אליו לב - בישראל, כרבע מהארגונים סבלו ממתקפת סייבר בעלת השלכות על הפעילות השוטפת במהלך שלוש השנים האחרונות, כך עולה מסקר ארצי שערכנו יחד עם דלויט ואיגוד האינטרנט הישראלי. בסקר השתתפו 150 מנהלי אבטחת מידע,

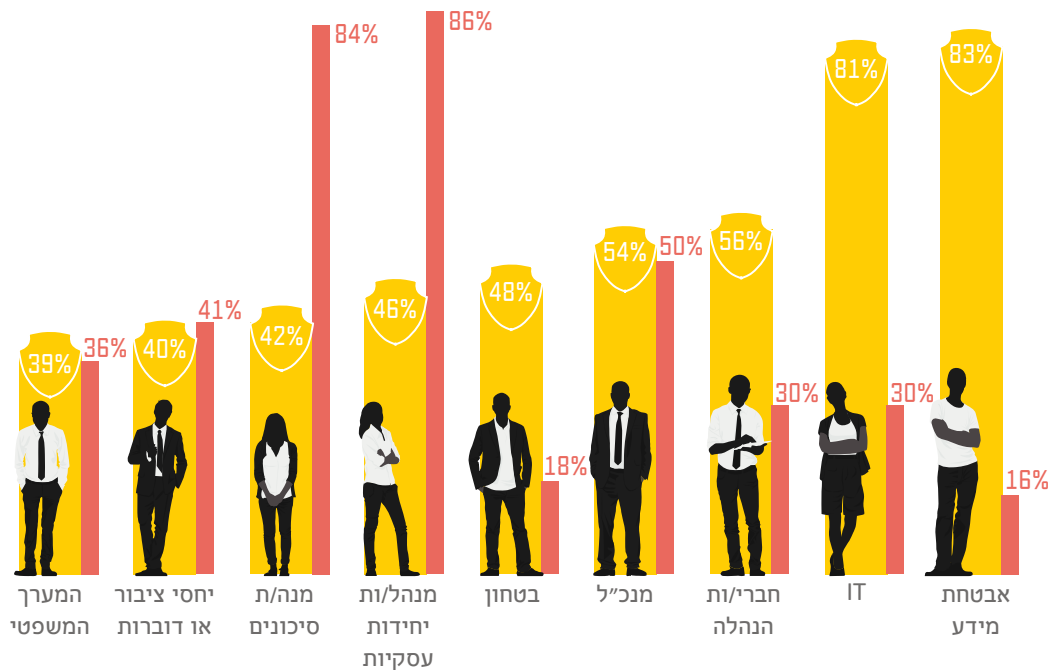


באיזו תדירות הצוות מתורגל?



בנוסף, ביותר מחצי מצוותי התגובה אין בעלי תפקידים הכרחיים, כגון מנהלים עסקיים, מנהלי סיכונים, דוברים, גורמים משפטיים וכו'.

מי הגורמים החברים בצוות ניהול משבר סייבר והאם תורגלו בשנתיים האחרונות?



בשעת משבר. בתוך סביבת חוסר הוודאות הטכנולוגית, הארגון חשוף לסיכונים עסקיים, משפטיים וכמובן סיכון לפגיעה במוניטין. על כן, תגובת הארגון היא קריטית ומצריכה שלל החלטות שאמורות להתבצע בשלב הזה באופן מהיר: איזה מסר מעבירים ללקוחות, לעובדים, לרשויות, לתקשורת; מה לוחות הזמנים, וכמובן מה מותר או אסור לעשות וכו'.

אחת הדרכים האפקטיביות ביותר לבחינת המוכנות הארגונית להתמודדות עם אירוע סייבר היא בעזרת סימולציה המדמה תקיפת סייבר. הסימולציה היא כלי יעיל במיוחד לביקורת, משום שהיא מאפשרת למפות את הפערים בין התכנון לביצוע ואת מכלול הפעולות שנעשו על מנת להגיב נכון בזמן אמת. סימולציה מתאימה תוכל לבחון את יכולת החברה לזהות ולהגיב למתקפות סייבר על פי וקטורים רלוונטיים לארגון, ולבדוק את כשירות הארגון ותהליך קבלת ההחלטות תחת אירוע סייבר. דרך אפקטיבית נוספת היא דיוני "What If". בדיונים אלה מעלים לדיון תרחיש סייבר שקרה בארגון דומה בארץ או בעולם, ומנתחים את ההשלכות של אירוע זה אילו היה קורה בארגון המתורגל. דיונים מסוג זה מעלים תובנות בעלות ערך רב בנוגע לרמת ההיערכות ואילו בקרות נוספו יש לממש, וכן ליכולת ולתהליך ניהול המשבר.

ניתן ללמוד מתוך הוראת ניהול בנקאי תקין 361 בנושא ניהול הגנת הסייבר, על חשיבות ראייה כלל ארגונית באיוש צוות התגובה לצורך התמודדות נכונה עם אירוע סייבר.

על פי סעיף 76 להוראה:

"לצורך ניהול אירוע סייבר יקים התאגיד הבנקאי חדר מצב, ויגדיר בראיה משולבת כלל-תאגידית, את קבוצת העובדים אשר יאיישו אותו, את תפקידיהם, סמכויותיהם, גורמי דיווח פנימיים וחיצוניים, דרכי תקשורת, כלי עבודה וכן נוהלי עבודה פרטניים".

לתרגל או לא לתרגל - זאת השאלה

הדבר הראשון שחשוב להבין הוא כי בעת אירוע סייבר, מתמודד הצוות הטכנולוגי של הארגון עם חוסר ודאות. תוקפים מיומנים יבצעו פעולות הטעיה, כך שלעתים יכול לעבור זמן רב עד שתאותר הבעיה האמיתית. השלבים הראשונים של הטיפול באירוע מתאפיינים בחוסר מידע - מה בדיוק קרה, מה הנזקים, מי התוקף ומה הוא רצה. לאור זאת, הארגון עלול להיתפס במצב של הפתעה, ואי מוכנות לפעולה בסביבת אי ודאות שכזו שעשויה להשפיע על היכולת של מנהלים להוביל את הארגון

להיות חכם ולא רק צודק: היערכות ארגונים למתקפת סייבר

לאור ממצאי הבדיקה של ה-ICO (הרגולטור הבריטי בתחום התקשורת), מנכ"לית החברה, הגברת דידו הרדינג, פוטר 18 חודשים לאחר האירוע ובזיקה ישירה אליו.

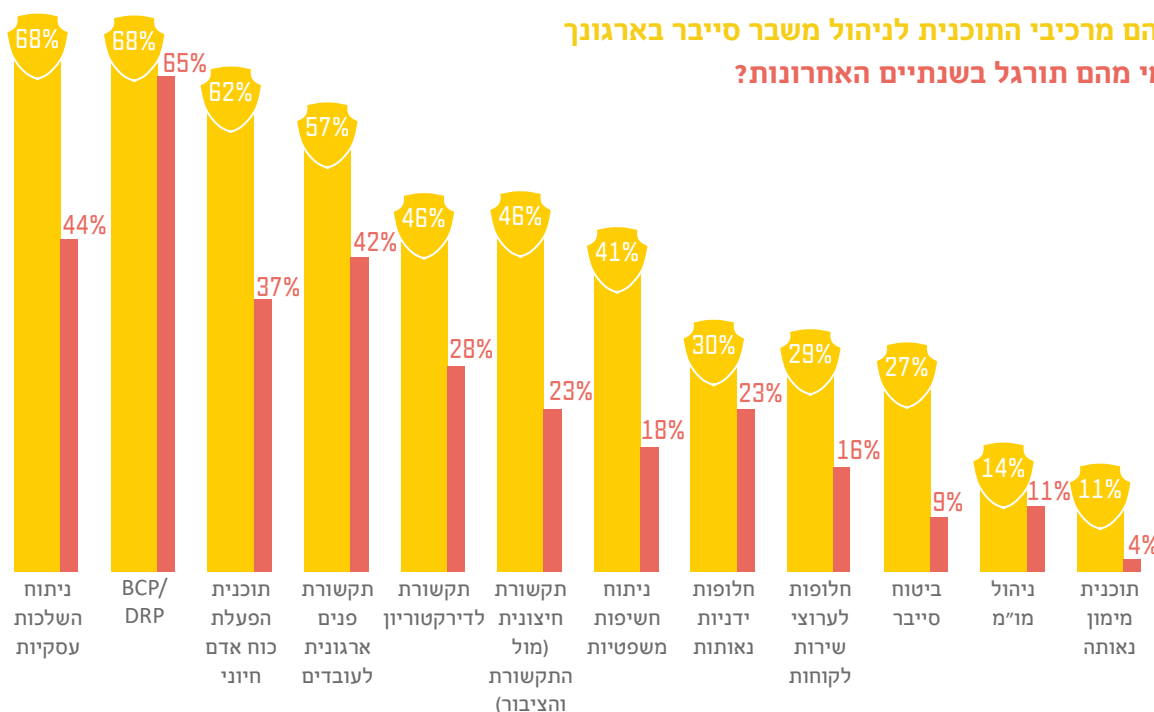
לעומת זאת, באוקטובר האחרון נתקפה חברת תשתית ה-DNS האמריקאית DYN במתקפת מניעת שירות, יש שיאמרו הגדולה בהיסטוריה, על ידי עשרות אלפי רכיבי IoT. אחת הסיבות המרכזיות שבגללן הם הצליחו לטפל באירוע בתוך שעות ספורות היה תרגול, כפי שהעידו על עצמם: "אנחנו מתאמנים ומתכוננים לתרחישים כאלה על בסיס קבוע. אנחנו מתרגלים תסריטים מתגלגלים (playbooks) ועובדים עם שותפים כדי להתמודד עם תרחישים כאלה".

בהמשך לכך, עולה מהסקר כי הנושאים הבאים לא מתורגלים באופן מספק: ניהול משא ומתן עם תוקף, ערוצי תקשורת חלופיים עם לקוחות וניתוח חשיפות משפטיות. אי תרגול נושאים אלה מהווה חשיפה לארגון ופוגע ביכולת שלו להגיב בצורה נאותה בזמן אירוע, שכן כל אלה הן יכולות שללא תרגול קשה מאוד ליישם אותם בזמן אירוע.

דוגמה בולטת להיערכות לא מספקת ותגובה לא נכונה היא של חברת Talk Talk, ספקית התקשורת השנייה בגודלה באנגליה, שחווה מתקפת סייבר משולבת ב-21 באוקטובר 2015.

תגובתה של החברה ומהלכי פתרון הבעיות הראשוניים שניסתה לבצע, באורח מבולבל ועמום, עשויים להעיד שלא הייתה לה תכנית חירום מתורגלת וברורה להתמודדות עם אירוע סייבר שכזה. יומיים לאחר התקיפה התראיינה המנכ"לית לרשת בי.בי. סי. היא נראתה מבולבלת וחסרת אונים, לא ידעה לספק פרטים על זהות הגורם שתקף את החברה, על אומדן הנזק, על יעדי הפגיעה ועל הסיבה לתקיפה. כמו כן, המנכ"לית סיפקה בריאיון מספר אמירות תמוהות, כמו ההבחנה שלפיה "הימים שבהם מידע נגנב כדי למכור אותו ברשת האפלה כמעט אינם, זה כבר לא כל כך רחוק". על פי הערכות, החברה איבדה מעל 250,000 לקוחות, והנזק מהתקיפה הוערך ב-60 מיליון ליש"ט, וכלל היבטים כגון הוצאות לצוותי התגובה לאירוע, עלויות IT, יועצים חיצוניים, פורנזיקה, שיקום המוניטין, אובדן מכירות, עלויות שדרוגים חנים וכ'.

מהם מרכיבי התוכנית לניהול משבר סייבר בארגון ומי מהם תורגל בשנתיים האחרונות?



סיכום

שנם ארגונים שיבחרו להמשיך לעצום עיניים ולקוות לטוב, אולם הנהלות וארגונים שמעדיפים לנהוג באחריות כלפי הלקוחות, העובדים ובעלי העניין האחרים, ייערכו לא רק בגזרת ההגנה אלא גם ייערכו לניהול אירוע סייבר, בין היתר על ידי הגדרת נהלי תגובה, מינוי צוות לניהול אירוע סייבר ותרגול תרחישים רלוונטיים.

כנס שנתי
SAVE THE DATE
4/1/2018

סדנאות

סדנא בנושא כתיבת דוחות ביקורת
סדנא בנושא אתיקה

קורסים

לימודי תעודת ביקורת פנימית
אוניברסיטת בר אילן
קורס הכנה ל-CRMA

השתלמויות שעוד צפויות לנו בהמשך השנה -

ערבי עיון

ערב עיון בנושא מעילות והונאות
ערב עיון על תשוא
ערב עיון בנושא אינפוגרפיקה
ערב עיון על גורמי שורש

סיורים

סיור בצה"ל
סיור בחברת נתיבי ישראל

חברתי

ביקורת על הבר

מדור טכנולוגיות מידע

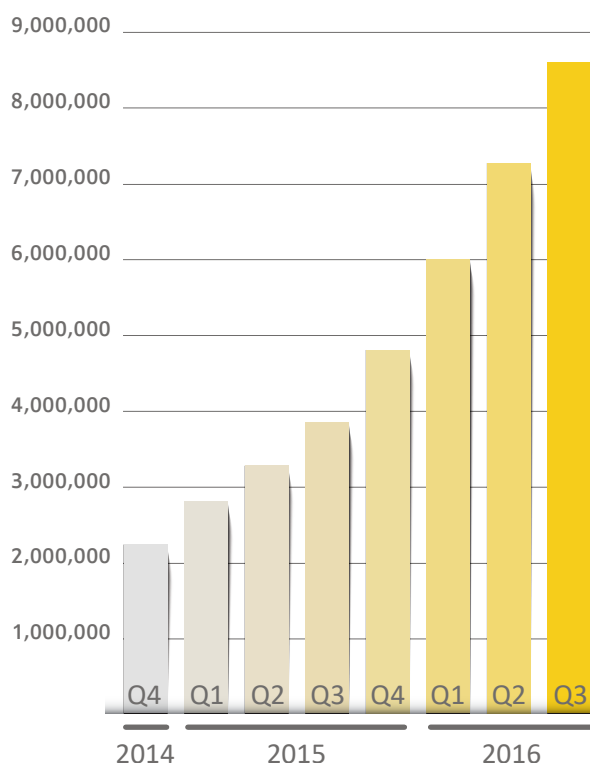
איום ה-Ransomware (כופרה)

מאפיינים ודרכי התגוננות

דוד בר משה, ר"ח, CISA, CRISC, LLM, CRMA, CIA - אמדוקס

תא

התרשים הבא מתאר את קצב העלייה בהיקף הכופרה על פני תקופה



תוכנת כופר ("כופרה") היא נזקה שמגבילה גישה למערכות המחשב הנגוע, ומשמשת לסחיטת תשלום דמי כופר מהמוזקק עבור הסרת מגבלת הגישה. לרוב, תוכנות הכופר מבצעות הצפנה או נעילה של הקבצים תוך שימוש בשיטות הצפנה מורכבות, כך שקשה מאוד להסיר את ההצפנה בלי לשלם כופר עבור מפתח ההצפנה. ישנו סוג נוסף של כופרה, החוסם שימוש במחשב או בהתקן נייד כלשהו. בדרך כלל, תוכנה זו תכלול הצפת הזיכרון של המחשב ושיבוש פעולה תקינה של תוכנות לגיטימיות, על ידי שליחה מסיבית של הודעות או עיכוב תהליך האתחול הרגיל של מערכת ההפעלה, תוך הצגת הודעת דרישת כופר מהקורבן במקום מסך הכניסה הרגיל.

בדרך כלל, כופרה חודרת למחשב כ"סוס טרויאני" המוסווה כקובץ תמים שצורף להודעת דואר אלקטרוני, ופתיחתו גורמת להפעלת ההצפנה. קיימת נטייה לתקוף את אלה שיש ברשותם חומר רגיש או בעל ערך, מהם הסיכוי לקבל כסף גבוה יותר. לרוב, התוקפים דורשים תשלום שיבוצע באמצעות מערכת תשלומים שלא ניתנת למעקב (מטבעות דיגיטליים כדוגמת ביטקוין). ראוי לציין כי ישנם מקרים לא מעטים שבהם גם לאחר תשלום הכופר לא מתקבל מפתח ההצפנה מהתוקף.

בשנים האחרונות הפכו תוכנות כופר לנפוצות יותר. על פי McAfee (חברת אבטחת מחשבים ויצרנית תוכנות אנטי וירוס ואבטחה מובילה בעולם), בשנת 2016 גדל היקף מתקפות הכופרה ב-80%.

