גיליון מספר 12
ספטמבר 2020

# עידן של שיבושים

8 תוצאות השפעת משבר הקורונה על הביקורת הפנימית בישראל ובצפון אמריקה

22 חדשנות בעת משבר

38 שוד ושבר – ביקורת פנימית על תהליך ניהול משברים

54 לכל מתקפה תשובה – פרקטיקה של ניהול אירועי סייבר

78 שדה הקרב של העסקים עובר למדיה החברתית – גם המבקר הפנימי מתייצב

# תוכן עניינים


**דברים**

2 דבר הנשיא

3 דבר העורכת

**על המדוכה**

4-5 מהנעשה בעולם

6-7 משולחן IIA ISRAEL חדשות, ועדות ועדכונים

8-11 תוצאות השפעת משבר הקורונה על הביקורת הפנימית בישראל ובצפון אמריקה

12 תאגידים בנקאיים בצל הקורונה - תובנות על פעילות הביקורת הפנימית

14-16 קורונה. בדיקה מרחוק - בדיקה מקרוב

**שיבושים וחידושים**

18-20 הערכת סיכונים בעולם שלאחר המגפה

22-25 חדשנות בעת משבר

26-30 NEW NORMAL - כיצד ליישם ולנהל עבודה מרחוק בצורה נכונה

32-36 הונאות ומעילות בישראל - תמונת מצב ומבט לעתיד על רקע משבר הקורונה

**כלים ופרקטיקות עבודה**

38-41 שוד ושבר - ביקורת פנימית על תהליך ניהול משברים

42-44 להמחיש בתרחיש - על היתרונות שבבדיקת עירנות (בדיקת פתע)

46-49 פיילוט לאוטומציה רובוטית של תהליכים

50-53 מהם סיכוני OT בארגון ואיך נדרש לבקר אותם

54-57 לכל מתקפה תשובה - פרקטיקה של ניהול אירועי סייבר

58-61 ביקורת ANALYTICS - מאקסל ועד DATA SCIENCE

**תובנות ודעות**

62-64 הדחף לשינויים בביקורת הפנימית

66-69 עדכון גרסה 20.20 - המבקר הפנימי על רקע שיבושים

70-73 GAME OVER - הביקורת הפנימית במשרדי הממשלה

74-76 כבר תרמתי במשרד - השפעת משבר הקורונה על המגזר השלישי

78-80 שדה הקרב של העסקים עובר למדיה החברתית - גם המבקר הפנימי מתייצב

**NOTES**

82 Editor's Note

83 President's Note



IIA Israel - Institute of Internal Auditors in Israel

office@theiia.org.il

לשכת המבקרים הפנימיים



עורכת כתב העת **שרון ויטקובסקי טביב**, רו"ח, CIA, CRMA

סגן העורכת **אורן שחר**, רו"ח, MBA, CISA, CIA

חברי המערכת **דוד אגרנט**, CIA, רו"ח

**איל אורון**, עו"ד

**שלומית איתן**, עו"ד, CIA

**יוסי אליאס**, רו"ח

**דרור בר משה**, רו"ח, LLM, CIA, CISA, CFE,CISM,CSX-F, CRMA, CRISC

**ננסי זכאכ אבו אלנסר**, רו"ח, MA, QAR

**נאוה חלמיש**, רו"ח, MA

**חן כץ**, רו"ח, EMBA, CIA

**ד"ר יוסי נטוביץ**, רו"ח

**ליאור סגל**, רו"ח, עו"ד, MBA

**ד"ר גבי סייג**, D.E.A

**בועז ענר**, רו"ח, MA, CIA

**דורון רונן**, רו"ח, CSX-F, CDPSE CIA, CRMA, QAR, CRISC, CFE, MA, LLM

**מרגלית שפרבר**, רו"ח, MBA, CIA

מנהלת לשכת נשיא הלשכה **אינה גולדרביטר**

עיצוב ועריכה גרפית **סטודיו דגה**

עריכה לשונית והגהה **אודי לוינגר**

מו"ל **לשכת המבקרים הפנימיים - IIA ישראל (חל"צ)**



לשכת המבקרים הפנימיים - IIA ישראל

כתובת למשלוח דואר **ת.ד. 29281 תל אביב 6129201**

טל **03-5116617** | פקס **03-5116647** | לתגובות והערות **office@theiia.org.il**



המובע במאמרים מבטא את דעת הכותבים בלבד. אין הלשכה נושאת באחריות כלשהי בגין הנכתב בהם.

כל הזכויות שמורות ל-לשכת המבקרים הפנימיים - **IIA** ישראל. ט.ל.ח

# דבר הנשיא

**דורון רונן, רו"ח**, CIA, CRMA
נשיא לשכת המבקרים הפנימיים IIA ישראל

מגפת הקורונה מאתגרת את העולם. מדינות, ארגונים ויחידים מתמודדים עם קשיים בריאותיים, כלכליים ותפעוליים חסרי תקדים, ועם חוסר ודאות מתמשך שקיצו אינו נראה באופק.

המגפה טלטלה גם את מקצוע הביקורת הפנימית, ועולות שאלות כמו: מהי מידת חיוניות המבקר הפנימי? כיצד הוא יכול לסייע לארגונים להתמודד עם המצב? האם לשנות פרדיגמות ישנות? ועוד. גיליון זה עוסק בנושא "**עידן של שיבושים**" וירחיב בסוגיות אלה.

לפני מספר חודשים נבחרתי לנשיא הלשכה, ואני מודה על האמון שניתן בי להוביל את הלשכה בתקופה מאתגרת זו. נשמור על לשכתנו מקצועית ולמען החברים והמקצוע. נמשיך לצייד את החברים בידע ובכלים: כנסים והשתלמויות, לימודים אקדמיים, כתב עת, תקנים והנחיות מקצועיות, מענה לשאלות מקצועיות, הגנת חברים, ושיתופי פעולה עם ארגונים בארץ ובעולם.

אני מבקש להודות לרו"ח **דורון כהן**, שסיים את תפקידו כנשיא הראשון של הלשכה לאחר שמונה למנכ"ל חברה גדולה. דורון כיהן תחילה כנשיא איגוד המבקרים הפנימיים, ולאחר שהוביל מטעם האיגוד את איחוד הגופים המקצועיים כיהן כנשיא הלשכה המאוחדת.

כאשר בארץ ובעולם מתמודדים עם משבר כלכלי לצד התפתחות טכנולוגית, מתגברת הנחיצות למתן ערך מוסף אמיתי ומשמעותי מהביקורת הפנימית, ולחיזוקה כשומרת סף חשובה. אנו תורמים לשיפור הבקרות הפנים-ארגוניות והתהליכים.