בשנה האחרונה מתקיים דיון ער בקרב מומחי אבטחה בנוגע לשאלת ההשלכות של שיתוף פעולה של מותקפים, עם עברייני הסייבר - התוקפים. יש הטוענים כי תשלום הכופר מעודד עבריינות וגורם להתרחבות התופעה. דעות אלו הביאו ביולי 2016 להתארגנות ושיתוף פעולה של מספר ארגונים וגורמי אכיפה בעולם במלחמה נגד הכופרה. התארגנות זו הניבה פעילויות כגון ייעוץ בדרכי מניעה, עזרה בחקירה, פיתוח ושיתוף כלי פענוח הצפנה. אתר האינטרנט של ההתארגנות No More Ransom! מספק מידע רב על כופרה, כולל קישורים לכלי פענוח. הצעד החשוב ביותר למניעה הוא מודעות והטמעה. לכן הדרכת עובדים והגברת מודעותם למתקפות אלו ולדרכי החדירה שלהן הם חיוניים. בפרט מומלץ לחדד את נוהלי העבודה באינטרנט ובדואר האלקטרוני.

הקפידו על התקנת עדכוני תוכנה (אלה כוללים עדכוני אבטחת מידע). יש להפריד רכיבים שאינם יכולים לעבור עדכוני תוכנה לאזורים נפרדים של הרשת הארגונית.

הגנו על נקודות הממשק בין הרשת הארגונית ל"עולם החיצון". ודאו כי הגדרות ברירת המחדל ברכיבים אלה שונות.

הכינו תכנית פעולה למקרה של התקפה. מפו את המידע הקריטי של הארגון ואת הגישה למידע.

הפעילו כלי "אנטי-ספאם", היעילים בדרך כלל במתקפות כופרה.

בצעו תרגילים כדי לוודא שהתכנית אפקטיבית.

דאגו לסגמנטציה של הרשת הארגונית.

ודאו כי הגיבויים תקינים ומתבצעים בצורה שוטפת.



**להלן מספר צעדים מומלצים
לצמצום הנזק של מתקפות כופרה**

סיכום

תוכנת כופר היא תופעה שההיקף שלה הולך וגדל כל הזמן. כדי לצמצם את החשיפה לפגיעה ואת הנזקים שהיא עלולה לגרום, יש להיערך הן באמצעות הסברה והדרכת העובדים, והן בתכנון תכנית פעולה להגברת יכולת ההתמודדות של מערכות המידע בארגון עם פגיעה פוטנציאלית.

ניהול סיכונים ארגוני - סדק בתודעה

תארת
יעל קלו-מור, MBA

ולשמור על המוניטין שלו, ובעיקר בנושאים שהיכולת לנהל אותם בידיו, כגון שביעות רצון הלקוחות, איכות המוצרים, הסביבה הפיננסית, מתחרים, תמיכת מערכות המידע ועוד - כל מה שקריטי להצלחה.

מנכ"ל שבחר להטמיע את תהליך ניהול הסיכונים אמר: "אנחנו נטמיע ניהול סיכונים ארגוני, כי יש כסף על הרצפה". וזה כל הסיפור: ניהול סיכונים ארגוני "מרים כסף" מהרצפה או מונע ממנו להישמט.

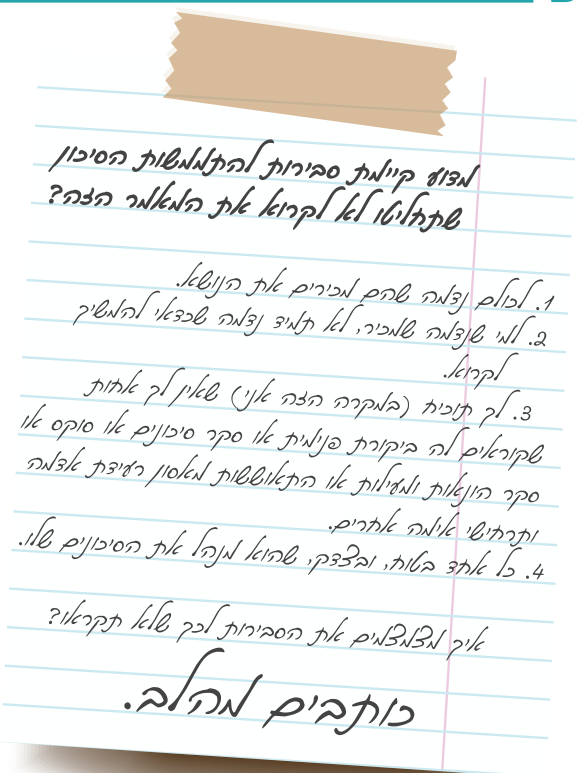
איך עושים זאת?

בשיטתיות, בהסדרת תהליך בתדירות קבועה, ובכלים מקצועיים שיהוו קטליזטור להגברת השיח בסוגיות אלו וליצירת ערך לארגון.

איינשטיין אמר "לא נוכל לפתור את הבעיות עם אותה שיטת חשיבה שבה יצרנו אותן". כלומר אם נוצרו סיכונים, ניהול הסיכונים הארגוני מציע לחשוב אחרת על אופן ניהולם.

החשוב לצד הדחוף (הן אנחנו יודעים מי מנצח)

ניהול סיכונים ארגוני הוא כלי נוסף לארגון, לצד אסטרטגיה, מדידים ותכניות עבודה. הוא הדבק - החוליה המקשרת. התהליך מסייע לארגון קודם כל לראות תמונה כוללת, כל מנהל ועובד עושים את המיטב בתחום אחריותם, ועדיין קיים הכרח לראות את הדברים במבט-על, לדבר בשפה אחידה, לאתר, למדוד ולהחליט כיצד לפעול בנושאים שיוגדרו כמהותיים. ומכאן שמדובר בתהליך שמשפיע משמעותית גם על חלוקת תקציבי השקעות, וכל כך בתבונה על בחירת הנתיב לקשב הארגוני.



מתי לאחרונה שאלתם את עצמכם מה עלול למנוע ממני לעמוד ביעדיי?

תהליך ניהול סיכונים ארגוני נועד להטמיע תהליך שיאפשר לכל מנהל לבחון באופן שוטף באילו מקומות הוא עלול להגיע לתוצאות שונות מהמתוכנן. להכריח אותו להביט ביעדים, ולבדוק בשיטתיות מה עלול למנוע ממנו להשיגם. תהליך ניהול סיכונים ארגוני מתמקד בנושאים השוטפים המעסיקים ארגון, בנושאים המאפשרים לו לעמוד בתוצאות

פרופ' כהנמן, זוכה פרס נובל לפסיכולוגיה וכלכלה, מספר שכדי לגרום למנהלים בחברת סטארט-אפ לחשוב מה עלול למנוע מהם להצליח, הוציאו אותם מחוץ למשרדים שלהם למרחב אחר, ורק אז הם נשאלו: נניח שעברו חמש שנים והסטארט-אפ נכשל, מה היה יכול להכשיל אותו? רוב האנשים מאוד מאמינים במה שהם עושים ומאוד קשה להם להניח שהדברים לא פועלים או לא יפעלו כפי שהיו רוצים. ניהול הסיכונים שואל שאלות כאלו.

כדי להטמיע את התהליך נדרשים: שפה אחידה, הליך מובנה שמאפשר שקיפות אובייקטיביות, וקטליזטור לחשיבה עמוקה ולטיפול בחשוב ולא רק בדחוף. יש צורך לשקול ולהחליט: מהו סיכון מהותי? איך מודדים אותו? איך אפשר להפחית אותו? מה עלול לקרות וכמה זה משמעותי? מי מטפל ואיך? וחוזר חלילה. וכמו באופניים, אסור להפסיק להניע את הפדלים של התהליך הזה.

התהליך מסייע ליצור צוותי חשיבה טרוגניים, להטיל ספק בפרות קדושות, לבחון שוב או לראשונה סוגיות שוטפות וכשלים החוזרים על עצמם פעם ועוד פעם ועוד פעם.

הרבה לפני בחינת השגת היעדים - KPI - תהליך הנהוג במרבית הארגונים, נברא כאן תהליך שמסתכל בלבן של העיניים, ורצוי בעיניים של ההנהלה כולה, ושואל: מה הסבירות שנשיג את היעדים שלנו? האם אכן אנו בוחרים לעשות משהו? מי אחראי על זה ומתי? וכן, מול תהליך הניהול הקיים, שעיקרו תוצאתי ואינו מבוסס סיכונים, זה מרגיש סוג חדש של נביא בעירו.

זה נשמע כל כך פשוט, כולנו כל כך בטוחים שאנחנו עושים את זה כשגרה, ולמרבה הפלא, לא! למה לא? כי זה נגד הטבע האנושי. כי זה לא כיף. ולכן נולדה השיטה והססמה המאוד נכונה: "קשה באימונים קל בקרב".

אנחנו שונים זה מזה

נניח שהייתם מכנסים בחדר אחד את הנהלת החברה או החטיבה, ושואלים את המנהלים את השאלות הבאות:

מה זה ניהול סיכונים?

מה זה סיכונים תפעוליים?

מהם חמשת הנושאים התפעוליים שעלולים למנוע מהארגון להשיג את יעדיו בשנת 2017?

מי אחראי על כל אחד מהם?

מה תהיה עוצמת הנזק?

מהם היעדים העקרים שלא הושגו בשנה הקודמת?

ניהול ארגון הוא כמו ג'אלינג עם אלפי כדורים ואלפי ידיים, כאשר כל אחד עסוק בלהבטיח שהכדורים שבטווח הראייה שלו לא ייפלו. אך מי רואה את סך הכדורים שנופלים? ומי רואה את כל הכדורים שבאוויר בזמן נתון? ומי רואה אם יש כדורים זחים שכל אחד מעיף למקום אחר בקצב אחר? ומי רואה כדורים שעפים מבחוץ ומי אוסף כדורים מהרצפה?

ניהול סיכונים ארגוני זה לראות מלמעלה את כל התמונה

זהו תהליך פרואקטיבי ושיטתי המתמקד בהצגת חצי הכוס הריקה; באופן שבו כלל הסיכונים "מונחים על השולחן" ומתועדפים, וגורמי הסיכון מנותחים על מנת לתקן את שורש הבעיות באופן שהארגון ילמד מטעויות ויצמצם את הסבירות לחזור עליהן.

מנכ"ל שמחליט להטמיע את נושא ניהול הסיכונים בארגון שבראשו הוא עומד, מחליט למעשה להכניס תהליך שמחייב את הארגון לעצור מפעם לפעם ולוודא שתהליכי העבודה שלו, מערכות המידע שלו, העובדים, כולם תומכים ברגע נתון בהשגת היעדים ולוקחים בחשבון את כל מה שניתן לחזות שישפיע על התוצאות מחוץ ומבית.

ניתן לבחור את הדרך. זה מודולרי. זה כמו כל יחידה אחרת שלא היינו מוותרים עליה בארגון. זה חלק מאורח החיים ולא דומה לגוף ביקורתי או לסקר. מדובר באחריות ישירה. בקו ראשון של הניהול עצמו.

תהליך ניהול סיכונים ארגוני מסייע להניח על המפה סיכונים, נושאים, תהליכים או פרויקטים שההנהלה החליטה שעלולים למנוע מהארגון להשיג את יעדיו, רווח, מוניטין, הכנסות, מוצרים, שווקים, חוקים ותקנות, וכמובן שניתן להוסיף או לגרוע מרשימה זו.

התהליך עוזר, שלא לומר מכריח, לאתר:

תהליכים שאינם שלמים.

תהליכים-נושאים חוצי חברה (ללא גורם אחראי מתכלל - נושאים יתומים).

נושאים שנותרים משנה לשנה בתכניות העבודה.

חלומות שחלמנו ולא קל להגשים.

תחזיות שנתנו בעל כורחנו ואין בידינו להשיגם.

פרויקטים שגדולים הרבה יותר ממה שהנחנו.

בחליפה או בגינס קרוע?

מנהל סיכונים של ארגון בינלאומי גדול אמר שהטמיע תהליך בלי להשתמש באף אחת מהמילים "האקדמיות", כגון תכניות הפחתה, מדדי התרעה, הערכת סיכון, מתודולוגיה ועוד, אלא החליף אותן במילים יותר נגישות לעובדי הארגון שלו.

כלומר, פחות חשוב באיזו מתודולוגיות ומדיניות נבחר. העיקר שנבחר להסתכל, והעיקר שנבחר לדבר בשפה אחידה ונשאל מה אנחנו צריכים כדי להשיג את היעדים, איך עושים את זה ומתי.

העיקר שנזהה עד כמה שניתן ונשלוט בתוצאה הרבוענית/שנתית של המשאבים שבידינו: אנשים, תהליכים ומערכות. העיקר שנייצר לנו דרך!

כך גם נרצה לבחון את איכות התהליך שלנו. השאלה אינה אילו כלים יש בתזמורת, אלא האם היא מנגנת היטב.

בעברית קלה

בעברית קלה: המשמעות של ניהול סיכונים ארגוני, בין היתר, הוא מינוי גורם אחראי שייצר כלים למנהלים בארגון על מנת לשכלל את יכולתם לאתר סיכונים ולצמצם את השפעתם, כך שיהיה ניתן לייצר תמונה שלמה ורחבה יותר. להבטיח שמנהלים יפנו זמן בתדירות קבועה, יאתרו סיכונים, ימדדו אותם ויתכננו תכניות להפחתתם והכול בשפה אחידה. התפקיד של מנהל הסיכונים, בנוסף על תפקידיו האחרים, הוא להיות קטליזטור ולחולל אצל מנהלים ועובדים תהליכי חשיבה ברבדים של מה חשוב (מעבר לרבדים של הדחוף).

להוציא לבת היענה את הראש מהחול

תחשבו על מנהל פיתוח ששואלים אותו פעם בחודש מה היעדים שלו ומה עלול להשתבש. מה השתנה בסדרי העדיפויות שלו ואיך זה ישפיע על הלו"ז, איפה יש צווארי בקבוק ואיזה ממשק צריך לשכלל. זה לא בא לנו לבד. אין לנו זמן! וככה עם מנהל הכספים והלוגיסטיקה ומערכות מידע והדוברות, וכל בעל תפקיד משמעותי.

ברור שכולם עושים כמיטב יכולתם. אבל מה עושים? מה הכי קריטי בראייה חוצת

אילו תהליכי הפקת לקחים בוצעו? מה מאיים על המוניטין שלנו באופן שבו אנחנו מתנהלים?

מה הנושא הקריטי ביותר למטרת הרווח השנה?

סביר מאוד שכמות התשובות לשאלות אלו תהייה ככמות האנשים היושבים בחדר.

ואם נמשיך וננסה לתעדף או להגיע לראייה משותפת, סביר מאוד שזה יהיה אתגר מורכב, מפני שכל מנהל רואה את הדברים מזווית הראייה של ניסיונו, של תחום אחריותו, של תפיסת הסיכון שלו, של הראייה התהליכית שלו, של האסרטיביות שלו, של המקורבות שלו, וגם כי כל מנהל יבחר את מידת השקיפות והשיתוף שלו, ומכאן המורכבות. הסיבה לכך היא שלכל אחד מאיתנו יש התבוננות ותפיסת עולם אחרת על הסבירות להיכשל ועל הסיכוי להצליח ועל מה זה אומר "אני מטפל בזה".

זו ההתנהלות האנושית בתוך ארגון המורכב מאוסף של אנשים. היינו רוצים ליצור תרבות שמשתלבת עם תפיסת ההנהלה לאופן ניהול הסיכונים המועדף עליה... ואז השאלה היא לא אם, אלא איך גורמים להנהלה להגיע לראייה משותפת על התהליכים, המערכות והנושאים המרכזיים שעשויים לפגוע במטרות הרווח, בתוך ניגוד עניינים מובנה, בתוך מרקם אנושי מגוון, בתוך "צרות" היום-יום? ומעל זה - איך מאתרים את גורמי הסיכון הספציפיים כדי לדעת לאן לנתב את המשאבים ואת מה למדוד?

זאת פריצת תודעה דרמטית, העניין הזה של תהליכי חשיבה מובנים פרואקטיביים ומתוזמנים. זה מוליך מהר מאוד למקום של "איך לא חשבו על זה קודם".

בשבחה של השפה שפת ניהול הסיכונים

ניהול סיכונים ממציא, יחד עם הארגון, שפה אחידה:

מה זה נושא בלגית סיכונים (סיכון)

אילו סוגי ניהול סיכונים ראויים

מה זה אחראי אל סיכון

איך לוצים סיכון

מה זאת אמת סיכונים בינלית

מה זה אטל בסיכון?

לצערי, בסוגיה של בריאות הגעתי לגיל שקופת החולים שלי מסדרת לי תור, מוותרת לי על הפניה, מתקשרת לקבוע לי תאריך והכול. הייתי רוצה לחשוב שזה נובע מאהבה אליי, אך לא. זה בעיקר מהחוכמה של למנוע את הוצאות הטיפול שעלולות להיגרם בהיעדר גלוי מוקדם. כלומר יש כאן ניהול סיכונים מושכל!

המתנה

דמינו חדר ישיבות הנהלה שבו, כמו במסכי הבורסה, נראים כ-20 נושאים/תהליכים/פרויקטים שברגע זה הם מוקדי תשומת הלב העיקריים שלכם, וצבעם אדום-כתום או צהוב בהתאמה, ועל כל אחד ידוע מי האחראי היחיד שלו ומה מקבלי ההחלטות בחרו לעשות ואיך ומתי. אז בינתיים עוד אין כזה מסך, אולי עוד יהיה... אבל התהליך הזה מניח משקפיים חדשים ופותח זוויות שלא בהכרח נראו קודם לכן.

לא בא לי

תחשבו, כל אחד בביתו, שמישהו מציע לנו לעצור בכל חודש ולבדוק מה עלול לקרות ומה אנחנו רוצים ויכולים לעשות כדי למנוע נפילות. כמה זה לא קורה לנו באופן טבעי, כמה לא בא לנו לדעת, ועד כמה היינו חוסכים כסף, משפרים את איכות חיינו ולפעמים גם מצילים את חיינו (במונחים של בדיקות רפואיות מקדימות).

סיכום

הכול לגיטימי - הכול פתוח, הכול יכול להופיע במפה - מהכנסת מערכת מחשב, תהליך שמירת ידע, השבתת החברה, ממשקים, שביעות רצון לקוחות ועוד. אין פרות קדושות. בכל דבר מוזמנים להטיל ספק ובשיטתיות.

נושאים שידענו שמהווים חשיפה ולא התפננו להכיר או לטפל בהם מקבלים הזדמנות, הזדמנות פז.

אז איך זה קורה? מחליטים שרוצים, ממנים אחראי, לומדים על מה מדובר, משוחחים עם מנהלים כדי לבחור נושאים מהותיים - top down, מכניסים שיטה לתעדוף ולבניית תכניות הפחתה, יוצרים תהליך מחזורי ושוטף, מדברים את זה יום ולילה. לא מפסיקים לדבר את זה.

כזה פשוט? בכלל לא. עם זאת, הרבה יותר פשוט מלהיות מופתעים... אחרי הנזק... אחרי שכבר אין מה לעשות.

ובמשפט מסכם: אחרי שארגון מתחיל לחוות את התהליך, המנהלים אומרים (או מלינים) "זה לא ניהול סיכונים, זה פשוט ניהול..."

ה כל הסיפור של ניהול סיכונים ארגוני.

להכריח לפנות זמן, לייצר תהליכים של חשיבה שאינה באורח החיים שלנו, לתת כלי מדידה אחידים, לייצר שפה אחידה, להצליח לראות תמונה שלמה.

זה האתגר, זאת ההבשלה והלמידה, ובהדמיה: להכניס מראה מעל הארגון ולהביט לעצמנו בעיניים. זה רק מוסיף ולא גורע, זה מתאים את עצמו, זה משנה בתוך זמן קצר את השפה, את ההתייחסות ואת המודעות.

וכמו אבן קטנה שנזרקת לאגם שקט, האפקט הוא מעגלים רבים שיוצר התהליך, שנוגע בכל ההתנהלות בארגון כמעט באופן מדי.

אם הצלחתם להתחיל ולייצר מפה עם הנושאים הכי קריטיים לארגון, אז אין דרך חזרה. במו עיניי ראיתי הנהלות דנות בנושאים שהיו טאבו, מנהלים מבררים לראשונה איך מתנהל תהליך באחריותם, וגורמים שונים שמשפיעים על אותו תהליך או פרויקט יושבים יחד ומוצאים צווארי בקבוק וסיכונים ופותרים אותם.

ביקורת ברשות המקומית - להבין, לשנות, להשפיע

מלכה דרור, CIA, CISA, CRISC - עיריית ירושלים

תא

גידול באוכלוסיית הערים במקביל להעברת שירותים מהשלטון המרכזי למקומי ללא תוספת תקציב הולמת.

תהליכי העיור שמתרחשים בעולם בעשרות השנים האחרונות, מובילים יותר ויותר אוכלוסיות להתגורר בערים הגדולות. תהליך זה מתרחש גם בארץ, ובאופן מואץ יותר מאז תחילת המאה העשרים ואחת. בעיר ירושלים קיימת מגמת גידול באוכלוסייה נוכח הריבוי הטבעי של הקבוצות המאכלסות אותה (מספר הילדים בעיר הגיע לכ-300 אלף בשנה האחרונה), ולנוכח בלימת מגמת ההגירה השלילית.

במקביל למגמה זו, השלטון המרכזי בארץ מעביר, במשך השנים, יותר ויותר שירותים שהיו בעבר באחריותו לאחריות השלטון המקומי - לרוב בלי להוסיף תקציבים המאפשרים מתן שירותים אלה. די אם נציין לדוגמה את הדרישה להקמת צהרונים בעקבות המלצות ועדת טרכטנברג, ואת הדרישה להציב שמירה בגני ילדים לנוכח המצב הביטחוני בירושלים, וזאת, עד כה, בלי להקצות את התקציב הנדרש ליישום דרישות אלה.

פער גדל בין רמת השירות המצופה מהרשות המקומית לזו המסופקת לתושבים

קיים פער הולך וגדל בין הציפיות לרמת שירות גבוהה מצד התושבים לבין יכולתה של הרשות לממש ציפיות אלו: מודעות גוברת של הציבור לרמת השירות שהוא מקבל מהרשות המקומית, מביאה לתחרות בין העיריות על מתן שירות טוב יותר לעסקים, לתושבים ולמבקרים, תחרות שבאה לידי ביטוי בתהליכי שיפור השירות והתמקדות בצורכי הלקוח. מנגד, הרשות המקומית מתקשה לממן את העלייה ברמת השירות הנדרשת, בהיעדר הגדלה של המקורות התקציביים בהתאמה. אם נוסיף לכך את העובדה

במאמר זה אסקור מספר פעולות ושיטות עבודה שיישמו בשנים האחרונות בביקורת העירייה. פעולות ושיטות אלו מאפשרות לביקורת בעיריית ירושלים להישאר רלוונטית ואף להיות גורם פרו-אקטיבי - גורם המוביל ומדרבן את הרשות לשפר את השירות הניתן ללקוחות - תושבי העיר, ולהשיג את המטרות והיעדים שקבעה לעצמה.

מגמות של שינוי

בשנים האחרונות רשויות מקומיות בארץ, ועיריית ירושלים בין המובילות שבהן, פועלות בקדחתנות לאימוץ שיטות ניהול מתקדמות, ובכלל זה: קביעת מטרות ויעדים, פיתוח כלים חדשניים למדידה של ביצועים, פיתוח מנהלים והטמעת טכנולוגיות חדשניות של "עיר חכמה" (המשתמשת במידע ובטכנולוגיות מתקדמות כדי להיות יעילה יותר בשימוש במשאבים, בחיסכון בעלויות ובאנרגיה, ובשיפור איכות החיים לתושבים).

למול שינויים אלה, גם פונקציית הביקורת ברשות המקומית, כדאי לה שתפעל לפי תפיסה הולמת וחדשנית, תגדיר אסטרטגיה מתאימה, ותאמץ כלים טכנולוגיים וניהוליים נכונים. פונקציית ביקורת שלא תתאים עצמה לשינויים המתחוללים ברשות שהיא מבקרת, תפסיק למלא את ייעודה, תישאר מאחור ותהפוך במהרה לגוף חסר חשיבות ובלתי רלוונטי.

שלוש המגמות, משנות המציאות, ברשויות המקומיות בשנים האחרונות מוצגות להלן.

בנוסף, רכשנו והטמענו כלי ביקורת חדשניים ששיפרו את איכות העבודה, שיפרנו את שיתופי הפעולה עם גורמים בעירייה ומחוצה לה, ואת תהליכי העבודה מול הנהלת העירייה, ובימים אלה אנו מעצבים מחדש את סל תוצרי הביקורת.

סנכרון עבודת הביקורת עם תכנית החומש העירונית

בשנת 2015 השיקה עיריית ירושלים, לאחר תהליך מעמיק בסיוע אנשי אקדמיה מהשורה הראשונה בעולם, תכנית חומש אסטרטגית לעירייה. עיקרה של התכנית: התמקדות בלקוח, והפיכת העיר ירושלים לאטרקטיבית לעסקים, לתושבים ולמבקרים.

במסגרת התכנית אימצה הנהלת העירייה את התפיסה שכדי להדביק את הפערים התקציביים הנדרשים לצורך שיפור השירות, יש הכרח לפעול להגברת היעילות, האפקטיביות והחיסכון, וזאת בדרך של אימוץ חדשנות טכנולוגית וניהולית.

למול תכנית החומש האסטרטגית של העירייה שאלה נחשפנו, שאלנו את עצמנו כיצד פונקציית הביקורת העירונית צריכה לפעול כדי להתאים את עצמה לשינוי המתרחש בעירייה, וכדי להמשיך להיות בעלת ערך לעירייה. החלטנו לערוך תכנון אסטרטגי מקביל לפונקציית הביקורת בעירייה, כדי לוודא שלמול תכנית החומש העירונית, יהיו לנו הכלים והיכולות הנדרשים על מנת להמשיך לספק תובנות לעירייה ולהיות אפקטיביים ורלוונטיים.

במסגרת התהליך האסטרטגי שערכנו בהשתתפות כל הצוות ובהנחיית יועץ חיצוני מומחה לאסטרטגיה:

- למדנו את התכנית האסטרטגית העירונית,
- ערכנו ניתוח SWOT (חוזקות, חולשות, הזדמנויות ואיומים) שבאמצעותו אספנו עשרות פריטי מידע, שאותם ניתחנו.
- ראינו את בעלי העניין המרכזיים של הביקורת, ולמדנו מהם כיצד אנו נתפסים היום בעיני בעלי עניין אלה, ומהן הציפיות מהביקורת בעתיד.
- בהמשך בנינו את "מפת הדרכים" שלנו, הכוללת זיהוי והגדרת הייעוד, החזון והערכים של הביקורת בעיריית ירושלים.
- קבענו מטרות, יעדים, דרכי פעולה, מדדים וכלים למדידת הביצועים.

ערכת סקר סיכונים בקרה תוך הטמעת תפיסת "ניהול סיכונים" בקרב מנהלים בעירייה.

שברוב הרשויות המקומיות עדיין נהוגות שיטות עבודה מסורתיות (ללא אסטרטגיות, מטרות, יעדים ומדדים), הרי שהפער בין הציפיות לבין השירות הניתן בפועל רק מחריף.

זמינות של טכנולוגיות חדשניות לשיפור השירותים הניתנים על ידי הרשות המקומית

ההתפתחות הטכנולוגית המואצת תחת המושג "עיר חכמה", מהווה הזדמנות לשיפור תהליכים ברשות המקומית. בניגוד לשתי המגמות הראשונות, מגמה זו מאפשרת לרשויות המקומיות שישכילו לאמצה, להדביק את פערי התקציב באמצעות התייעלות והטמעת כלים חדשניים זמינים, שניתן להסב אותם וליישם לטובת שיפור השירות, לרוב אף ללא הגדלת תקציבים.

הערכות הביקורת בעיריית ירושלים על רקע המגמות

על רקע קיומן של מגמות אלו, נוכחתי לדעת עם היכנסי לתפקידי כמבקר עיריית ירושלים, שכדי שפונקציית הביקורת תהיה רלוונטית ומשמעותית ותוכל להשפיע על הנעשה בעירייה, על הביקורת לקדם פעולות נוספות - פרו-אקטיביות, הקשורות לאקלים הארגוני ולממשל התאגידי בעירייה ובתאגידים. כמו כן, מן הראוי להטמיע שיטות עבודה וניהול מתקדמות וחדשניות, תחילה בביקורת ואחר כך גם בעירייה עצמה. זאת, מלבד עבודת ביקורת שוטפת הנדרשת מתפקידה הסטטוטורי של ביקורת העירייה.

מטרת הפעולות הללו היא הגברת השפעתה של הביקורת הפנימית על הארגון תוך ניצול יעיל של המשאבים הקיימים.

ביקורת פנימית - פעולות נדרשות

להלן סקירה של הפעולות הנדרשות על מנת להשיג את יעדי הביקורת לאור שלוש המגמות שתוארו לעיל.

שיפור מקצועיות צוות הביקורת ואימוץ תקנים מקצועיים בין-לאומיים

כצעד ראשון החלטנו לאמץ את התקנים המקצועיים של ה-IAA ולהטמיע שינוי בתפיסת הביקורת בעירייה, בקרב הנהלת העירייה ובקרב צוות עובדי הביקורת. כך, מתפיסה הרואה בביקורת גורם חיצוני לעירייה (בדומה למבקר המדינה), הפכנו לפונקציה שהיא חלק מהארגון ופועלת במקצוענות ובדרכים מגוונות כדי להביא ערך מוסף לארגון. כחלק ממהלך זה פעלנו להכשרת הצוות באמצעות קורסים ייעודיים לצורך קבלת הסמכות בין-לאומיות בביקורת.

“פתחי השירות” והמרכזיות שהביקורת ייחסה לנושא בתכניות העבודה שלה, תרמו לשינוי מהותי בתפיסת השירות של העירייה בקרב הנהלת העירייה והעובדים, ולשיפור השירות הניתן לתושבים.

מיצוי הכנסות העירייה ממשרדי ממשלה

השתתפות משרדי הממשלה במימון הרשויות המקומיות היא אחד המקורות החשובים ביותר בהכנסותיהן. נוסף על המענק הכללי המועבר ממשרד הפנים, משרדי ממשלה ייעודיים (כגון משרד החינוך) מממנים שירותים ממלכתיים שבתחום סמכויותיהם ואשר מוענקים באמצעות הרשויות המקומיות. בשנת 2015 תוקצבו ההכנסות לעיריית ירושלים ממשרדי הממשלה בכ-1.3 מיליארד ש”ח (לא כולל מענק הבירה), ומהם 756 מיליון ש”ח ממשרד החינוך.

לאור מהותיות ההכנסות מהשלטון המרכזי, כללנו בתכנית העבודה של הביקורת סדרה של בדיקות לבחינת מיצוי הכנסות העירייה ממשרדי ממשלה ומגורמים חיצוניים, ובכלל זה: משרד החינוך, משרד הרווחה, המשרד לביטחון פנים ומפעל הפיס. דוחות ביקורת אלה הניבו לעירייה הכנסות בהיקף כספי מהותי (הן בהחזרים כספיים ישירים והן במניעת הפסדים עתידיים).

“הפיכת הפירמידה” של הבקרה בתאגידים העירוניים וחיזוק הממשל התאגידי

בעיריית ירושלים יש למעלה מ-40 תאגידים עירוניים ומעין-עירוניים המשלימים בפעילותם את השירותים שהעירייה מחויבת לספק. על פי המדיניות של ראש העירייה, העירייה היא הרגולטור, ואילו פעילות השטח בכל המישורים מתבצעת בפועל באמצעות התאגידים. כך למשל פעילות בינוי כיתות לימוד של העירייה הועברה לתאגיד עירוני המתמחה בבינוי, ופעילות הפקת האירועים הועברה, ברובה, לתאגיד עירוני המתמחה בהפקת אירועים.

מאחר שמדובר בגופים מבוקרים, כהגדרתם בפקודת העיריות, מתחייבת היערכות מתאימה של הביקורת בעירייה כדי שניתן יהיה להתמודד עם היקף מהותי של פעילות עירונית המועברת לתאגידים אלה.

בבחינה של מצב הביקורת הפנימית בתאגידים, התברר שבתאגידים העירוניים חסרה רגולציה המחייבת קיום מערך בקרה פנימית בתאגיד. מנגד, התברר שמנהלי התאגידים חווים ריבוי גורמי ביקורת חיצוניים, בכלל זה: מבקר המדינה, מבקר העירייה, רשם העמותות במשרד המשפטים, משרד הפנים ומשרדי ממשלה רלוונטיים נוספים.

מצב זה, של ריבוי ביקורת חיצונית ללא ביקורת פנימית נאותה, דרש שינוי, משום שהתברר שהביקורת לא הייתה

- במקביל לתהליך האסטרטגי, סיימנו את מיפוי הסיכונים בעירייה, והכנו תכנית חומש לביצוע מטלות ביקורת.
- למיפוי הסיכונים שיזמנו בעירייה קבענו שתי מטרות עיקריות:

« האחת - גיבוש תכנית עבודה רב-שנתית שתהיה מקבילה לתקופה הקבועה על ידי העירייה כתקופת התכנית האסטרטגית (תכנית החומש).