המגפה הציבה ללשכה אתגרים מורכבים. למרות הקשיים, הגדרנו צ'רטרים לוועדות, קיימנו השתלמויות רבות מרחוק, ניסחנו ניירות עמדה (לרבות בנושאים שלעיל), אישרנו הנחיות מקצועיות ייחודיות לישראל (כגון תפקיד המבקר הפנימי כנת"ץ), השקנו לראשונה מסלול תואר שני במשפטים בהתמחות ביקורת פנימית (נוסף על המסלולים הקיימים באקדמיה), שילבנו חומר מקצועי רב באתר, ואנו נערכים בגמישות מחשבתית (כיאה למצב) לכנס המקצועי השנתי שייערך ב-21.1.21.

כמו כן התנענו ועדת אסטרטגיה שתעסוק בדמותו של המבקר בעתיד. במקביל, מתקיימת תחרות לאיתור מבקרים צעירים פורצי דרך שיוכרו בכנס השנתי.

**אני קורא למבקרים שטרם עשו זאת להצטרף ללשכה.** נושאים חשובים רבים על הפרק: מעמד המבקר הפנימי, חוק הביקורת הפנימית ועוד. לשכה גדולה וחזקה תוכל לקדם את הנושאים באפקטיביות ולתרום לכלל המבקרים.

נוסף על הוועדות הקמנו **פורומים: מגזריים** (פיננסי, חברות ממשלתיות, משרדי ממשלה, רשויות מקומיות), **מקצועיים להתמחויות** (ניהול סיכונים, מעילות והונאות, חדשנות ואנליטיקס, אבטחת מידע וסייבר), **למבקרים ראשיים, ולמבקרים צעירים.**

**כל חבר וחברה שרוצים לקדם נושא בלשכה מוזמנים לעשות זאת; רק ביחד נוכל לפעול לטובת המקצוע והחברים!**

**שנה טובה, בריאות, חוסן, וחזרה מהירה לשגרה,**
**שלכם ובשבילכם,**
**דורון רונן**



# דבר העורכת

**שרון ויטקובסקי טביב**, רו"ח, CIA, CRMA
סגנית נשיא לשכת המבקרים הפנימיים - IIA Israel

את הגיליון הקודם הוצאנו במהלך חודש מרץ 2020, בשיאו של "משבר הקורונה". נראה כי בתוך משבר העל שהביא עימו נגיף הקורונה, הארגונים מנהלים תתי-משברים והמערכת נדרשת לפעול מהר, בתנאי לחץ ובאי ודאות עצומה - תנאים גרועים לקבלת החלטות. כעת ברור לכולם כי אין מדובר במשבר זמני או חולף, אלא במציאות חדשה שתלווה אותנו לא מעט חודשים (ויש שיגידו גם שנים) - The New Normal. המציאות החדשה שנכפתה עלינו מהווה ביטוי מובהק למשבר המגלם בתוכו איומים וסיכונים אך גם הזדמנויות רבות, הן בהיבט האישי (לא מעט מאיתנו "גילו מחדש את המשפחה") והן בהיבט המקצועי (למדנו שניתן לייעל את תהליכי העבודה בלי לפגום באיכות).

כדי להעריך את השפעת משבר הקורונה על הביקורת הפנימית, הופץ באפריל 2020 סקר של ה-IIA בצפון אמריקה. במקביל ערכנו ביולי 2020 סקר בקרב המבקרים הפנימיים הראשיים בישראל, במטרה לנתח את השינויים שחלו בארץ בעקבות המשבר בהשוואה לסקר של ה-IIA - עיקרי הסקר וההשוואה מוצגים בגיליון.

מהסקר עולה כי הביקורת הפנימית בישראל זריזה, גמישה ומגיבה מהר לשינויים.

עוד עולה מהסקר כי חלו שינויים משמעותיים בעבודת הביקורת הפנימית: בהיקף כוח האדם, בתוכניות העבודה השנתית ובמטלות הביקורת, וכן בתקציב הביקורת ובפוקוס שלה.

כתב העת נכתב בסימן "עידן של שיבושים" וחילקנו את המאמרים בו לכמה קבוצות:

**שיבושים וחידושים:** הערכת סיכונים בעולם שלאחר מגפה עולמית, חדשנות בעת משבר - אתגרי המגפה כהזדמנות, כיצד ליישם ולנהל עבודה מרחוק.

**כלים ופרקטיקות עבודה:** ביקורת פנימית בעידן של משברים - סיכון מהותי וקיומי המהווה חלק מניהול הסיכונים התאגידי, אתגר "הירידה לשטח" והיתרונות שב"בדיקת ערנות", ניהול אירועי סייבר ועוד.

**תובנות ודעות:** מבקרים משתפים: הדחף לשינויים בביקורת הפנימית - בתקופה הקורונה; השינויים שנדרש המבקר הפנימי לבצע על רקע השיבושים; מיקומה של הביקורת פנימית במשרדי ממשלה בעת חירום; השפעת משבר הקורונה על המגזר השלישי ועוד.

אנו נדרשים לבצע שינויים משמעותיים בתהליכים ואולי אף שינוי תפיסתי, והתקופה הזאת היא שעת מבחן לביקורת הפנימית: האם אנחנו מיישמים בעצמנו את הרעיונות? האם אנחנו עצמנו מסוגלים להשתנות ולהתאים את עצמנו למציאות החדשה והמתחדשת? האם אנחנו עסוקים בהסתגלות או מובילים קידום תהליכים שהיו תקועים בחסות הקורונה? האם אנחנו מחכים שיקראו לנו או תופסים מקום תחת האלונקה? האם אנחנו משמשים דוגמה אישית וארגונית לכל אלה?

ובימים אלה של תחילת השנה החדשה אני מקווה שנדע ונשכיל להיות מן המובילים שרואים את נקודת האור בכל מצב וצומחים ממנה.

אני מבקשת לסיים באחת מהברכות הנהוגות בערב ראש השנה: "שנהיה לראש ולא לזנב".

**אני מאחלת לכולכם קריאה מהנה ומפרה,**
**שנה טובה ובריאות איתנה,**

**שרון ויטקובסקי טביב**

# מהנעשה בעולם

## הלחצים של מגפות עולם

"במהלך המגפה המבקרים הפנימיים צריכים להתמקד בבניית בקרות חזקות יותר", כך אומר נשיא המוסד לניהול המשכיות עסקית, מר מו האנג גו.