« השנייה - חשיפת הנהלת העירייה לתחום ניהול סיכונים במטרה להניע תהליך ניהול סיכונים מובנה בעירייה ברמת ראש העירייה, מנכ”ל העירייה וראשי המנהלים. זהו אחד הכלים באפוד הכלים הניהוליים המשמשים את המנהלים בתהליכי קבלת ההחלטות והניהול השוטף, במטרה להביא ערך מוסף ושיפור יכולת השגת יעדים ומטרות.

- בשנת 2016 השלמנו, בתהליך שיתופי עם מנהלים ועובדים בעירייה, את מיפוי הסיכונים, וגיבשנו תכנית עבודה רב-שנתית לחומש. כפועל יוצא, הנהלת העירייה נחשפה לתפיסת “ניהול סיכונים”, ומנכ”ל העירייה החליט להטמיע תפיסה זו בדיוני תכניות עבודה ובתהליכי הניהול השוטף.

שילוב תכנון מטלות הביקורת, הנגזר מסקר הסיכונים, בתיאום ובשילוב עם התכנון האסטרטגי המתווה את דרכי הפעולה להשגת החזון, המטרות והיעדים של הביקורת, יגבירו את הביטחון שנמשיך לספק ערך לבעלי העניין שלנו.

התמקדות בשיפור השירות

מאחר שנושא השירות הניתן על ידי העירייה לתושב הוא במהות תפקידה של הרשות המקומית, הצבנו נושא זה בראש סדר העדיפות של הביקורת. כפועל יוצא:

- החלטנו למקד מאמץ שיביא לשיפור השירות הפרונטלי, המענה הטלפוני והאינטרנטי הניתן בעירייה.
- לצורך זה: גיבשנו מתודולוגיה חדשנית לבדיקת הנושא, מנקודת מבטו של מקבל השירות.
- מיפינו, לראשונה בעירייה, את כל אותם “פתחי שירות” שבהם ניתן שירות פרונטלי.
- ערכנו שאלון תוך שימוש בכלי טכנולוגי לעריכת סקרים, וגייסנו לצורך ביצוע הבדיקה את כל עובדי הביקורת, כולל צוות התלונות והצוות המנהלי.
- המתודולוגיה, המיפוי והשאלון שגיבשנו, הועברו בסיום הבדיקה להמשך טיפול הממונה על איכות השירות - דבר שתרם לבניית יחסי אמון ושיתוף עם המבוקרים.
- תוצאות סדרת הדוחות שערכנו בנושא, בשילוב עם מיפוי

אפקטיבית.

המתבקש: "להפוך את הפירמידה" של הבקרה בתאגידים, ולבסס אותה על ממשל תאגידי ומערך בקרה פנימי בתאגיד, הכולל: מבקר פנימי שיהיה מקצועי ובלתי תלוי, ועדת ביקורת, הנחיות לסנכרון עבודתם של הדירקטוריון, ועדת ביקורת והמנכ"ל, והגדרת קשרי הגומלין בין הביקורת הפנימית של התאגיד לבין ועדת הביקורת בתאגיד וגורמי הביקורת החיצונית.

לצורך כך גיבשנו עקרונות ל"ביקורת בתאגידים עירוניים ומעין-עירוניים" הפועלים מול עיריית ירושלים, ויזמנו תהליך שיתופי לכתיבה של נוהל שישקף עקרונות אלה, תוך כדי בניית יחסי אמון והידברות עם הנהלות התאגידים והנהלת העירייה בסיוע גורמים מקצועיים.

הנוהל הושלם והופץ ביולי 2015, ומאז הוא מצוי בתהליכי הטמעה בתאגידים, באחריות הגורם העירוני האחראי

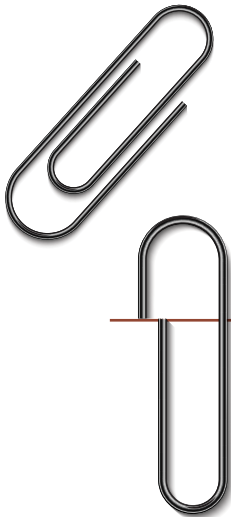
לממשק מול התאגידים. חלק מהתאגידים כבר נקטו פעולות לאישור וליישום הוראות הנוהל באורגנים הפנימיים שלהם. במסגרת "מהפכה" זו, במקביל לגיבוש הנוהל, ובמטרה לחזק ולגבש את גורמי הבקרה והביקורת בתאגידים ובעירייה, יזמנו סדרה של כנסים מקצועיים בעיריית ירושלים.

כנסים אלה נועדו להפגיש את כל בעלי העניין בתחום הביקורת בתאגידים, ובכלל זה: חברי ועדת הביקורת, דירקטורים חיצוניים ונציגי העירייה בדירקטוריונים, מנכ"ל ויו"ר התאגיד.

בכנסים נחשפו הנהלות התאגידים והגורמים האמונים על ביקורת ובקרה לעקרונות הממשל התאגידי, לניהול סיכונים בעבודת הדירקטוריון, ולניהול סיכונים ככלי ניהולי בתאגידים. בכנסים אלה התקיימו הרצאות, דיונים ומפגשי סיעור מוחות בנושאים מגוונים, והמשתתפים נחשפו לתפיסת הביקורת הנהוגה בעירייה.

סיכום

לנוכח שינויים בלתי פוסקים במציאות הכלכלית-חברתית-תקציבית-טכנולוגית שחלים על הרשות המקומית, הרי שביקורת פנימית בשלטון מקומי המבקשת להיות אפקטיבית ותורמת, צריכה לאמץ אסטרטגיה של חדשנות מתמשכת ולא להתייחס לשינוי כאירוע חד-פעמי. עם זאת, אף כלי, חדשני ומתוחכם ככל שיהיה, לא יהיה אפקטיבי אם הביקורת לא תצליח לבנות יחסי אמון עם המבוקרים. שימוש נכון בשיטות ובכלים חדשניים, יחד עם בניית קשרי עבודה נכונים ויצירת שיתופי פעולה עם המבוקרים, יובילו לאימוץ הכלים מצדם, ויאפשרו לביקורת להגדיל את השפעתה ואת הערך שהיא מביאה לעירייה.



הפקת תובנות ממקבץ דוחות ביקורת פנימית

תאריך
בעז ענר, ר"ח, CIA, MA

המאמר מתייחס לכלי חדשני יחסית בעבודת הביקורת: הפקת תובנות-מסקנות (INSHIGT). הרעיון המסדר של המאמר הוא:

האפשרות להפיק תובנות לאו דווקא מדוח ביקורת מסוים כמקובל וכנדרש, אלא ממקבץ של דוחות ביקורת

ופרסומן של תובנות אלה בדוח (ביקורת) העומד בפני עצמו - דוח תובנות ממקבץ דוחות. היתרונות של דוח כזה: הוא עשוי להציף תובנות מערכתיות, להוסיף ערך מהותי לארגון, וגם להעניק יוקרה ליחידת הביקורת הפנימית והציבורית. הליך זה מתאים לכלל העוסקים בביקורת הפנימית: מבקרים פנימיים בתאגידים עסקיים וציבוריים; משרדי ייעוץ ושירותי ביקורת; מבקרים פנימיים במגזר השלטוני על גווניו השונים; ולמבקר המדינה.

תובנות - הרעיון התורתי המסדר

אחד מההדגשים של IIA לשכת המבקרים הפנימיים העולמית הוא: הגעה לתובנות באמצעות מבט מ"מעוף הציפור" על הממצאים שעלו בדוח מסוים, תוך הסקת מסקנות מהתמונה המצטיירת מהדוח.

בשפה המחקרית-אקדמית מכנים זאת "אינדוקציה": הדרך שבה מסיקים מסקנה ממקרים פרטיים ומחלצים מהם קביעה כללית. יש המתארים הליך זה, שהוא הליך יצירתי, גם כ"חיבור הנקודות" - חיפוש מכנה משותף לממצאים שעלו בדוח. אחרים מתארים זאת כקיבוץ הממצאים של הדוח, שהם מעין "עצים ל"חורשות" ול"יער" תחת מכנה משותף אחד - כותרת וכותרות

משנה. קבוצות אלו של "חורשות ויער" במסגרת המכנה המשותף הזה, הן המאפשרות הכללה והסקת מסקנות-תובנות.

בנוסף, הפקת תובנות בעת כתיבת דוח ביקורת עשויה לתרום לקיצורו ולבהירותו של המוצר הסופי: הדוח ידגיש רק נקודות משותפות ותובנות שעלו מהבדיקה, וימנע או יצמצם את הצורך בפירוט רחב של הממצאים אך יציג את המסקנות הכלליות העולות מהם (זאת תוך הצגת דוגמאות ספורות בלבד, כאשר כל יתר המקרים הפרטניים יקובצו בנספח לדוח).

הפקת תובנות ממקבץ דוחות

כאמור, הרעיון המסדר של המאמר הוא שרצוי להפיק תובנות לא רק מדוח ביקורת מסוים אלא ממקבץ דוחות ביקורת. השם המקצועי להליכים וכלים אלה הוא גם ניהול ידע - KNOWLEDGE MANAGEMENT - ניהול הידע של הביקורת הפנימית כפי שעולה ממקבצי דוחות.

הפקת תובנות ממקבץ דוחות המחשבות והדגמות

דוגמה ראשונה לחילוף תובנות ממקבץ דוחות (וישנן בהמשך גם דוגמאות הנוגעות למבקר בתאגיד), ניתן לראות בפעולת יחידת הביקורת הפנימית ברשות לניירות ערך (להלן "הרשות"). היחידה עוסקת, בין היתר, בבדיקת פעילות תאגידים שחוק ניירות ערך חל עליהם. הבדיקות נעשות בכמה היקפים-מסגרות: בדיקת נושא מסוים בתאגיד מסוים; "בדיקת עומק" - בדיקה מערכתית רב-נושאת של תאגיד מסוים; ולענייננו, גם בחתך רחב - בדיקת נושא מסוים במדגם תאגידים תוך הפקת תובנות והפצת הידע לכלל התאגידים של הרשות. הנה כי כן, המדובר בהליך כפול של

2.

ישימות למבקרים פנימיים בתאגיד או במשרד ממשלתי מסוים

המבקרים יכולים להתייחס למכלול הדוחות בשנת עבודה מסוימת או אף למכלול הדוחות מהשנים האחרונות, ולהעלות מהם מכנים משותפים שיזכרו להנהלת הארגון כדוח מסכם - דוח תובנות. לדוגמה: תובנות בדבר איכות התרבות הארגונית; רמת הציות הארגונית - COMPLIANCE; סיכונים והמענה להם; איכות השירות לציבור; טוהר המידות וכדומה. דוח מעין זה תרומתו רבה: הוא יוצר הליך של ניהול ידע ארגוני, כלי תורתי ושיווקי, ולא פחות חשוב - כלי התורם להשבת עבודתם ותרומתם לארגון של המבקרים הפנימיים.

3.

ישימות למבקר המדינה

חשוב שמבקר המדינה יפיק תובנות מערכתיות ממקבץ הדוחות השנתי והרב-שנתי שלו וייצור כלי תורתי-ניהולי בתוך משרדו. לדוגמה, תובנות בדבר משילות, יעילות וחיסכון, מועילות, צדק חלוקתי, מרכז ופריפריה, היערכות לשעת חירום, השירות לציבור, סדרי ניהול פרויקטים, שיתוף פעולה בין-משרדי, טוהר המידות, סדרי בקרה, שקיפות, וכדומה.

כאשר יופץ ויפורסם "דוח תובנות" מעין זה, הוא יאפשר למבקר המדינה להפנות לנושאים מהותיים את תשומת הלב של ועדת הכנסת לענייני ביקורת המדינה, ממשלת ישראל, יושבי ראש ועדות הכנסת, חברי הכנסת וכלל הציבור, ויאפשר פיקוח של הרשות המחוקקת על הממשלה ועל קידום פתרונות בנידון, וגם יפנה זרקור של התקשורת, גורמי מחקר וגורמי חברה אזרחיים לבעיות המערכתיות של הממשל והמינהל הציבורי הדורשות פתרון מערכתי.

ממד הזמן והיקף ההשקעה בהפקת תובנות ממקבץ דוחות

ככל שרוצים להפיק תובנות מדוחות מהטווח הקצר, למשל משנת העבודה האחרונה, כך הפקת התובנות קלה יחסית. ככל שממד הזמן ארוך יותר ויש שאיפה להפיק תובנות גם ממגוון דוחות משנים קודמות, כך עשוי לעלות הצורך במעקב מקדים, כדי לבחון מה תוקן ומה מהווה עדיין סוגיה או סוגיות חוזרות להפקת תובנות.

אם המעקב מגלה שבוצע תיקון מהותי-שיטתי, הרי שהתובנה היא שהתרבות הארגונית היא טובה, מגיבה, בוחנת ומתקנת. אם לא בוצע תיקון כזה, הרי שהתובנה שתעלה היא הפוכה.

הפקת תובנות ממספר דוחות ובמגוון תאגידים.

המחשה בולטת לכך הוא "דוח ריכוז ממצאים מבדיקת מלאי" מנובמבר 2016 (ראו באתר הרשות). הבדיקה הרוחבית של המלאי נערכה במדגם של חמישה "תאגידים מדווחים" מענפים שונים, כלשון הרשות. המאפיין אותם תאגידים: ניהול מלאי מהותי המחייב ספירה ודיווח חשבונאי-כספי בדוחות הכספיים, כשערכי המלאי ואיכות הדיווח החשבונאי-כספי הם גורם משמעותי בהצגת התוצאות הכספיות של התאגיד, ובראשן - הרווח או ההפסד.

הבדיקה כללה בין היתר את אופן המדידה הראוי של ערכי המלאי ומידת הגילוי הנאות בספרי אותם תאגידים, לעומת הדיווח בפועל בדוחות הכספיים של אותם תאגידים.

החדשנות באותה בדיקה לא הייתה במתן הערות פרטניות לתאגיד המדגם, אלא בהפצת נייר תורתי (נייר תובנות) של הרשות לכלל התאגידים שיש להם מלאי ושחל עליהם חוק ניירות ערך, וכן למשרדי רואי החשבון של אותם תאגידים. בכך הציגה הרשות את עמדתה בשאלות עקרוניות-תורתיות אלו, ונתנה את דעתה המקצועית בשאלות של מדידה והצגת ערכי מלאי בספרים. יתרה מזאת, כך מחייבת הרשות את התאגידים לפעול על פי אותן התובנות, העמדות המקצועיות, וכל תאגיד שיחרג מהן בעתיד עשוי להיקנס בקנס מנהלי.

ראוי ללמוד וליישם את מה שעשתה הרשות לניירות ערך גם בקרב כלל העוסקים בביקורת פנימית, כמפורט להלן:

1.

ישימות למשרדי ייעוץ ושירותי ביקורת פנימית

יתרונם של משרדים אלה הוא בהכרה ובראייה מערכתית-ביקורתית של מגוון תאגידים ושל הנושאים המשותפים להם, כמו שכר, רכש, מלאי, ניהול סיכונים וכו'. לענייננו, יישום היתרון אפשרי שיהיה גם בהפקת תובנות ממקבץ דוחות. מהבדיקות הפרטניות של משרדים אלה, הכוללות מגוון דוחות ביקורת תוך ראייה רוחבית, ניתן להגיע לתובנות כוללות בנוגע להדגשי ביקורת תורתיים-מערכתיים. תובנות אלו, שיפצו המשרדים לעובדיהם כדוח או כנייר מטה, עשויות להוות כלי לימודי-תורתי חשוב לחניכה, להכוונה ולבקרת איכות של צוותי הביקורת באותו משרד, וכך גם להוסיף ערך לדוחות הביקורת שהמשרד יכין.

את הדוח או נייר המטה זה, שהוא למעשה דוח נוסף - דוח תובנות ממקבץ דוחות - המשרדים יכולים להעביר לוועדות הביקורת ולמנכ"לים של הגופים שבהם נערכת הביקורת, כלומר למקבלי ההחלטות (תוך שמירה על האנונימיות והסודיות של הגופים שנבדקו ושמהם הופקו התובנות). דוח מסכם מעין זה יפיק ערך נוסף לאותם תאגידים ויעלה את היוקרה של משרדי הייעוץ ושירותי הביקורת הפנימית.