איך יכולים המבקרים הפנימיים לתמוך בהמשכיות עסקית בעת מגפה עולמית? ברגע שמתפרצת מגפה עולמית כמו הקורונה, מבקרים פנימיים צריכים להפחית את מרבית פעילותם, מאחר שעבודתם כרוכה בסיכון ההדבקה בין מבקר למבוקר. מה עוד שתשומת לב הלקוח ממוקדת במתן מענה למשבר ובהתאוששותן של הפונקציות הקריטיות בארגון.

במהלך המגפה צוות המבקרים יכול להתמקד באיתור תקלות פוטנציאליות בבקרות על תהליכים, מפני שהעובדים פועלים ממקום מרוחק או חלופי או אפילו מביתם. הדבר החשוב ביותר הוא לחזק את הבקרות כדי למזער את הפוטנציאל לשגיאות הנובעות מפעולות המתבצעות באופן ידני ואת הפוטנציאל למקרי הונאה. ראוי לציין כי המעקב אחר אי-ציות לנהלים הקיימים צריך להתבסס על מקרים מהותיים כדי לאפשר לארגון להגיב ולהתאושש במהירות האפשרית.

בדרך כלל, סקירות של תוכניות המשכיות עסקית נקבעות מראש על פי המדיניות לניהול ההמשכיות העסקית, והסקירה והעדכון מתבצעים בדרך כלל פעם בשנה. אולם בעת מגפה עולמית, כמו בעת כל אירוע משבש אחר, צריך לבצע את הסקירות הללו בתדירות גבוהה יותר, מפני שבתקופה כזו הלקוח מתמודד עם תחלופת כוח אדם גבוהה או מעביר משימות עסקיות למיקור חוץ או לצד שלישי ובכך יוצר סיכון של תלות החברה בספק.

## איתור והתקשרות עם ספקים במהלך משבר

**"התקשרויות עם ספקים חדשים עלולות ליצור סיכונים חדשים", אומר אריק הנקה, מנהל מחלקת ההמשכיות העסקית במרכז הרפואי מאיו קליניק.**

מגפת הקורונה גרמה לכך שחברות רבות נאלצות לבחון מחדש את יכולת השרידות של ספקיהן. כיצד ארגונים יכולים לעבור במהירות לספקים חדשים? מגפת הקורונה חשפה לא רק את סיכוני הספקים המסורתיים בכל הנוגע לשיבושים בשרשרת האספקה, אלא גם יצרה זירה חדשה של ספקים מתווכים שמכניסים סיכונים חדשים לתוך השוק. בתחום הרפואה, קיים מחסור במוצרים באמצעות הערוצים המסורתיים עקב בעיות עודף ביקוש, ולכן אנו מחפשים מוצרים בשווקים אלטרנטיביים. בעת החיפוש עבור ערוץ חלופי, אנו עדים לתופעה גוברת של מוצרים מזויפים ולתופעה של מתווכים הדורשים תשלום מראש ואז נעלמים עם הכספים שניתנו להם. תופעות כאלה מעידות על הצורך לפתח כלים חדשים לביצוע מהיר של בדיקות רקע ואמינות של ספקים ומתווכים חדשים.

הביקורת הפנימית צריכה לסייע לבעלי התפקידים לבצע את משימותיהם באופן מיטבי על ידי הצגת כל הסיכונים הארגוניים על כל רמותיהם באופן רחב ומעמיק ביותר. כמו כן, המבקרים צריכים להיות זמינים לפעול כיועצים על מנת לסייע במזעור הסיכונים בשווקים בעת היווצרותם, בין באמצעות מתן עזרה בבניית תוכנית לניהול סיכוני צד שלישי ובין הסיוע במציאת ספקים אסטרטגיים. המבקרים יכולים להציע "עוד זוג עיניים" אובייקטיבי על התהליך, שהוא בדרך כלל לא מוכר בשרשרת האספקה בתחום הרפואי.





## תמונת מצב של בינה מלאכותית

**למקבלי ההחלטות בחברות הטכנולוגיה בארצות הברית יש תקוות גבוהות ולא מעט חששות לגבי בינה מלאכותית.**

**88%** סבורים שחברות צריכות ליישם מדיניות אתיקה על מנת לפקח על השימוש בבינה מלאכותית אצלן.

**62%** סבורים שהשימוש בבינה מלאכותית מתקדם בקצב ראוי בקרב חברות בתעשיית הטכנולוגיה.

**69%** סבורים שממשלות צריכות להסדיר את השימוש בבינה מלאכותית.

**61%** סבורים שהעובדים הקיימים מוכנים ליישום של בינה מלאכותית.

**37%** טוענים שבינה מלאכותית יכולה להחליף אותם בתפקיד.

מקור: KPMG, "Living in an AI World" –2020 Report; Technology Insiders.

## התאוששות באמצעות כתיבה ספרתית (דיגיטציה)

מחקרים מראים כי הטכנולוגיה היא המפתח העיקרי לניווט משברים

דוח חדש מאת מקינזי מייעץ לעסקים להתמקד בדיגיטליזציה כדרך לנווט את משבר מגפת הקורונה. לפי הדוח, כאשר מנהלי ארגונים שוקלים איך להתקדם, ההיבטים החשובים ביותר יהיו גמישות ומהירות. חברת הייעוץ מציינת בדוח כי ההתאוששות ממגפת הקורונה מבוססת על אמצעים דיגיטליים.

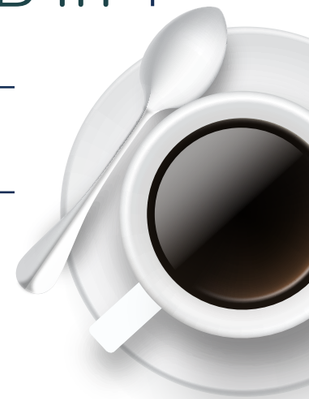
מגפת הקורונה מעמידה במבחן את המודלים העסקיים הישנים, וסביר להניח שהדבר יגרום להאצת המעבר לאמצעים דיגיטליים. כותבי הדוח מודעים לכך שארגונים חייבים לנקוט צעדים אמיצים, אך בה בעת הם צריכים לפעול בזהירות "ולהעריך כראוי את הסיכוניהחל מאובדן כוח אדם מוכשר וכלה בהתקפות סייבר". שינויים טכנולוגיים הדרגתיים וצעדים חלקיים מהווים מתכונת לכישלון.