מדור ביקורת במגזר השלטוני

תאריך
בעד ענר, ח"ח, MA, CIA

נדחתה הצעת מבקר המדינה לקבוע מתכונת לדיווח
אחר סדרי תיקון הליקויים שהעלתה הביקורת



בשנת 2016, לאחר יוזמה של מבקר המדינה ולאחר סדרה של דיונים מקדימים בוועדה, הגיש מבקר המדינה נוסח מתוקן של הצעת תקנות למעקב אחר תיקון הליקויים (המדובר בעיקר בליקויים שבאחריות משרדי הממשלה לתקנם). אך הוועדה, שבה יש רוב לקואליציה, דחתה את ההצעה. בהקשר לכך, בסוף דצמבר 2016 פרסמה ועדת הכנסת לענייני ביקורת המדינה הודעה (מעציבה) בדבר הדחייה. התהליך ודברי המשתתפים באותו דיון מפורטים להלן:

בשנת 2001 חוקקה הכנסת תיקון לחוק מבקר המדינה, הקובע חובת דיווח של הגופים המבוקרים למבקר המדינה, על תיקון ליקויים שהאחרון העלה. החוק גם קבע כי המבקר רשאי, באישור ועדת הכנסת לענייני ביקורת המדינה (להלן "הוועדה"), לקבוע מתכונת לדיווח של הגופים המבוקרים על תיקון ליקויים, לרבות פרטים שייכללו במתכונת (להלן "התקנות"). עד לשנת 2016 לא נקבעו תקנות בניהול. במהלך שנת

עו"ד תומר רוזנר



היועץ המשפטי של הוועדה, התייחס להליכים המינהליים בהקשר לגיבוש התקנות. הוא הדגיש שבמשך מספר חודשים התקיימו ישיבות והתייעצויות עם משרדי הממשלה בניהול ושהנוסח של התקנות סוכם. אך לדבריו "רק לפני שבועיים הודיעו המשרדים כי הם שוקלים מחדש את הסכמתם, ואמש בשעה חמש בערב הודיע משרד ראש הממשלה כי הוא חולק על מרבית ההמלצות".

עו"ד נירית להב-קניזו



יועצת משפטית במשרד ראש הממשלה, השיבה כי "לכל משתתפי הישיבות היה ברור לאורך כל הדרך שתקנות רבות אינן מקובלות על דעתנו".

ח"כ דוד ביטן



כבר בתחילת הדיון הודיע ח"כ דוד ביטן (הליכוד), יו"ר הקואליציה, ליו"ר הוועדה כי משרד המשפטים מתנגד לבקשת המבקר - והבהיר כי הקואליציה תפיל את התקנות.

ח"כ קארין אלהרר



(יש עתיד) הגיבה: "התנהלות הקואליציה מבישה, הממשלה מפחדת מביקורת. לא פעם ולא פעמיים מתגלה בדיוני המעקב אחרי פעולות משרדי הממשלה כי יש רפיון מהותי מצדם בתיקון הליקויים שחושף מבקר המדינה".

המבקר לתיקון ליקויים בשעת מעשה, והרחבת סמכותו לפיקוח על משרדי הממשלה לתיקון הליקויים, רק תהפוך אותו ליועץ משפטי שני, תגרום לו לפלוש לסמכויות גופים אחרים.

ח"כ יוליה מלינובסקי

(ישראל ביתנו) קראה בדיון לעריכת ביקורת על מבקר המדינה עצמו - לפני הרחבת סמכויותיו.



ח"כ בצלאל סמוטריץ'

(הבית היהודי) חלק על עצם הרעיון של יצירת תקנות. לדבריו: "ברור שאת הכשלים יש לתקן, אך לא על המבקר לאכוף תיקון זה. בתפיסה הבסיסית מבקר המדינה איננו שחקן ברשות המבצעת, הביקורת שלו היא לאחר מעשה, והוא חיצוני למהלכים... כניסת



תובנות

• כפועל יוצא, משרדי ממשלה שחשו שיש בהוראות החוק הטלת עומס רב עליהם, ובה בעת לא הייתה דחיפה מהותית של משרד מבקר המדינה שמדרבנת אותם לעשייה, נכנסו ל"אזור של נוחות" - אזור של אי דיווח ואי ציות לחוק.

מזווית ראייתי האישית, כמי שליווה את הנושא במשך שנים רבות במשרד מבקר המדינה, יש כאן אירוע מעציב - כשל רב-שנתי של הממשלה בתיקון ליקויים, אך גם כשל של משרד מבקר המדינה, כמפורט להלן:

- כאמור, כבר משנת 2001 קיים תיקון לחוק מבקר המדינה שקובע חובת דיווח בדבר תיקון ליקויים שהעלה מבקר המדינה. אולם במשך 15 השנים מאז נקבע התיקון לחוק, לא הצליח משרד מבקר המדינה לעקוב, להתריע ולבסס חובות אלו בתרבות הארגונית של הממשלה על משרדיה וגם לא יזם מתכונת לדיווח בנדרש.
- משרד מבקר המדינה עצמו גם מיעט לערוך מעקבים אחר תיקון הליקויים, ומשעשה מעקבים הוא לא שיווק אותם כראוי ולא נאבק ציבורית על העיקרון של חובת תיקון הליקויים.
- תיקון נוסף לחוק משנת 2011, שבא לחזק את חובת תיקון הליקויים, יצר איום מהותי: החוק קבע כי אם לא קיים עובד גוף מבוקר את הוראות החוק בלא הצדק סביר, יהווה הדבר עבירת משמעת. אך מאז 2011 לא התפרסמו מקרים שבהם נבחנה או מומשה הסנקציה.



סיכום

הליך פגע במוסד מבקר המדינה וביוקרתו. אך הכדור עדיין בידי המבקר: במסגרת הוראות החוק וסמכויות מבקר המדינה, אף ללא התקנות דלעיל (שברובן הן טכניות), משרדו יכול היה ויכול מכאן ואילך לעשות רבות להטמעת תרבות של תיקון ליקויים. אסטרטגיה ומדיניות ברורה של משרד מבקר המדינה בדבר מעקב של משרדו אחר תיקון ליקויים, תוך דגש ומעקב רק על מקבץ הליקויים המערכתיים והמהותיים ביותר, יחד עם שיווק ראוי של תוצאות דוחות המעקב שהוא יערוך בנדרש, עשויה להיות הדרך.

אירועי "קו פרשת המים" המחייבים חשיבה מחודשת על תפיסות מסורתיות בביקורת הפנימית

חזק
שמואל רוזנבלום, ר"ח מוסמך במשפטים, LL.M, CFE, CIA

מתי מתבצעת בדיקת פליטה על ידי גופי התקינה. החיישנים שידרו למחשב המנוע לדמות פליטת גז תקינה בעת ביצוע הבדיקה, כך שבאופן זמני תאמה פעילות המנוע לעמוד בתקינה. כאשר מסתיימת בדיקת התקינה - שב המנוע לפלוט רמת גזים "רגילה" שהיא מעל התקן המותר. כך הצליחה פולקסווגן לשווק את רכבי הדיזל שלה בעולם, לאחר ש"הצליחה" באמצעות התקנים זדוניים לעמוד בסטנדרטים של רשויות התקינה. מחוכם.

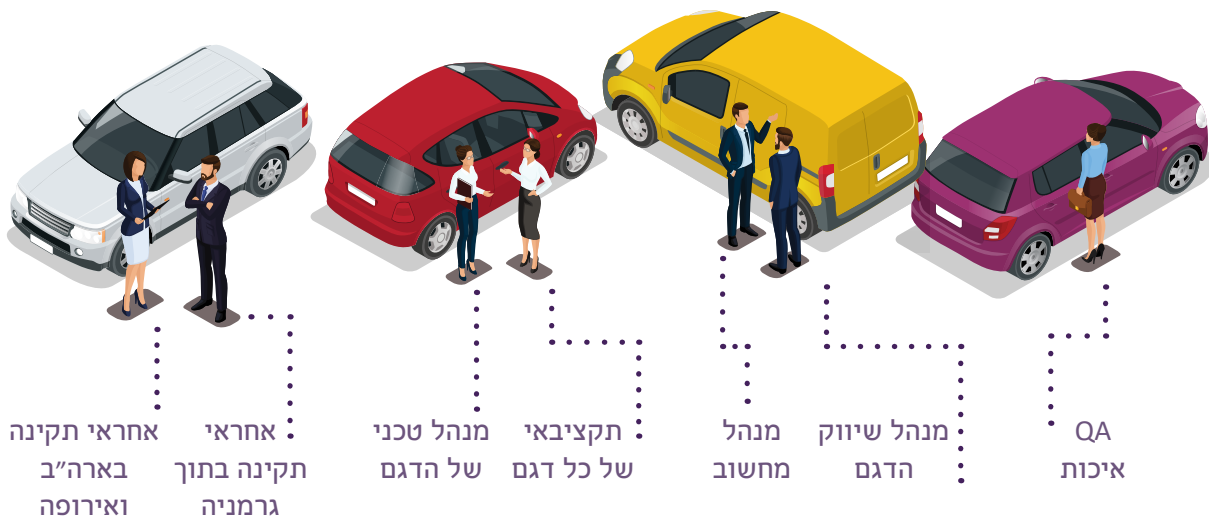
אני נזכר בערגה בהרצאה הראשונה באוניברסיטה, בקורס "ביקורת חשבונות". המרצה, בעל שם ומוניטין, קבע בפסקנות כי הפרדת תפקידים בארגון (Segregation of duties) היא הערובה החזקה והמרכזית למניעת אי סדרים כספיים. העיקרון נשמע הגיוני ומשכנע!! מאז - כעשרות שנים, אנו כמבקרים מתבססים, מתבסמים ומתמכרים לכלל ה"נ"ל. בעקבותיו אנו יוצאים חוצץ נגד One man show, תחת המנטרה המסורתית שכלל שיהיו מעורבים בתהליך אנשים רבים יותר בארגון - כך נצמצם למינימום ביצוע מעילות ואי סדרים כספיים. ברצוני להתריע: קיום הפרדת תפקידים ומעורבות גורמים רבים בהליכים - אינם תמיד ערובה אוטומטית למניעת אי סדרים.

ראוי לנתח כיצד התאפשרה ההונאה בתוככי פולקסווגן - תאגיד המעסיק עובדים רבים ובכירים, שאמורים היו לדעת על הרמייה והיו שותפים בה באופן פעיל! מדובר במהנדסים, מהנדסי תוכנה, אנשי רכש, עיצוב, בקרת איכות, מנהלי תקציב ועוד - שהיו חייבים להיות בסוד ההונאה!

ומחים בתעשיית הרכב מעריכים כי עלות הנזק מ"סקנדל הדיזל" ("DIESELGATE SCANDAL") של פולקסווגן תגיע ל-50 מיליארד אירו. התחשיב מבוסס על הערכות של הקנסות החמורים מרשויות חוק בעולם (בראשן ארה"ב), תביעות ממשלתיות להחזרי סובסידיות למכוניות "ירוקות", תביעות מצרכנים פרטיים ומארגוני הירוקים, עלויות RECALLS למיליוני כלי רכב בעולם, וכן נזקים הנוגעים להצטמקות שוק הדיזל של החברה. גם אם נניח שההערכות מוגזמות, הרי שגם מחצית מהסכום המוערך יש בו כדי לזעזע את ענקית הרכב הגרמנית (ואגב: נמסר כי ממשלת ישראל תובעת 300 מיליון ש"ח בגין הפרשי מכס).

השאלה המהדהדת בקרב מומחי ביקורת, מומחי ניהול ומשפטנים היא: כיצד תיתכן בתאגיד מאורגן, פעילות זדונית רחבת היקף במשך שנים כה רבות, בלי שתיחשף בתוך זמן קצר? שאלת משנה: כיצד ניתן להילחם מראש בתופעה כזאת? ושאלת השאלות: האם עוול מאורגן בהיקף כזה עלול להתרחש בתעשיות אחרות, והאם תעשיות דומות נערכות לטיפול מונע? בקצרה: כלי רכב מחויבים בעמידה תחת תקני פליטה מחמירים. אי עמידה בתקני הפליטה במדינות השונות שוללת אפשרות לשיווק כלי הרכב. עמידה בתקנים זיכתה את היצרן במכסים מופחתים ובמענקים "ירוקים".

פולקסווגן הודתה כי מהנדסיה המוכשרים התקינו תוכנה זדונית ברכביה במטרה להטעות את בוחני פליטת הגזים ולזייף את התוצאות המתקבלות. מדובר בחיישנים שזיהו



בגרוש". הייתי מגדיר בתכניות העבודה שלנו הליך של "סקר סיכונים פסיכולוגי-התנהגותי". עד היום אנו מבצעים סקרי סיכונים - תפעוליים או פיננסיים. אין די בכך! כנס של ה-IIA (הלשכה האירופית ECIIA) שהתקיים בשווייץ באוקטובר 2016, הובעה הדעה כי "ביקורת פנימית אמורה להתאים עצמה לתרבות המקומית" (הדיונים נסבו סביב פרשת השחיתות ב-FIFA) ושיש להתחשב ב"תרבות הארגון". הנה כי כן, הדעה המתגבשת בקרב אנשי מקצוע כי ההיבט הפסיכולוגי-התנהגותי חייב לתפוס מקום חשוב בתכנון יעדי הביקורת.

מסקנת לוואי: לא להיצמד לתיאוריות בלתי מעשיות הנושבות מארה"ב. מאז הופעת ה-SOX חדרו לביקורת כללים מכניים מדי של אמצעי ביקורת ללא "נשמה". כך למשל, מינוי

WHISTLE BLOWER ("השורק במשרוקית") שיתריע על אי סדרים. כך למשל ה"טלפון האדום", שהאמריקאים כל כך גאים בו. הניסיון שלי בביקורות בחו"ל ובארץ מלמד שהטלפון האדום אינו יעיל.

חברים מבקרים פנימיים! אל נא תפריזו במשקל המיוחס לאמצעים טכניים אלה. הטלפון האדום בפולקסווגן - העלה אבק! אך לא רק בגרמניה הושבתו מנגנוני ההתרעה. הטלפון לא צלצל בחברת חשמל (מרכז הטורבינות) וכמובן שלא ב"סימנס", יצרנית הטורבינות בגרמניה.

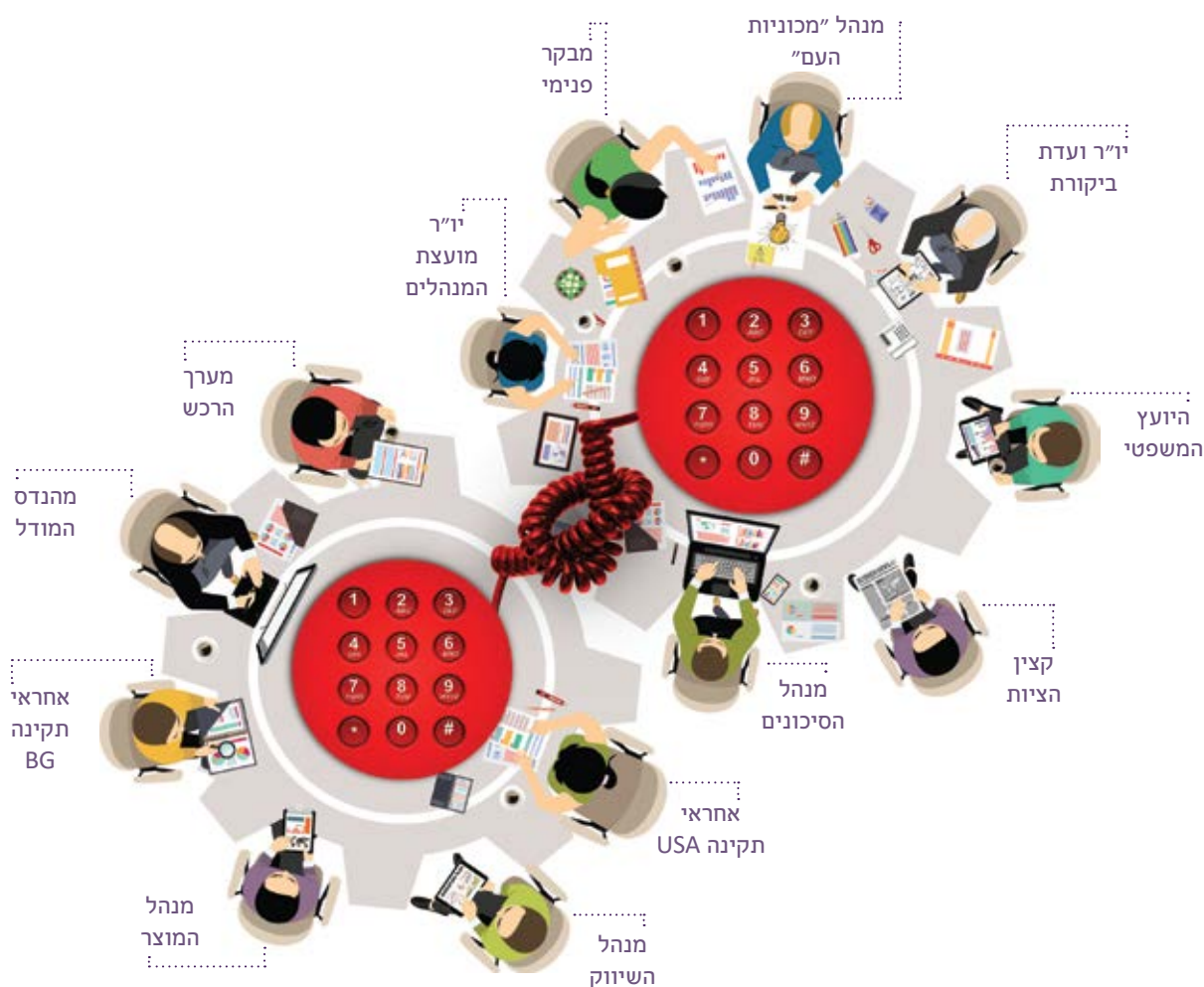
מומחי רכב משערים שמדובר בלפחות 100 עובדים בדרכות שונות. איך ייתכן ש"אף אחד לא קם"? אף לא אחד הפעיל את ה-"HOT LINE" להתריע על מחדלים פנימיים! איפה היה מצפון העובדים, איך לא צלצלו הפעמונים?

אם כך, מדוע בפולקסווגן קרסה הנחת הבסיס המסורתית? הנה, המוני מועסקים משולבים במבצעי הונאה מתוחכמים ומתמשך ללא כל הדלפה! בניגוד למוסכמות שעליהן התחכנו.

התשובה נמצאת בתחום הפסיכולוגי-חברתי. נראה כי התרבות הארגונית שמאפיינת את התאגיד היא כי "פולקסווגן מעל לכל" (VOLKSWAGEN UBER ALLES). שיטת "הקו החם" והפרדת התפקידים אינה רלוונטית כאשר עובדים סבורים שהחברה שלהם היא התגלמות של אידיאל! כאשר קיימת קנאות לסמל החברה ולסמלים בכלל, ה"מלשינון" הפנימי אינו אופציה למעורבים.

המסקנה ברורה: במקום שהאווירה הכללית היא "העיקר הארגון", בשילוב ההתנהגות צייתנית ופטריוטית ללא פשרות, שומה על גופי הביקורת והדירקטוריון להפעיל ולמסד הסברה פנימית תקיפה כדי למגר את ה"פטריוטיות". עליהם לשכנע שהסיכון באי ציות לחוקים הוא מסוכן מדי, ושהתוצאה הסופית של "פולקסווגן מעל לכל" עלולה להביא לקטסטרופה.

מסקנה למבקרים פנימיים: לא להישען על אקסיומות של הפרדת תפקידים (SEGREGATION OF DUTIES). לפי דעתי, בעניין הזה הביקורת הפנימית חייבת להפעיל "פסיכולוגיה



תופעה נוספת מחייבת חשיבה

יש לשים לב כי פולקסווגן ביצעה הונאות בעיקר מחוץ לגרמניה. הנה לפנינו סימפטום נוסף, שובר מוסמכות וחוצה גבולות, שנחשף ב"פרשת הסדר בנק לאומי עם רשויות המס האמריקאיות".

אי עמידה ברגולציה בארה"ב עלתה לבנק לאומי הישראלי סכום עתק של כ-1.5 מיליארד שקלים. מדובר בבנק שהוא הסמן הימני והדוגמה להקפדה רגולטורית. בזמן כתיבת שורות אלה מתבצעת ביקורת מטעם הרשויות בארה"ב גם על בנק הפועלים וייתכן שבמוסדות פיננסיים נוספים. הלקח העיקרי לדיסקוריונים ולביקורת בישראל הוא כי יש לתת עדיפות לטיפול ברגולציה הבינלאומית. כיום,

בחלק מהארגונים בישראל, רוב שימת הלב עדיין מופנית להקפדה על רגולציה בישראל. לא עוד!

אני סבור שיש לתת עדיפות לתקינות הבינ"ל. עמידה ברגולציה בחו"ל תהיה לעתים בעלת עדיפות ראשונית. נראה כי אם הייתה מתרחשת סטייה זהה מרגולציה בארץ המוצא (במקרה זה ישראל), היו הקנסות נמוכים בהרבה. בסיטואציה של העמדה לדין בישראל (ובאופן לא פורמלי), היה בית המשפט בישראל מתחשב בכך שבנק לאומי מעסיק אלפי עובדים בישראל. בית המשפט הישראלי היה מתחשב ב"ציבות הבנקאות בישראל". היקף הקנסות בישראל על חברה ישראלית מושפע באופן טבעי משיקולים מקומיים, כך שהקנס הסופי היה נמוך מזה שהיה מוטל על אותה החברה בחו"ל.

ומדינות זרות שבהן מבוצעת רמייה וסטייה רגולטורית על ידי תאגיד זר, יחמירו איתו ככל שניתן.

כל התאגידים הבנקאיים בישראל, כל היצואנים, יצרני התרופות (ממש בעת כתיבת שורות אלה התפרסמה הטלת קנס רגולטורי בגין פעילות קידום מכירות של טבע), יצואני חומרה, דשנים, מזון וכו', יהיו חייבים להסיט את המאמצים לעמידה ברגולציה בינלאומית. השיח הרגולטורי, הן בביקורת הפנימית ובוודאי בהנהלות ובדירקטוריונים, יהיה שיח בעל מבטא זר/בינלאומי.

ההתייחסות במדינה זרה היא הפוכה. לרשויות בארה"ב לא יהיו סנטימנטים לכלכלת ישראל וליציבות של בנק ישראל! מבחינת השופטים בארה"ב מדובר בתאגיד זר(!) שבחר לא לציית לרגולציה ולפגוע בכך בכלכלת ארה"ב. והתוצאה - קנס של 1.5 מיליארד שקלים.

והלקח ברור: על הדירקטוריונים והמופקדים על הביקורת בתאגידים בעלי פעילות בחו"ל או פעילות משיקה בחו"ל, להפנות משאבים רציניים יותר לעמידת התאגיד בחוקי המדינות הזרות שבהן הם פעילים. וכך גם לגבי פולקסווגן, נראה כי הקנסות עליה יהיו גבוהים, מפני שרשויות

סיכום

ב

מסגרת הפקת לקחים מהירה ניתן לקבוע מסקנות ראשוניות:

הגישה האמריקאית של HOT LINE ושל Whistleblower תיושם במידה, אך יש לתת לטכניקה זאת משקל מופחת.

הביקורת הפנימית חייבת להשתחרר מגישות טכניות - יש להפעיל "ביקורת עם נשמה".

הטיפול של הביקורת הפנימית ברגולציה בינלאומית יקבל עדיפות עליונה.

שומה על הביקורת הפנימית לבצע "סקר סיכונים התנהגותיים", זאת בנוסף על סקרי הסיכונים השגרתיים.

רוח הארגון, דפוסי ההתנהגות והפסיכולוגיה ההתנהגותית - יובאו בחשבון וישפיעו מהותית על תכניות הביקורת.

בארגון שבו האווירה הכללית היא "הארגון מעל לכל" - היכן שהתרבות היא חינוך לצייתנות ופטריזטיות ללא פשרות

שומה על גופי הביקורת והדירקטוריון להפעיל ולמסד הסברה פנימית תקיפה, כדי לשכנע את "הפטריזטים הנלהבים" שהסיכון גבוה מדי! התוצאה הסופית ל"פולקסווגן מעל לכל" ("Volkswagen uber alles") עלולה להרוס אותה.

הביקורת הפנימית תהיה מודעת לאפשרות של קיום "עבירות מרובות משתתפים" בתוך הגוף המבוקר. כלומר: ייתכנו מצבים שבהם מספר רב של מעורבים יבצעו יחד סטייה מהוראות - ללא הדלפה שתסייע לחשיפה.

יצירת הפרדת תפקידים SEGREGATION OF DUTIES - אין בה די.

הפוליגרף ככלי מסייע בעבודת המבקר הפנימי הלכה למעשה

חונן ארצי, MA
תא

במאמר זה נפתח צוהר ונכיר את אחד מכלי הסיוע
הטובים והאמינים בביצוע חקירה באשר היא -
ביטחונית, פלילית, מהימנות עובדים, חשש לעבירה
על טוהר המידות ועוד - הפוליגרף



מכשיר זה, המכונה בשפת העם "מכונת אמת", הומצא בשנות העשרים של המאה ה-20 בארה"ב, ופעילותו מתבססת על ההנחה שלפיה כאשר אדם משקר, בגופו מתרחשות תגובות פיזיולוגיות בלתי רצוניות ובלתי נשלטות. כמי שנחשף לא אחת לבדיקות פולִיגרף ולתוצריה אקדים ואומר - קל מאוד, ובמיוחד אם מאמינים בכלי זה ליפול בפיתוי, להשתמש בו ולהאמין שמדובר בכלי שתוצאותיו הן חד-משמעיות ואמינות ביותר.

ולא כן היא - לא תמיד ניתן להשתמש בפולִיגרף (גם מקצועית), וישנן טעויות לא מעטות.

מחקרים וועדות בדיקה בנושא הפולִיגרף קבעו שתקפות בדיקת הפולִיגרף נעה בין 80% ל-90%. שונות זו נובעת, בין היתר, משיטות שונות של בדיקות.

עלינו המבקרים להכיר את הפולִיגרף, את יכולותיו ומגבלותיו ואת הסוגיות המשפטיות הקשורות בו, שכן לא אחת עולה לדיון בארגונים השאלה: האם צריך, נכון ורצוי להשתמש בפולִיגרף בעטיו של חשד לפלילים או חשד לפגיעה בטוהר המידות? נרחיב על כך בגוף המאמר.

הפולִיגרף - סקירה כללית

למונח שקר יש הגדרות רבות. כך למשל, מוגדר שקר - כמעשה, אמירה או עמדה שאינם מתאימים למציאות המובאת לידיעת הזולת, ושתכליתם להשיג או לספק יתרון בדרך של רכישת אמון או הטעיה.

ודוק - שקר הוא כוונה לרמות כדי להשיג יתרון/תועלת, או להימנע מאי נעימות או סנקציות הכרוכות באמירת אמת.

העובדה שמתח נפשי הקשור באמירת שקר, בהתרגשות, בפחד ובמבוכה גורמים לשינויים פיזיולוגיים באדם - ידועה מזה שנים.

בעבר הרחוק היו מקומות שבהם נהגו למלא את פיהם של החשודים בשקר באורז גולמי, ומי שהתקשה ביריקתו - נמצא אשם; וזאת מתוך הנחה ששקר גורם לאדם ליבוש בפה. זה היה מכשיר הפולִיגרף של אותם ימים.

כאמור, בשנות העשרים של המאה ה-20 הומצא מכשיר הפולִיגרף בארה"ב. למכשיר לפחות שלושה ערוצי בדיקה הבודקים את השינויים הפיזיולוגיים של הנבדק - שינויים בלחץ דם, דופק, הזעה ונשימה.

הבדיקה אינה כוללת רק את "חיבורו" של הנבדק למכשיר, אלא הצגת שאלות וקבלת תשובות עליהן. מתקיימת אינטראקציה הדוקה בין החוקר/בודק לבין הנבדק - החל מהכנת הנבדק לבדיקה, ניסוח השאלות; חקירה תגובתית עקב ממצאי הבדיקה ועוד.

בהכללה ניתן לומר שקיימות שתי שיטות בדיקה עיקריות:

1. שיטת שאלות הביקורת | בשיטה זו נעשה שימוש בדרך כלל בבדיקת מהימנות כללית לצורכי מיון עובדים. במסגרת בדיקה זו מוצגים לנבדק שאלות שעליהן עליו לענות ב"כן" או "לא". אין לבדוק מידע מסוים ולוונטי על הנבדק (למשל, שגב ממעסיק קודם). בשיטה זו נערכת השוואה בין תגובותיו הפיזיולוגיות על הנבדק לשאלות העומדות בבסיס הבדיקה (לדוגמה, האם גנב ממעסיק קודם) לבין תגובותיו לשאלות ביקורת (לדוגמה, האם גנבת אי פעם, האם שיקרת למעביד אי פעם).

2. שיטת פרטי חקירה מוכמנים (פח"מ) | הנבדק נשאל לגבי פרטים מסוימים שלכאורה רק הוא מודע להם (לדוגמה, רק הנבדק יודע באיזה חשבון בנק נמצא הכסף שנגנב). מקובל ששיטה זו היא מהימנה יותר, אך גם לגביה אין הסכמה שניתן להסתמך עליה באופן גורף.

חקירה באמצעות מכשיר הפולִיגרף - היבטים נפשיים

מסמך הנחיות היועץ המשפטי לממשלה מתמצת היטב את המשמעות הנפשית העלולה לנבוע כתוצאה מחקירה באמצעות מכשיר הפולִיגרף, וזו לשונו:

"חקירה באמצעות מכשיר הפולִיגרף היא הליך חודרני מאוד, ועלולה להיות חוויה רגשית בלתי נעימה ואף משפילה. מדובר בבדיקה שנועדה להעמיק אל הלא מודע ובכך לפגוע בחופש הרצון, תוך חדירה לנבכי נפשו של אדם וגביית תגובות בלתי מודעות.

לצד הפגיעה הטבועה בזכויות הקיימת בעצם השימוש במכשיר הפולִיגרף, נאלץ הנבדק בשיטת שאלות הביקורת, על מנת "לעבור בשלום" את הבדיקה, לחשוף בפני הבודק כל פרט מציק בעברו, לרבות נושאים אינטימיים או מעשים בלתי ראויים חסרי חשיבות ופעוטי ערך שנעשו לפניו שנים רבות.

בית המשפט אימץ את התפיסה כי חובת תום הלב מטילה על המעסיק את החובה לוודא שהמבחנים שאליהם הוא שולח את העובדים הפוטנציאליים הם בעלי מהימנות ותוקף גבוהים לצורך קבלת ההחלטה.

חיוב עובד לעמוד בבדיקת פולליגרף

לא ניתן לחייב עובד לבצע בדיקות פולליגרף, גם אם הוא נתן את הסכמתו לכך במסגרת חוזה עבודה. יש לקבל הסכמה ספציפית.

פיטורים בהסתמך על בדיקת פולליגרף

סירוב להיבדק או תוצאות שליליות בבדיקת הפולליגרף לא יהיו עילה בלעדית לפיטורין ללא פיצויי פיטורים.

עם זאת, ניתן לראות בסירוב פגיעה ברמת האמון הנדרשת מעובד, וככל שהוא בכיר יותר - הפגיעה תהא חמורה יותר. עובד לא יכול להסכים (באופן ספציפי) להיבדק, ועם קבלת התוצאות לחזור בו מהסכמתו.

המבקר הפנימי והפולליגרף

במסגרת הביקורת הפנימית, אפשר וייעשה שימוש בפולליגרף במקרים מסוימים, לדוגמה:

- במסגרת הערכת הבקרה הפנימית בארגון, המבקר הפנימי עשוי להמליץ לשלב כאחד ממנגנוני הבקרה הפנימית גם בדיקת פולליגרף (לדוגמה, כחלק מהליך גיוס עובדים לתפקידים רגישים).
 - במסגרת חקירות אירועים (כגון הונאות ומעילות) שעורכת הביקורת הפנימית, כאשר האמנה של הביקורת הפנימית בארגון (internal audit charter) קובעת שחקירות בארגון הן בתחום אחריותה. גם אם המבקר הפנימי אינו מבצע חקירות בעצמו, אזי לעתים כשמתרחש אירוע הוא משולב בצוותי חקירה או מלווה את הצוות. הפולליגרף עשוי להיות כלי רב עוצמה בחקירות אלו.
- המבקר הפנימי אמור להכיר את מכשיר הפולליגרף, לדעת את יתרונותיו וחסרונותיו, וכן לדעת מה לשאול ולבקש ממבצע בדיקת הפולליגרף.
- במקרים שבהם החליט המבקר הפנימי לעשות שימוש בבדיקת פולליגרף; או ממליץ על שימוש זה, עליו לוודא כי ההליך יבוצע באופן נאות ובדגש על הנקודות הבאות:
- יש לוודא שהעובד מודע למהות הבדיקה, למגבלותיה,

בעת בחינת קבלת עובד לעבודה, מותר לעשות שימוש ב"מבחני התאמה"

כך למשל, בתשובה לשאלת ביקורת שגרתית אודות פגיעה באמון בעבר, מחויב הנבדק לחשוף בגידות בחיי הנישואין, שקרים למעביד ועוד. בכל אלה יש כדי להטיל אימה על הנבדק. יתר על כן, מכשיר הפולליגרף מתעד את תגובות הנבדק לשאלות ביקורת אף במקרה בו הנבדק מסרב לענות לשאלה מסוימת.