ביצוען של ההשקעות הנכונות בטכנולוגיה יהיה עניין קריטי בהמשך, ומנהלי ארגונים יצטרכו לעבוד באופן הדוק עם מנהלי הטכנולוגיה שלהם כדי לעדכן מערכות ישנות ולהקים יכולות דיגיטליות חדשות. הטכנולוגיה היא התורמת לערך הארגוןלרבות השימוש בכלים אנליטיים מתקדמים.

בדוח מצוין כי "הצורך בנתונים מדויקים בעיתוי הנכון אף פעם לא היה חיוני כל כך בעבר כמו היום". אולם מנהלי החברות יצטרכו לעבוד עם מנהלי הסיכונים שלהם על מנת לוודא שתוך כדי המרוץ להשגת הנתונים הנדרשים, ארגוניהם עדיין מקפידים לעמוד בחוקי הגנת הפרטיות ומיישמים את השיטות המיטביות בתחום הגנת הסייבר.

על מנת להבטיח שיוזמות טכנולוגיות מתממשות, מנכ"לים יצטרכו גם לנהל שיחות מעמיקות עם סמנכ"ל הכספים שלהם. הסקר של Covide-19 CFO Pulse Survery - PwC מצא שיותר משני שלישים ממנהלי הכספים שהשתתפו בסקר השיבו שהם מתכוונים לדחות או לבטל השקעות מתוכננות בעקבות משבר הקורונה - מתוכם יותר ממחצית ציינו שהם שוקלים לבטל יוזמות בתחום מערכות טכנולוגיות. עוד רבע מהנשאלים ציינו שהם דוחים או מבטלים השקעות בתחום הטרנספורמציה הדיגיטלית.

# משולחן IIA ISRAEL
# חדשות ועדות ועדכונים



**מבקר המדינה** נפגש עם רו"ח דורון רונן, הנשיא הנכנס של הלשכה.
בפגישה נדונו שיתופי פעולה אפשריים בין שני הגופים.

**בני צ'יפרוט מונה למבקר הפנימי של הלשכה**

הלשכה מצאה כי **"מכרז לשירותי ביקורת פנימית לאיגוד ערים איכות סביבה אשדוד חבל יבנה".** אינו עומד בדרישות רגולטוריות ובדרישות התקנים המקצועיים לביקורת פנימית, ולא תאפשר למבקר הפנימי שייבחר למלא את ייעודו; היקף שעות זניח, קביעת תחומי הביקורת עבור המבקר, אפשרות להפסקת התקשרות בכל עת (פגיעה באי-התלות של המבקר).

**במפגש הראשון של פורום מבקרים פנימיים ראשיים בחברות ממשלתיות,** השתתפו 30 מבקרים פנימיים בחברות ממשלתיות וכן חסן טואפרה ועדיאל רונן, מבכירי רשות החברות הממשלתיות. המפגש יוחד לנושא חוזרי רשות החברות הממשלתיות וההנחיות הנגזרות מהם לביקורת הפנימית.

ניתנה סקירה כללית על ההנחיות והוצג ריכוז של כל משימות הביקורת הפנימית, הנגזרות מהנחיות אלו (לרבות, לו"ז, אחריות ונמען).

במהלך המפגש, המבקרת הפנימית של חברת החשמל וראש מינהל תהליכי ניהול בחברת התעשייה האווירית, נתנו סקירה ודגשים על דרך יישום הנחיות רשות החברות בחברות שלהן.

**הוועדה המקצועית** אישרה הנחייה מקצועית בנושא "המבקר הפנימי כנציב תלונות הציבור ודרכי הטיפול בתלונות", וקווים מנחים בנושא "ביצוע ביקורת פנימית בראי תקנות הגנת הפרטיות". הוועדה מתכננת לתרגם לעברית את "מודל שלושת הקווים" המעודכן, וכן את ה IG (הנחיות יישום) של ה IIA. בנוסף, הוועדה מכינה קווים מנחים בנושא תחקור נתונים לביקורת







# מביטים לעתיד: איך תיראה הביקורת הפנימית בשנת 2030 ?

אומנם בקצב ההתפתחות המטורף והתנודות שעוברות על העולם, 2030 נראית כמו עתיד רחוק, אי שם מעבר להרי החושך או בעצם הקורונה, אך אנו בלשכת המבקרים הפנימים יודעים שארגון שלא מסתכל לעתיד, מקטין את הסיכויים שלו להצלחה. אז החלטנו, והקמנו ועדת אסטרטגיה בהובלת גיל בר, הכוללת נציגים של כולנו, של מבקרים ותיקים ומבקרים צעירים, מבקרים מהמגזר הממשלתי, הפרטי והציבורי, מבקרי תהליכים ומבקרי טכנולוגיה, מבקרים שכירים ומבקרים עצמאים,אנשים שרואים מזוויות שונות אבל יש להם את אותה מטרה, וביקשנו מהם לחשוב אסטרטגיה, להתחיל במסע אל העתיד ולשאול בין השאר איך תיראה הביקורת הפנימית בשנת 2030? האם הביקורת הפנימית בדרך לקטסטרופה עתידית או שדווקא יש הזדמנות לצמיחה בעשור הבא ?מה יהיה פרופיל אנשי הביקורת ועוד סוגיות אסטרטגיות שעולות מהחברים.

מדובר במסע שהתוצרים שלו לא יהיו מיידים אך יהיו משמעותיים. אז רצינו לאחל לוועדת אסטרטגיה, ובעצם לעצמנו הצלחה במסע שיביא אותנו לעתיד טוב יותר

**חג שמח**
שנה טובה ומתוקה
ובריאות איתנה לכולם

נפגש בגיליון הבא שצפוי לצאת לקראת חג פסח
**מרץ 2021 , ניסן תשפ"א**

# תוצאות השפעת משבר הקורונה על הביקורת הפנימית בישראל ובצפון אמריקה

## סקר שהופץ למבקרים פנימיים ראשיים אודות שינויים בתקופת משבר הקורונה

**ניתחו וריכזו:** שרון ויטקובסקי טביב | רו"ח, MA - שותפה BDO Israel,
ראש מגזר סיכונים (RAS) - סגנית נשיא ועורכת כתב העת

בעז ענר | רו"ח, MA, CIA, מרצה, יועץ, מנהל סדנאות ביקורת,
לשעבר משנה למנכ"ל - משרד מבקר המדינה

במהלך חודש אפריל 2020 ביצע ארגון IIA סקר בצפון אמריקה במטרה להעריך את השפעת משבר הקורונה על הביקורת הפנימית. מענה לסקר התקבל ממבקרים ראשיים או מקביליהם: 90% מהם מארצות הברית, 9% מקנדה ו-1% מהקריביים.