אל מול בעיית המהימנות והפגיעה בזכויות יסוד, יש להציב תועלות אפשריות שבשימוש במכשיר הפולליגרף. כך למשל, אין חולק כי לשימוש במכשיר הפולליגרף יתרונות הרתעתיים מסוימים. בנוסף, רווחת הדעה בקרב גופי החקירה בישראל כי הבדיקה יכולה לשמש, בנסיבות מסוימות, כלי עזר בחקירה. השימוש במכשיר הפולליגרף עשוי גם לסייע לחשוד בהפרכת האשמות שווא, ובמקרים מסוימים הוא מסייע לחפים מפשע להזים עוד בשלב החקירה ראיות נסיבתיות הקושרות אותם אל העבירה.

היבטים משפטיים בנושא הפולליגרף

הגישה המשפטית לבדיקות פולליגרף שונה בהתאם לסוגי ההליכים:

הליך פלילי

בהליך פלילי בבדיקת הפולליגרף אינה קבילה כראיה, אף לא בהסכמת הנאשם עצמו, למעט חריג אחד - ניתן לבצע בדיקת פולליגרף ולעשות שימוש בתוצאותיה לשם מעצר לצורכי חקירה.

הליך אזרחי

בהליך אזרחי, בית המשפט רשאי לקבל כראיה את תוצאות הפולליגרף, ובתנאי ששני הצדדים הסכימו מראש לביצוע הבדיקה ושתוצאותיה יוגשו כראיה בהליך המשפטי הספציפי הזה. בנוסף, על ההסכמה של הנבדק להיות מפורשת ומרצון (לא די בהסכמה שבשתיקה). אין לכפות את הסכמתו של נבדק (עובד, לדוגמה) באמצעות איומים.

פולליגרף כתנאי לקבלה לעבודה

באופן עקרוני, בעת בחינת קבלת עובד לעבודה, מותר לעשות שימוש ב"מבחני התאמה" (פולליגרף, גרפולוג, מבחנים פסיכולוגיים וכדומה).

- להשלכותיה, וליכולת לעשות בה שימוש כראיה בבית המשפט.
- יש להחתים את העובד על הסכמתו הספציפית לביצוע הבדיקה, ולהבהיר לו את מהותה. הדבר תקף גם כשהעובד מציע ביוזמתו לבצע את הבדיקה.
- לא ניתן לחייב את העובד לבצע בדיקה.
- אין להפעיל על העובד לחץ או לאיים עליו. אין לגרום לעובד לחתום על הסכמה בדרך של פיתוי.
- יש לבצע את הבדיקה באופן חף מהטיות ככל הניתן, תוך התחשבות במגבלות הנבדק (כגון מגבלות רפואיות, מגבלות שפה, נטילת תרופות).
- יש להקפיד ולבצע את הבדיקה רק באמצעות בודק מוסמך.
- יש לזכור שהבדיקה היא רגישה, ושעצם שיגור עובד לבדיקה עלול להתפרש במקרים מסוימים על ידי הסובבים כהבעת אי אמון בעובד או אף גרוע יותר - כהטלת אשמה (בבחינת "אין עשן בלי אש"). לכן יש להימנע ככל הניתן מעצם חשיפת הבדיקה עד תומה.



מדור היתולי

מיומנה של מבקרת פנימית

למאת: חונית שוורץ, MA - בנק הפועלים

צורך מילוי תפקידו נדרש המבקר הפנימי לידע רב. עליו להכיר את הארגון שבו הוא עובד, את הרגולציה הרלוונטית, את התרבות הארגונית ותרבות הסיכון, את האסטרטגיה, את המדיניות, את תפיסת הבקרה, את תהליכי העבודה ועוד.

בנוסף עליו להתמחות במקצוע הביקורת הפנימית, להכיר את התקנים המקצועיים, חקיקה רלוונטית, שיטות דגימה וניתוח, יכולת הסקת מסקנות, כישורי כתיבה, וזה רק על קצה המזלג.

אבל כל אלה לא יספיקו אם תחסרנה למבקר מספר מיומנויות בסיסיות, ובהן ידע מינימלי בפסיכולוגיה, קריאת שפת גוף, יכולת הקשבה, ויכולת לאבחן למה

באמת התכוון המבוקר בדבריו.

למשל, אמירה מצד מבוקר בסגנון "הביקורת הקודמת שנערכה ביחידתי הייתה מצוינת! בזכותכם למדתי כיצד יש לכתוב נהלים בצורה אפקטיבית", משמעותה בעצם "בגללכם בזבזתי ים של זמן בכתיבת נהלים שאין בהם צורך".

דוגמה נוספת, כשהמבוקר אומר "מצאתם כל כך הרבה ממצאים בביקורת אחת - כל הכבוד", הוא רצה בעצם לומר "מרוב עצים לא רואים את היער! תתחילו להתעסק במהות ולא בכמות".

במהלך 9 שנות עבודתי כמבקרת פנימית, פגשתי כבר מבוקר או שניים. בטור הנוכחי אנסה לאפיינם

המבוקר האמיתי

כל הזמן מנסה לברר מה בדיוק בודקים ומה כבר נמצא. אם המבוקר לא מגיע במשך כמה ימים הוא מתקשר לברר מה קורה (זה לא באמת, סתם הגזמתי...)

המבוקר האמיתי

בביקורת הקודמת לא עזרתם ולא תרמתם כלום! רק הפרעתם לי לעבוד

המבוקר האמיתי

מנסה להכתיב את ממצאי הדוח, ובמיוחד את ההמלצות (שהן כמובן תוספת תקציב וכוח אדם).

המבוקר האמיתי

"אין בעיה אחי", "תרגיש חופשי לכתוב מה שנראה לך"

המבוקר האמיתי

מגיב לכל פסקה בדוח הביקורת, כולל למבוא ולרקע.

המבוקר האמיתי

לא מוצא זמן להיפגש, אין להפריע לו, מאחר אפילו לפגישות טלפוניות.

המבוקר האמיתי

אני שמח מאוד שאתם לביקורת ביחידתי. מניסיוני הביקורת עוזרת ותורמת המון

המבוקר האמיתי

מבקש לשנות ניסוחים לכל אורך טיוטת הדוח.

המבוקר האמיתי

"עכשיו לא זמן לכתוב"

תמיד הביקורת מתחילה מבחינתו בזמן לא מתאים: בדיוק לפני שינוי ארגוני/ אחרי שינוי ארגוני, בדיוק לפני חתימת עסקה גדולה, כל העובדים בדיוק במילואים וכל העובדות בדיוק בחופשת לידה...

המבוקר לא יבקר
תגובותיו להמלצות הן "מקבל" או "לא מקבל"

המבוקר האדיש
ממשיך בעבודתו כרגיל, לא באמת נראה שאכפת לו, לא טורח להגיב לטייטות.

המבוקר האמיתי
כל הזמן מנסה לברר מה בדיוק בודקים ומה כבר נמצא. אם המבקר לא מגיע במשך כמה ימים הוא מתקשר לברר מה קורה (זה לא באמת, סתם הגזמתי...)

המבוקר האלטרנטיבי
מתאמץ לתקן את כל הליקויים במהלך הביקורת.

המבוקר האלטרנטיבי
שולח מיוזמתו אסמכתאות, עונה תגובות ארוכות ומפורטות (שלא לומר מייגעויות), שולח תגובות מתוקנות גם לאחר פרסום הדוח הסופי, שמח על הקדמת הדיון בדוח בוועדת הביקורת.

המבוקר הראשון
"יהיה בסדר", "הכול יטופל..." (הכלאה של המבוקר האדיש והסחבק).

המבוקר הסקארוזי
לא זוכר כלום, לא יודע, לא מוצא את האסמכתאות.

המבוקר אפסר האופר
עונה על כל מה שלא נשאל, מעביר למבקר נהלים, ניירות ותיעוד לנושאים שכלל לא נבדקו.

היורש כל
לא חידשנו לו כלום, הוא כבר חשב על כל ההמלצות לבד...

המבוקר האמיתי
יותר צדיק מהאפיפיור. מתקן את מלוא הליקויים, מתקשר אותם לאחרון העובדים, באותה הזדמנות סוקר את כל נוהלי היחידה ומרענן אותם, ושולח אסמכתאות על הביצוע לביקורת (בן דודו של המבוקר המשתדל).

כיצד הכישרונות
מזהה את היכולות והכישרונות של המבקר (ברורו) ומציע לו לעבור לעבוד אצלו.

מורה למחוק סעיפים, היכן לשלב את התגובות, מנסח תיקונים להמלצות ומנחה מה חשוב לכתוב בתמצית המנהלים.

המבוקר שהיה פעם מבקר בעצמו
בטוח שמכיר את כל שיטות העבודה, מנסה לנחש מהם הכיוונים של הביקורת ומופתע לגלות את עומק השינוי בעולם הביקורת מאז שהוא היה מבקר.

המבוקר עם הפצצה הפתוחה
לא מתאושש מהביקורת שהתנהלה אצלו לפני 12 שנים, ושהייתה כמובן לא אפקטיבית ולא צודקת.

המבוקר הפוליטיקאי
אם דוח הביקורת אינו חמור, פועל לתקשרו בארגון. שולח מכתב תודה לביקורת עם העתק למנכ"ל.

thank you

המבוקר האופטימלי ענייני, משתף פעולה, מדבר בנימוס אל המבקרים, מצביע בעצמו על כשלים ופערים בבקורת, מגיב לטייטה עוד לפני מועד התגובה הסופי, פועל לתיקון הליקויים בזמן סביר וברצינות. מכירים כזה?

שאלת השאלה - כיצד על המבקר להתמודד מול כל אלה? אפשרות ראשונה: "חנוך לנער על פי דרכו", כלומר מול המבוקר המתלהב - תתלהב; למבוקר המשתדל - תן צל"ש; לנותן ההוראות - העמד פנים קשובות ועשה מה שנראה לך. אפשרות שנייה - הפגש את כל המבוקרים יחד. הרגוע

ירגיע את הלחץ, האדיש יצנן את המתלהב, הסחבק יסתחבק עם הפוליטיקאי, ובא לציון גואל. אפשרות שלישית: היעזר בתכונות המבקר שטבועות בך: אינטליגנציה רגשית גבוהה, קור רוח, תחכום ואמפתיה. כל זה, והעובדה שבסופו של דבר אתה זה שמחזיק את העט (או המקלדת)...



פורום "שולחן עגול" למבקרים פנימיים ראשיים

**כמה פעמים הייתה לך הזדמנות להיות חבר בפורום שיכול להשפיע
על פעילות הביקורת הפנימית ועל עתיד הביקורת בכלל?**

פורום "שולחן עגול" מבקרים פנימיים ראשיים הוא פורום המאגד והמייצג את מבקרי הפנים הראשיים של החברות והארגונים המובילים במשק.

ייחודו של הפורום בהיותו מאגד את כלל המשק הישראלי - חברות ציבוריות, פרטיות, וממשלתיות, מוסדות פיננסים, בנקים, חברות ביטוח, משרדי ממשלה, רשויות מקומיות, ועמותות. כתוצאה מכל אלו, מייצג הפורום, יותר מכל גוף אחר, את הצרכים של כלל המבקרים ללא הטיה סקטוריאלית או אינטרסנטית זו או אחרת.

הפורום ממוקד בהבאת ערך לחבריו, בייצוג עמדותיהם ובטיפול הידע המקצועי הנדרש בתפקידם בארגונים. הפורום יוזם מפגשים, השתלמויות ודיונים מעמיקים העוסקים בנושאים הרבים והמגוונים הנמצאים על שולחנו של המבקר הפנימי הראשי. עוצמתו היא עוצמתם של החברים בו.

את הפורום מוביל גיל כר, מבקר הפנים הראשי של אל על נתיבי אויר לישראל ודירקטור ב- IIA ישראל.

המפגשים האחרונים התקיימו במתחם ההדרכה של חברת שיכון ובינוי.
בהזדמנות זו ברצוני להודות לשיכון ובינוי על האירוח החם ושיתוף הפעולה.

מטרות הפורום

קידום הביקורת הפנימית | לתרום לשיפור האיכות והמצוינות בתחום הביקורת הפנימית בישראל.

ידע | ליצור מקום מפגש לשיתוף ידע, הכרות, התייעצות, לטיפול הידע ויצירת פתרונות משותפים.

חדשנות | לקדם חשדנות ויצירתיות בעולם הביקורת הפנימית.

Networking | לשמש במה לכל המבקרים הפנימיים הראשים לחשיפה אישית וארגונית.

בית | להוות בית למבקרים הראשיים.

על מנת לממש מטרות אלו, מקיים הפורום מפגשים לאורך השנה, מזמין מרצים ועורך סקרים בנושאים הקשורים לפעילות הביקורת הפנימית בכלל ופעילות המבקרים הראשים בפרט. בנוסף מקיים הפורום קבוצת ווטצ' אפ המאפשרת לחברי הפורום מקום לקשר שוטף ומידי. גיבוש מאגר יועצים המומחים בביצוע ביקורת במגוון נושאים ועוד.



- בין הנושאים שיעלו במפגש הקרוב *
- קביעת היקף הביקורת הנכון - נוסחה, Bench Mark או תחושת בטן
- ממשק ויחסי גומלין בין מבקר פנים לדירקטוריון
- אפשרויות תגמול מבקר פנים
- מקומו של המבקר בליווי פרויקטים גדולים
- כיסוי נושא מעילות והונאות במסגרת תוכנית העבודה השנתית
- מעקב אחר יישום המלצות הביקורת - גישות, מערכות ועוד
- עשר טיפים לשיפור שיווק הביקורת הפנימית

* הנושאים וסדר הדיון עשויים להשתנות

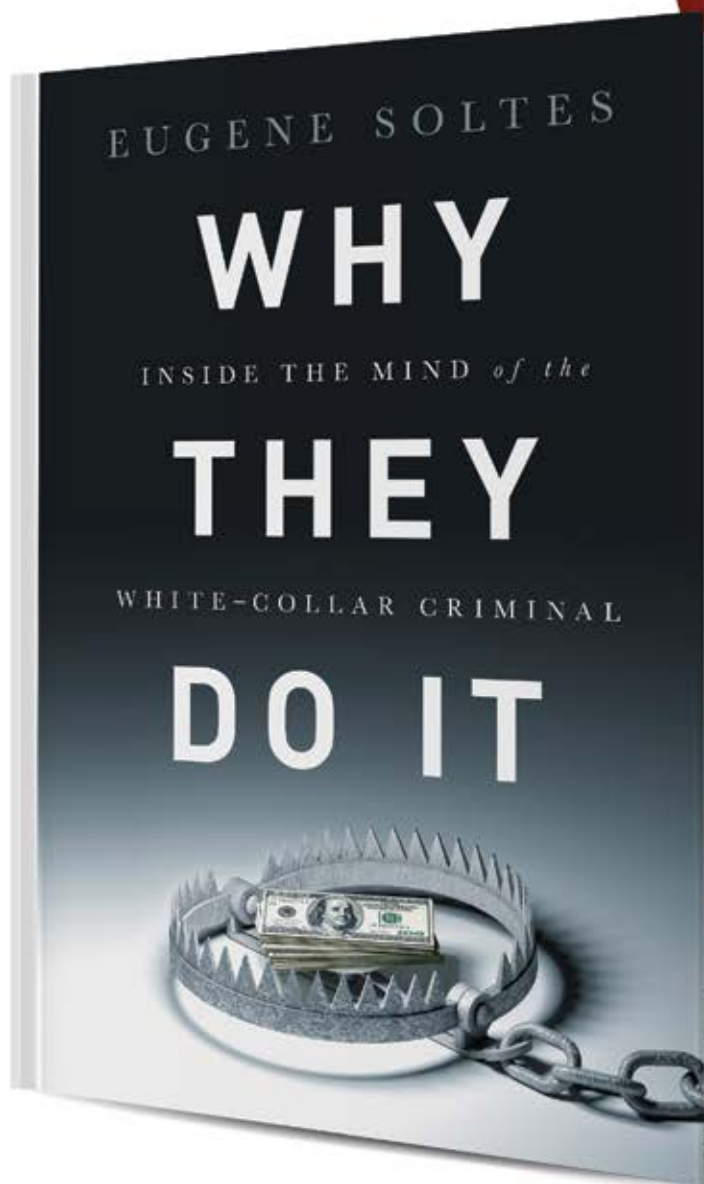


המפגש הבא של הפורום יתקיים ביום רביעי ה- 5 באפריל 2017 במשרדי חברת פרטנר רחוב העמל 8, פארק אפק ראש העין

**להרשמה למפגש הקרוב יש לפנות לאינה גולדרביטר מזכירת IIA
טלפון: 03-5116617 | theiiaisrael@gmail.com**

**לפרטים נוספים על פעילות הפורום ניתן לפנות לגיל בר
0542466718 - נייד | gilber@elal.co.il**

*** החברות בפורום מוגבלת למבקרים פנימיים ראשיים בלבד.
בפורום כ- 60 חברים המשמשים כמבקרים פנימיים ראשיים בארגונים המובילים בישראל.**



ביקורת על ספרים
כשהמנכ"ל חוצה
קווים אדומים

ד"ר יוסי נטוביץ, רו"ח

מאת

ביקורת ספר: מדוע הם עושים את זה (Why they do it)

מחבר: יוג'ין סולטס (Eugene Soltes)

בהוצאת: Public Affairs New York, 2016

חידת המנהלים העבריינים

בחודש דצמבר האחרון נפל דבר בעולם הניהול, נוחי דנקנר הורשע בגין עבירת הרצת מניות ונידון לשנתיים מאסר. דנקנר, שנחשב עד לא מזמן לאיש החזק ביותר בכלכלה הישראלית, הוא אולי דוגמה בולטת אבל בהחלט אינו המורשע היחיד - בספטמבר נשלח למאסר ג'קי בן זקן, איש עסקים מתוקשר המכונה ה"כריש", בגין הרצת מניות. גם אפי רוזנהויז ואלי גידור, המכ"ל וסמנכ"ל הסחר של שופרסל, נשלחו בשנת 2015 למאסר בגין פגיעה בתחרות, כאשר רק מספר שנים קודם לכן, בשנת 2009,

דרישת שלום מבית הסוהר

והנה כעת, אולי בהשראתו של קרסי, ערך יוג'ין סולטס מבית הספר למנהל עסקים באוניברסיטת הרווארד מחקר, שבמסגרתו איתר בבתי הכלא כ-50 מנהלים בכירים שהורשעו בעבירות כלכליות חמורות והתכתב איתם תקופה ממושכת בדואר האלקטרוני ובדואר, רכש את אמונם והם שיתפו אותו בגילוי לב בסיפורם האישי. בין המרואיינים יש גם מורשעים מפורסמים כגון ברני מידוף, וכן מנהלי החברות אנרון ו-Tyco. העבירות שביצעו המנהלים מגוונות - רישומים כוזבים בספרי תאגיד, דוחות כספיים מטעים,

אחת התופעות הבולטות אצל המנהלים העבריינים היא

חוסר המודעות לחומרת העבירה בשעת מעשה

מסירת הודעות שקריות לבורסה, תשלומי שוחד, מעילות ענק, וכמובן הונאות "פונזי" ועוד מעשים "טובים" אחרים. באופן בהיר וקולח, בלי לוותר על העומק הלמדני, סולטס מביא את הסיפורים ומנתח אותם. אחת התופעות הבולטות שהוא מזהה אצל המנהלים העבריינים היא חוסר המודעות לחומרת העבירה בשעת מעשה. המעשים החריגים שלהם כלל לא נתפסים בעיניהם כפליליים, אלא כניצול לגיטימי, לעתים "מבריק", של פרצה שזוהתה בחוק, כפעילות בשטח ה"אפור" בלי לחצות את הקו הפלילי, וגם אם כן - העבירה שנעברה נתפסה כטכנית, קלה ובלתי מזיקה.

מיליון דולר למסיבת יום הולדת לאישה

לדוגמה, סולטס מביא את סיפורו של דניס קוזלובסקי, המנכ"ל לשעבר של חברת Tyco, שלמרות היותו אחד המנהלים המתוגמלים באמריקה, לא נמנע מלבצע מעילה של כ-100 מיליון דולר על ידי מחילה לא תקינה של הלוואות שהוא עצמו היה חייב לחברה. קוזלובסקי מספר:

הוכתר רוזנהויז על ידי גלובס כ"איש השנה". וזו רק רשימה חלקית. תופעת המנהלים המצליחים והנערצים שהופכים לעבריינים מתפשטת בארץ ובעולם. מה מניע מנהלים בכירים שהשיגו בעמל של שנים רבות מוניטין, כסף וכוח, לסכן את כל הישגיהם ולבצע עבירות כלכליות?

שאלה זו אינה נשאלת מתוך סקרנות בלבד. התשובה עליה חשובה לכל הלוחמים בעבריינות כלכלית. כבר לפני כשישה עשורים, הסוציולוג דונלד קרסי כיתת את רגליו בין בתי כלא בארה"ב וראיין מאות אסירי צווארון לבן שביצעו הונאות ומעילות במטרה להבין את מניעיהם. ספרו "כסף של אנשים אחרים" (Other People's Money) הניח את היסודות למודל הידוע כיום בשם "משולש ההונאה" - תנאים שבהתקיימם נוטה אדם לבצע מעילה: לחצים שלא ניתנים לשיתוף, קיום הזדמנות טכנית, והצדקה עצמית. מודל זה מהווה עד היום אבן יסוד בפרקטיקה למניעה וגילוי של הונאות ומעילות.

הוצאה מזויפות בגובה השוחד ששילמו, והחברה אישרה את החשבונות ושילמה להם החזרים בגין. הם טענו כי החברה עצמה היא זו שהנחתה אותם לפעול בדרך זו. בהפגנה נשאו העובדים שלטים שבהם נכתב "החזירו לנו את כספנו שעשינו בעבודה קשה". מסתבר שאת הפרקטיקה - הן של תשלום השוחד והן של קבלת ההחזר באמצעות קבלות מזויפות - הם למדו למעשה מהמנהלים שלהם.

מודעות נמוכה לתוצאות

אף אדם שבוחר בקריירה ניהולית לא מתכנן להפוך לעברייך, אומר סולטס. אז מה משתבש בדרך? סולטס מנתח את הגורמים למעשיהם העברייניים של המנהלים מהיבטים ביולוגיים, פסיכולוגיים, חברתיים וכלכליים. בין היתר הוא מסביר שמנהלים מקבלים החלטות על סמך אינטואיציה ותחושות בטן. אלא שבעולם העסקים המודרני "המצפן המוסרי" הפנימי של מנהלים שהנחה אותם בעבר להבחין

"כאשר המנכ"ל נמצא בחדר, כל הדירקטורים נוטים לנסות ולרצות אותו. הדירקטוריון היה נותן לי כל מה שביקשתי. הכול". לא מפתיע שהדבר יצר אצלו תחושה של "מגיע לי" - "האמנו בפרסומים של עצמנו... אתה מתחיל להיכבש על ידי הארגונטיות של עצמך ובאמת מאמין שאתה יכול לעשות כל דבר, ללא כל התנגדות מצד אחרים בחברה". קוזלובסקי לא הרגיש צורך לוודא את תקינות מעשיו. "לא שמתי לב לענייני האישורים", הוא אומר, "מה שהייתי באמת צריך לעשות זה פשוט לקחת פיסת נייר ולהחתים את הדירקטוריון לכל בונס שביקשתי. זה משהו שאתה לא חושב עליו ונעשה במהלך הבנייה של החברה. אתה חושב על איפה נמצא הרווח וההפסד, מה קורה עם 260,000 המועסקים, כלומר אנו עשינו מכירות של 250-350 מיליון דולר ביום. עם מספרי ענק כאלה אתה לא יושב וחושב על הטכניקה שבה יאושר הבונס שלך".

הארגונטיות של קוזלובסקי הייתה חסרת גבולות: בחשבון

"האמנו בפרסומים של עצמנו... אתה מתחיל להיכבש על ידי הארגונטיות של עצמך ובאמת מאמין שאתה יכול לעשות כל דבר, ללא כל התנגדות מצד אחרים בחברה"

- בין טוב לרע, נוטה כיום "להתבלבל" ממספר סיבות:
 - היעדר קשרים בין המנהל העברייך לבין הנפגעים ממנו - הגלובליזציה של העסקים מרחיקה פיזית ומפרידה ביניהם, ומגמדת את החומרה שבה הוא תופס את מעשיו ("רחוק מהעין רחוק מהלב").
 - שינויים מהירים ברגולציה - מה שהיה רק לפני כמה שנים מותר - היום אסור, ולא תמיד התפיסה האתית הניהולית משתנה במקביל.
 - עומס העבודה המטורף גורם למנהל לקבל החלטות ללא הקדשת זמן מספיק למחשבה וללא מודעות מספקת למלוא ההשלכות.
 - מנגנון של דיסוננס קוגניטיבי מייצר צידוקים ורציונליזציות שמסייעים למנהל להתגבר על אי הנוחות שלו, אם קיימת, ממעשיו הבלתי מוסריים.
- נראה לי, מהיכרותי את הנושא ומניסיוני בביקורת פנימית, כי ייתכן שסולטס עושה קצת "הנחות" לעברייני הצווארון

ההוצאות שלו נמצאו תשלומים של 6,000 דולר על וילון מקלחת, 15,000 דולר לרכישת מעמד למטריות בצורת כלב, ומיליון דולר עבור עיבוד מסיבת יום הולדת בסגנון רומאי באי סרדיניה שערך לכבוד אשתו. מה שהפיל את קוזלובסקי בסופו של דבר הוא קנאה שעורר תשלום של כ-20 מיליון דולר, ללא אישור, לדירקטור יחיד על חלקו בארגון רכישת חברת בת. דירקטור אחר ששמע על המענק לחברו במסיבת קוקטייל נמלא כעס והעמיד לראשונה את הדירקטוריון בעימות עם המנכ"ל.

מדאיג עוד יותר להיווכח כיצד חוסר מודעות לפגמים אתיים חמורים בעשייה עלולים לדבוק בקלות לא במנהל אחד בלבד אלא בקבוצת עובדים שלמה. לשם המחשה, בשנת 2014, מול משרדי חברת הפארמה גלקסו-סמית-קליין (GSK) בשנגחאי הפגינו עשרות אנשי מכירות, הם מחו על החלטת החברה שלא לשלם להם יותר החזר בגין שוחד שנהגו לתת באופן קבוע לרופאים ולבתי חולים לקידום מוצרי החברה. במשך שנים הם הגישו חשבונות

מכנה "דיסוננס אי נוחות" - הצבת חסמים שימנעו קבלת כל הצעת החלטה של המנהל בהנהלה באופן אוטומטי, וידרשו ממנו להאט, לחשוב ולשקול יותר לעומק את עמדתו, לדוגמה על ידי שמיעת דעות מנוגדות ועצמאיות מצד גורמים אחרים, מעין "איפכא מסתברא". דיסוננס כזה, אם היה קיים ב-Tyco, היה מחייב את קוזלובסקי לעצור ולבחון בשיקול דעת את החלטותיו ואולי להימנע מהוצאה ללא אישור של מיליון דולר על יום הולדת לאשתו ושל 20 מיליון דולר לדירקטור. האתגר הגדול הוא כיצד לייצר מצבי אי נוחות כאלה. הביקורת הפנימית תהיה מן הסתם חייבת לוודא שהממשל התאגידי של הארגון עומד באתגר ואכן מייצר "אי נוחות" ברמה מספקת באמצעות תרבות אתית של שקיפות ונשיאה באחריות מצד המוסדות המנהלים, ואולי אף ליטול בעצמה חלק ביצירת "אי נוחות" זו.

לסיום, סולטס מזהיר את קוראיו שלא ללקות בהרגשת עליונות מוסרית ובשיפוטיות כלפי המנהלים שמעדו, שכן זה עלול לקרות לכולנו. רק אם ננהג בענווה ונכיר בחולשות האנוש שלנו, לא נקבל החלטות על סמך תחושות בטן, נפעיל כלפי עצמנו יותר ביקורת עצמית, ונסכים לשמוע דעות מנקודות מבט אחרות ועצמאיות ונתחשב בהן, רק אז נוכל להרחיק עצמנו במידה מסוימת מסיכון זה. לא ניתן לתאר טוב מזה את חשיבותה של הביקורת הפנימית במניעת עבירות כלכליות בארגון.

הלבן, ומקבל את תירוציהם כעובדות בלתי מעורערות. ייתכן גם שההתחככות שלו איתם במשך תקופה ארוכה כפי שתיאר, גורמת לו לאמפתיה כלפיהם. קשה להאמין שאנשים נבונים, ומניפולטיביים, המודעים היטב למעשיהם ולהחלטותיהם - שהרי אם לא היו כאלה לא היו מגיעים לעמדות הניהוליות הבכירות שמילאו - מאבדים מודעות ושוגים בנאיביות באופן סלקטיבי רק ביחס למעשים האסורים שביצעו. עם זאת, אני מוכן לקבל שהתיאור הזה נאמן לאופן שבו מעשיהם נתפסים במחשבתם.

המבקר הפנימי ו"דיסוננס אי הנוחות"

מבקרים פנימיים, בין אם יקבלו את התיאוריה המרתקת של סולטס ובין אם לאו, ימצאו עניין רב בספר אף שאין בו התייחסות ישירה לביקורת פנימית. התיאורים המפורטים בספר של מהלכי ביצוע העבירות וכשלי הבקרה הפנימית יספקו להם תובנות על תפקידם ועל האתגרים שניצבים בפניהם. הקורא יוכל להעריך עד כמה חשוב לארגון מבקר פנימי עצמאי, מקצועי ובלתי תלוי, הנאמן לתפקידו גם כאשר "רוח מפקד" קלוקלת נושבת מחדר ההנהלה.

גם הפתרונות שבהם דן הספר עשויים לעניין מבקרים. לדוגמה, כדי למנוע ממנהל להגיע למצבים של החלטות שגויות, סולטס מציע בין היתר לקיים בארגון מה שהוא



Editor's Note

Sharon Witkowski Tabib, CPA
CIA, CRMA

Until recently, internal audit engagements topics were fairly constant and auditors applied reraped audit methods . Well, no more!

Business activities are dynamic and ever-changing, which requires us, as internal auditors, to adapt ourselves accordingly. Examples from recent years include audits on topics related to media, digital, FinTech, IoT, cyber and countless more activities.

Prominent trends for topics in which internal auditors are already required to provide added value include new methods for reporting audit findings such as the " continuous audit" presented in this issue, as well as increased use of advanced tools such as "analytics", as presented in the previous issue. Tools such as these facilitate efficient, high-level audits at any given moment and the ability to identify important findings using a minimum of resources.

An additional trend that the internal auditor is required to take into consideration is organizational culture, which constitutes an inherent risk for an organization. Organizational structure is at the heart of the decision-making process in the organization, and can present a critical risk in certain organizations. One such example is the "Volkswagen Scandal", as detailed within this issue. This fifth issue of "the Internal Auditor" journal, which

is titled "One Step Ahead", will provide you with leading professionals' input on "the internal auditors of tomorrow", which for us is already upon us.

In addition, this issue presents new academic research in the internal audit field, risk management processes that are entailed within the internal audit work and knowledge management topics. It also offers useful tools and skills, including professional IIA standards and examination of the use of polygraph for ongoing needs and requirements.

Did we say it was going to be challenging?

In the next issue we will take another step forward and examine the concept of "the internal auditor as a business partner?!". Undoubtedly, this is a very interesting and challenging matter.

A big "thank you" is due to our editorial staff, who did not compromise in the process of preparing this issue. I am also grateful to Margalit Sperber for her significant contribution to the upgrading of the issue, and to you - our readers - who show interest and send us your comments. Your input is imortant to us.

You are more than welcome to join us, take part in the journal's professional activities, express yourselves and have influence.

Upon this holiday season, I wish you all a happy Passover.



President's Note

Doron Cohen, CPA

President IIA Israel - Institute of Internal Auditors

In the last IIA conference that took place on January, I had the privilege of being re-elected for a second term as the Israel IIA president. I would like to thank the IIA members for their trust.

During my first term, our institute has established its status as the biggest professional body of internal auditors in Israel. The number of members in the organization has tripled and is now close to 800. The variety of trainings, conferences and seminars we offer is highly valued by internal auditors. We are strengthening our ties with global professional institutes and have been recognized as a leading IIA chapter. During 2016 we had the honor of hosting internal auditors from Kenya who were invited to take part in professional training, while auditors from other countries took part in other seminars that we held.

We have also significantly strengthened our ties with the local regulators and governmental bodies.

IIA Israel publishes on a regular basis a professional journal that is highly esteemed by auditors and

professionals from related areas. The journal also helps in increasing the prestige of the internal audit profession.

For all of the above, I would like to express my sincere gratitude towards my colleagues in IIA Israel management and board of directors, who work tirelessly in their spare time to promote the profession.

In the coming period, our institute will continue to enhance the internal auditor's status by promoting and influencing related legislation, first of which are the amendments of the Israel internal audit law that was enacted 25 years ago.

We are now diligently working towards upgrading the Israel IIA website in order to make it a home for internal auditors in Israel and a place that will facilitate the formation of a professional community for enriching the knowledge of each one of us.

Happy Passover to our dear readers and their family members.



נשמח בקליון הבא
לצבוי לצאת לקראת חגי תשרי, תשע"ח
ספטמבר 2017

Until the next issue, which is expected to be
released on September 2017,
We wish you a fruitful summer season