במקביל ערכנו אנחנו בישראל ביולי 2020 סקר בקרב מבקרים פנימיים ראשיים. בסקר השתתפו 50 משיבים.

מטרת הסקר הייתה לבחון ולנתח שינויים שחלו במערך הביקורת הפנימית בארץ בתקופת משבר הקורונה (החל מחודש מרץ 2020), בהשוואה לסקר ה-IIA כאמור.

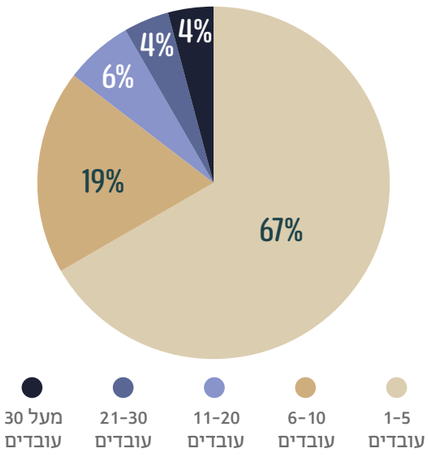
הסקר בישראל כלל 16 שאלות הנוגעות למידע כללי על הארגון, מידע על תוכנית העבודה השנתית והשינויים שחלו בה, ומידע על יחידת הביקורת הפנימית והשינויים בצוות הביקורת.

להלן עיקרי הנתונים (ולכן לא בהכרח יצטברו כל התחומים ל-100%).

## שינויים שחלו בצוות הביקורת הפנימית בישראל

### גודל יחידות הביקורת הפנימית

להלן תרשים לתיאור התפלגות מספר העובדים והמנהלים בצוותי הביקורת בארגונים שבהם ממונים המשיבים כמבקרים פנימיים:




ניתן לראות באופן מובהק כי במרבית הארגונים (כ-70%), צוות הביקורת הפנימית, לרבות העובדים והמנהלים, כולל 1-5 עובדים.

### צמצום כוח האדם ביחידות הביקורת הפנימית בעקבות משבר הקורונה

להלן התפלגות שיעור הצמצום בכוח האדם הכולל, הן צמצום קבוע והן צמצום זמני, בכלל הארגונים שבהם המשיבים הם מבקרים פנימיים:

**לא היה צמצום בכוח האדם**

שיעור המשיבים
**71%**

**צמצום בשיעור של עד 50%**

שיעור המשיבים
**18%**

**צמצום בשיעור הגבוה מ-50%**

שיעור המשיבים
**11%**

מכאן עולה שבמרבית יחידות הביקורת הפנימית, משבר הקורונה לא השפיע על היקף צוות הביקורת ולא נערך צמצום (קבוע או זמני) של כוח האדם. מנגד, ב-29% מהארגונים חל צמצום בכוח האדם, בחלקו עד 50% ובחלקו אף מעל 50%. כלומר, לצד העובדה שבמרבית הארגונים לא היה צמצום בכוח האדם, בארגונים שבהם כן נערך צמצום במספר עובדי הביקורת, בחלק מהמקרים הצמצום היה חד מאוד - מעל 50%.

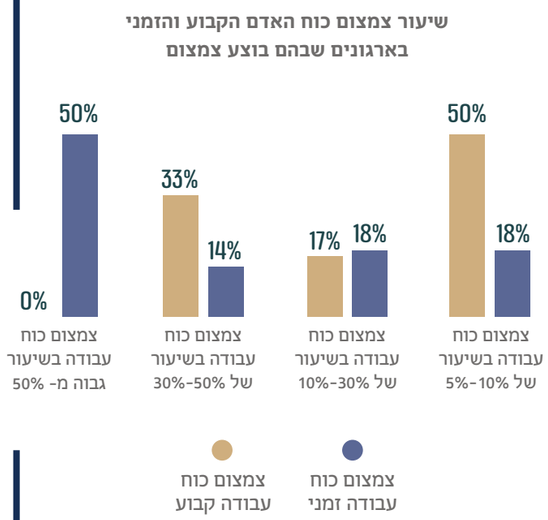




לצורך השוואה, בסקר ה-IIA עלו ממצאים דומים: ב-74% מהארגונים לא נערך צמצום כוח האדם בצוותי הביקורת, ב-21% מהארגונים חל צמצום בצוות הביקורת, ובשאר המקרים חל גידול ו/או לא התקבלה תשובה חד-משמעית.

לשם הרחבה, להלן **תרשים לתיאור שיעור צמצום כוח האדם הזמני והקבוע בצוותי הביקורת בישראל** (מתוך 29% המקרים שבהם היה צמצום), תוך הבחנה בין הפחתה קבועה להפחתה זמנית בהיקף צוותי הביקורת:

**שיעור צמצום כוח האדם הקבוע והזמני בארגונים שבהם בוצע צמצום**




מהתרשים עולה שבארגונים שבהם חל צמצום קבוע בכוח האדם, 50% מהמשיבים ציינו כי מדובר בצמצום של 5%-10% בצוות הביקורת, ובאף אחד מהארגונים לא חל צמצום כוח אדם קבוע בשיעור הגבוה מ-50%.

לעומת זאת, מתוך הנשאלים שהשיבו כי חל בארגונם צמצום זמני בצוות הביקורת, 50% מהמשיבים ציינו כי מדובר בצמצום הגבוה מ-50% מצוות הביקורת.

## שינויים בתוכנית העבודה השנתית של הביקורת הפנימית

על רקע השינויים שחלו בארגונים השונים, בחלק ניכר מהם חלו שינויים גם בתוכנית העבודה השנתית של הביקורת הפנימית. להלן התפלגות סוגי השינויים שחלו בתוכנית העבודה של יחידות הביקורת הפנימית (בנושא זה יכלו המשיבים לסמן יותר מתשובה אחת):

**עדכון תוכנית העבודה - שינוי נושאי הביקורת**

שיעור המשיבים
**40%**

**הפחתה בהיקף שעות הביקורת**

שיעור המשיבים
**23%**

**עדכון הערכת הסיכונים**

שיעור המשיבים
**20%**

**שינוי באופי ההמלצות**

שיעור המשיבים
**3%**

**אחר**

שיעור המשיבים
**14%**

**השיעור הגבוה של השינויים, בעיקר בדגש על שינוי מהותי בתוכנית העבודה, מצביע על גמישות וזריזות (AGILITY).**

לצורך השוואה, 56% מהנשאלים בסקר ה-IIA הפחיתו או שינו מטלות בתוכנית השנתית, 48% ביטלו מטלות, 39% הוסיפו מטלות חדשות, 38% הורו לצוותים לבצע עבודות שאינן בגדר ביקורת פנימית, ו-15% שינו והרחיבו מטלות ביקורת מסוימות.

## שינויים בהיקף שעות הביקורת בתוכנית העבודה השנתית (תקציב הביקורת)

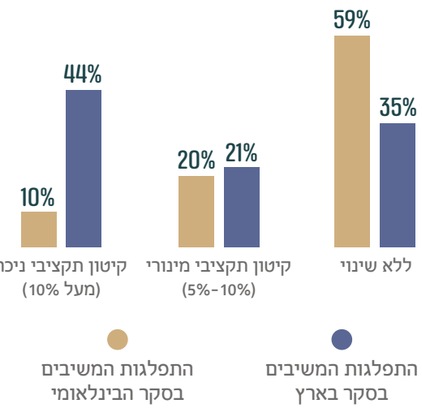
בישראל, למעלה ממחצית מהנשאלים השיבו כי לא חל שינוי בהיקף שעות הביקורת, או שחל שינוי בשיעור נמוך של עד 10%. מתוך הנשאלים שהשיבו כי חל קיטון תקציבי של שעות הביקורת, 10% העידו כי חל קיטון של למעלה מ-50%.

ערכנו השוואה בין תשובות הנשאלים בסקר בארץ לבין תשובות הנשאלים בסקר ה-IIA באשר להיקף ואופי השינוי שחל בתקציב הביקורת השנתי בעקבות משבר הקורונה.

הנחות: לצורך ההשוואה, לקחנו בחשבון שקיטון מינורי, כפי שמוגדר בסקר ה-IIA, הוא שיעור שאינו עולה על 10%, ואת ההגדרה הזאת של שינוי מינורי החלנו על תשובות הנשאלים בסקר בארץ.

בהתאם, להלן תרשים לתיאור אופי השינוי בתקציב הביקורת בסקר בארץ לעומת סקר ה-IIA:

**שינויים בתקציב הביקורת השנתי בסקר בהשוואה לסקר ה- IIA**




בסקר ה-IIA 59% מהמשיבים ציינו כי לא חל אצלם שינוי תקציבי. לצד זאת, 30% מהמשיבים חוו קיצוץ תקציבי, מתוכם כשליש חוו קיצוץ תקציבי ניכר. 2% דווקא קיבלו תוספת תקציב.

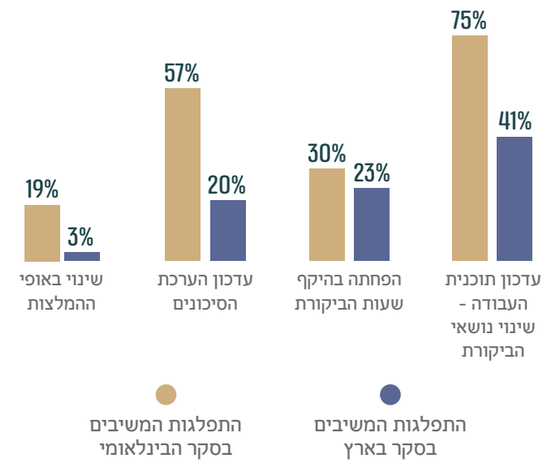
מהתרשים לעיל ניתן ללמוד כי השינויים בתקציב הביקורת בסקר ה-IIA היו מתונים יותר מהשינויים בתקציב לפי הסקר שנערך בארץ, וכי מרבית הנשאלים בסקר ה-IIA לא חוו שינוי (כ-60%), בעוד שבארץ מרבית הנשאלים חוו שינוי (כ-65%).

בהנחה שעוצמת הקיצוץ מלמדת על תפישת חיוניות הביקורת, הרי שיש כאן ממצא האומר דרשני באשר לביקורת הפנימית בישראל.

**על מהותם של השינויים בתוכנית העבודה:**

תשובות המשיבים בסקר IIA העידו על מעבר מהותי להעדפת נושאים הקשורים בשאלת ההתמודדות עם סיכונים

**השוואה בין תוצאות הסקר בארץ לתוצאות סקר ה- IIA בהתייחס לשינויים בתכנית העבודה**




הנובעים מהקורונה: 75% מהמשיבים ערכו שינויי תוכניות, 67% עסקו בזיהוי סיכונים פורצים חדשים, 57% בחנו את הערכת הסיכונים באירגון, ו-19% המליצו על תוכניות ודרכי התמודדות.

בהתאם, ערכנו השוואה בין תוצאות המשיבים בסקר בישראל לבין תוצאות סקר ה-IIA במספר סעיפים מהותיים הנוגעים לאופן ההתמודדות עם משבר הקורונה. להלן עיקרי ההשוואה:

ניתן לראות שככלל, המשיבים בסקר ה-IIA חוו שינויים בשיעורים גבוהים יותר בתוכנית העבודה מאלה שחלו אצל המשיבים בסקר בארץ.





## שינויים שחלו בנושאי המטלות (פוקוס הביקורת)

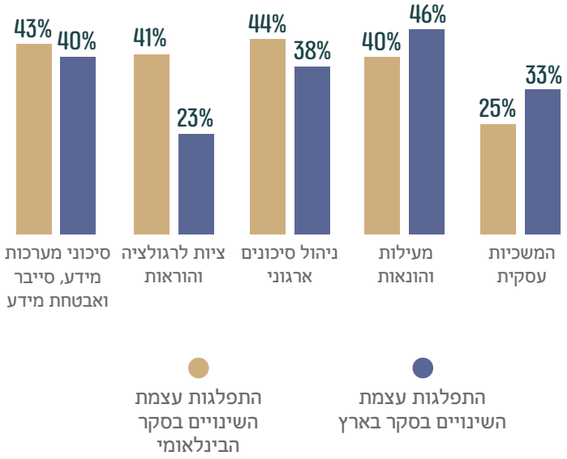
המשיבים בישראל נשאלו לגבי שינויים שחלו בנושאי מטלות הביקורת שהם מבצעים, האם חל קיטון או גידול בהיקף הבדיקה המבוצעת, וכן נשאלו באשר למוקד (הפוקוס) של השינויים: IT סיכוני סייבר ואבטחת מידע, המשכיות עסקית, שרשרת אספקה, ניהול סיכונים ארגוני, מעילות והונאות, ציות לרגולציה והוראות ושירותים שאינם ביקורת (לרבות ייעוץ שוטף וכדומה).

באשר לשאלת הקיטון או הגידול, בשקלול תשובות כלל המשיבים בישראל עולה כי בקרב 63% מהנשאלים לא חל שינוי במטלות הביקורת, אצל 34% חל גידול בהיקף הביקורת, ואצל 4% בלבד חל קיטון בהיקף הביקורת.

באשר למיקוד, נושאי מטלות הביקורת שבהן חל בישראל שיעור הגידול הגבוה ביותר הם מעילות והונאות (46%), שירותים שאינם ביקורת (42%), סיכוני מערכות מידע, סייבר ואבטחת מידע (40%), והמשכיות עסקית (33%).

בהתאם, ערכנו השוואה בין שיעור הגידול בנושאים אלה בארץ לבין התשובות שעלו בסקר ה-IIA (למעט בנושאי שירותים שאינם ביקורת ושרשרת אספקה שלא נכללו בסקר ה-IIA). התוצאות הן כדלקמן:

**שיעור גידול בנושאי מטלות ביקורת בהשוואה לסקר ה- IIA**




מהתרשים עולה כי במרבית נושאי מטלות הביקורת, ההפרשים בין שיעור הגידול בסקר בארץ לבין שיעור הגידול בסקר ה-IIA אינם מהותיים והם נעים בין 3%- 8% בלבד, למעט שיעור הגידול בנושא ציות לרגולציה והוראות, שבסקר ה-IIA עמד על 41% לעומת 23% בלבד בסקר בארץ. פער גדול קיים גם בנושא המשכיות עסקית: בארץ הקדישו לו תשומת לב גבוהה יותר בשיעור של 33% לעומת 25% בלבד בסקר של ה-IIA.

יודגש כי המשכיות עסקית היא נושא מהותי, בעיקר בתקופת משבר, ולכן היקף השינוי בישראל הוא נקודת זכות מקצועית.

הבדל מעניין שניתן לראות בסקר בארץ לעומת סקר ה-IIA הוא באשר לאופי השינויים במטלות הביקורת: המבקרים בארץ פחות הדגישו את נושא הציות והרגולציה מאשר הנשאלים בסקר ה-IIA, ומצד שני העדיפו לערוך שינויים בנושאים מקצועיים אחרים, כמפורט לעיל. אפשר שפערים אלו באשר לרגולציה מלמדים על שוני בתרבות הארגונית בין ישראל לצפון אמריקה.

לעומת זאת, בתחום סיכוני מערכות מידע, סייבר ואבטחת מידע, תשומת הלב בישראל אינה נופלת מתשומת הלב בסקר ה-IIA, וזאת נקודת זכות מקצועית.

כמו כן, מתשובות הנשאלים בארץ עולה כי בשלושה נושאי מטלות הביקורת בלבד חל שיעור קיטון בהיקף הביקורת: שירותים שאינם ביקורת (10%), ציות לרגולציה והוראות (8%) ושרשרת אספקה (4%).

לצורך השוואה, בסקר ה-IIA השיבו הנשאלים כי חל קיטון (בשיעור כזה או אחר) בכל נושאי מטלות הביקורת. שיעור הקיטון בנושאי המטלות ביקורת נע בין 31%-6%, כלומר בשיעורים גבוהים באופן ניכר מאלה שחוו המבקרים בארץ.

## סיכום

ככלל, ניתן לראות כי בעקבות משבר הקורונה חלו שינויים משמעותיים בעבודת הביקורת הפנימית בארגונים השונים: שינויים בהיקף כוח האדם, שינויים בתוכנית העבודה השנתית, שינויים בתקציב הביקורת, ושינויים במוקד הביקורת והיקפה בנושאי המטלות השונים.

באשר לשינויים בעבודת הביקורת: בהשוואה בין התשובות שעלו בסקר בארץ לבין התשובות בסקר ה-IIA, נראה כי המגמה אינה חד-משמעית, וכי ישנם תחומים שבהם חלו שינויים בשיעורים גבוהים יותר בסקר ה-IIA (כדוגמת גידול בהיקף עדכון תוכנית העבודה ועדכון הערכת הסיכונים), ואילו בתחומים אחרים חלו בארץ שינויים בשיעורים גבוהים יותר (כדוגמת קיטון בתקציב השעות מצד אחד וגידול בנושאי המטלות מצד שני, בדגש על מטלות מקצועיות שלמשבר הקורונה השפעה ישירה עליהן, כגון חשש ממעילות והונאות והמשכיות עסקית).

# תאגידים בנקאיים בצל הקורונה – תובנות על פעילות הביקורת הפנימית

בתחילת מאי 2020 התקיים שולחן עגול של מבקרים פנימיים בתאגידים הבנקאיים. הדיון עסק בפעילות הביקורת הפנימית בצל הקורונה.

## תובנות עיקריות שעלו מהשיח שהתקיים במסגרת השולחן העגול:

**ניתן להסתכל על התקופה כנחלקת לשני שלבים עיקריים:** שלב החירום המיידי - ממרץ ועד סוף אפריל; שלב של "שגרת קורונה" - החל ממאי ועד סוף השנה. אציין שלאור ההתפתחויות מאז תחילת מאי, ובראייה קדימה של תכנון פעילות הביקורת החל ממאי, יש מקום לראות בתוך התקופה של "שגרת הקורונה" שתי חלופות שאליהן יש להיערך (כפי שגם הוגדרו על ידי בנק ישראל): האחת - חיים בצל הנגיף, האחרת - גל תחלואה שני (שאנו כבר מצויים בתוכו).

**פעילות הביקורת בשלב החירום המיידי:** הגישה הרווחת הייתה הקפאה של הביקורות השוטפות והממשקים עם המבוקרים. ביצוע בדיקות וניטורים ממוקדים רק לסיכונים המתפתחים.

**עקרונות לתכנון פעילות הביקורת להמשך השנה:**

**התאמה של תוכנית העבודה ויצירת תוכנית עבודה מעודכנת. יש לשים לב ל:**

- נתינת דגש לסיכונים המתפתחים.
- נתינת דגש לשינויים שבוצעו ויבוצעו כפועל יוצא של הנחיות רגולטוריות לתקופת הקורונה.
- מוצרים ושינויים בתהליכים שבוצעו ויבוצעו כפועל יוצא של תקופת הקורונה.
- תשומות מופחתות של הביקורת כפועל יוצא של הצמצום באיוש וההאטה בפעילות.

**דפוסי פעולה:**

- פתיחה הדרגתית של ממשקים עם המבוקרים, התחשבות בעומסים יחד עם העברת מסר שהביקורת חוזרת לפעילות.
- דגש על פעילויות שלא דורשות ממשקים עם מבוקרים או דורשות ממשקים מצומצמים יחסית.
- השלמת ביקורות שנמצאות בתהליך.
- מתן תשומת לב לפעילויות של הטמעת מתודולוגיות, תהליכי עבודה ומערכות המשמשות את הביקורת הפנימית.

**תהליכי עבודה ותוצרים:**

- ביקורת קצרות וממוקדות יותר.
- חלוקה של ביקורות מורכבות ליחידת עבודה קצרות עם תוצרים מוגדרים (כחלק מיישום גישת אג"יל וכהתאמה למצב).
- דגש על תחקורי נתונים.

**דגשים נוספים:**

- גישה מרחוק - ההתייחסות המיידית היא להיבטי אבטחת מידע ותכנון קיבולת. אולם בהנחה שעבודה מרחוק תהפוך לדפוס פעולה מתמשך ולא אד-הוק לתקופת החירום הראשונית, נדרש לבחון יישום היבטים הקשורים לניהול המשאב האנושי והתפוקות (מתודות ניהול, שגרות, כלים תומכים).
- תהליכי הפקת לקחים של תוכנית החירום בראייה עתידית של שיפור ההיערכות לתרחישי חירום - הגישה הרווחת היא השתלבות של הביקורת בתהליך הארגוני כביקורת מלווה/ליווי תהליך על יד הביקורת הפנימית.
- סיכוני מוניטין/תדמית - עלייה ברגישות הציבורית כפועל יוצא מהמצב.
- אשראי בערבות המדינה - התאמת נהלים וקביעת קריטריונים, עמידה בכללים שנקבעו, סיכוני CONDUCT.

ניהלה את הדיון במסגרת השולחן העגול ורשמה את התובנות: יעל רונן, רו"ח, סגנית נשיא לשכת המבקרים הפנימיים IIA ישראל, מבקרת פנימית ראשית - הבנק הבינלאומי.



יש לך תובנה, ידע, רעיון בתחום הביקורת הפנימית, ניהול סיכונים או בקרה שאתה רוצה לשתף או לקדם? את/ה חיית במה או רק רוצה לשתף ?

**זו ההזדמנות שלך!**

**TALKAUDIT**

כנס בסגנון TED הנותן לך מקום והזדמנות להציג ולשתף את הרעיון שלך עם מאות משתתפים מהתחום.

**משך ההצגה העומד לרשותך הינו עד 15 דקות!**
זה אומר שאתה צריך להיות ממוקד, יעיל, בקיצור מקצוען.

איך מגיעים? מתחילים בלשלוח פרטים על הנושא שאתם מעוניינים להציג. לאחר מכן יערך אודישן ומי שיעבור יוזמן להציג ב- TalkAudit.

מי שיכנס לנבחרת המציגים יזכה בליווי מקצועי להכנת ההצגה.

לפרטים נוספים ולצעד הראשון במסע מדהים יש לשלוח מייל לגיל בר gilber@elal.co.il או לשלוח ווצאפ ל- 0542466718

# קורונה. בדיקה מרחוק – בדיקה מקרוב

**מאת:** מרגלית שפרבר | רו"ח, MBA, CIA, מבקרת פנימית ראשית, תנובה

**בעקבות הקורונה בוטלה נסיעה למטרת ביקורת בחברת בת במזרח אירופה. חילוקי דעות מתמשכים בנושא השקעות והצטיידות במכונות חדשות מעיבים על היחסים בין המטה להנהלת חברת הבת. כנראה שביטול הביקורים לא עורר בחברת הבת צער גדול...**

**במבט ראשון נראה שביטול הנסיעה לבחינת רכש המכונות, הוא תקלה רצינית שתמנע מאיתנו לדעת מה קורה בחברת הבת המרוחקת. האם זה באמת כך?**

הסיטואציה מזמינה אותנו להתבונן מחדש ולחשוב באיזו מידה הקונספט של 'שבוע ביקורת ביחידה בחו"ל' באמת מביא ערך? האם יכול להיות שיש דרכים נוספות לבדוק את נושא רכש המכונות בחברת הבת?

על מנת להתרענן ולקבל זווית חדשה, פתחתי גיליונות קודמים של המגזין שלנו. מצאתי בהם שפע של רעיונות נפלאים, ידע וניסיון מקצועי מארגונים שונים שאפשר לגייס לטובת פתרונות יצירתיים של הסיטואציה. במאמר זה אציע חמישה רעיונות שונים, כיצד להתמודד עם הסיטואציה.





## 1 מומחה מקומי בתחום המקצועי

במאמר נפלא של דוד אגרנט בגיליון מס' 9 ממרץ 2019, "המסלול המהיר להבנת התרבויות השונות", הוא מפרט חסמים תרבותיים שעלולים להשפיע על עבודת הביקורת. לדוגמה: ברוסיה מעורבות הגורמים הזוטרים בקבלת החלטות נמוכה ויש ציפייה לצייתנות ללא דופי. לאור זאת יש לקבל בעירבון מוגבל מידע הנמסר בראיונות ולשים דגש על בדיקות מבססות. ככל הנראה, גם במדינות נוספות במזרח אירופה בעלות עבר קומוניסטי יש לצפות לחסמים תרבותיים דומים. דוד ממליץ:

**"אם משאבי הביקורת מאפשרים זאת, מומלץ לשקול להיעזר בנותן שירותים מקומי ששולט בשפה ובעל הבנה עמוקה של היבטים מקצועיים בתהליכים עסקיים יחודיים לאותה מדינה".**

בסיטואציה שלנו, הישענות על מהנדס מכונות מקומי או מומחה מקומי לרכש ציוד מכני משדרגת את איכות הביקורת! ולעניין המשאבים: דווקא משום שהיום כולנו התכווצנו, זו הזדמנות פז למצוא מומחים מקומיים תותחים שבימים כתיקונם עמוסים ויקרים, ולתכנן מחדש את התקציב.

> הנעת ביקורת באמצעות שיחת וידאו עשויה להיות אירוע מתוח יותר, כדאי לחשוב מראש על ICE BREAKERS שיתאימו לסיטואציה – שיתוף במשהו אישי או מצחיק ואפילו גיחה של אחד הילדים בסביבה עשויה להועיל...

## 2 ביקורת מרחוק באמצעות תקשורת וידאו (SKYPE ,ZOOM ,TEAMS)

בסיטואציית הקורונה שאליה נקלענו, ייתכן מצב שבו האתרים נסגרים למבקרים מן החוץ כמדיניות, או שישנה הנחיה גורפת שלא לקיים פגישות פרונטליות. בנוגע למקרה שתיארתי בפתיח, עוד לא צברנו מספיק ניסיון בניהול ביקורת באמצעות תקשורת וידאו, והייתי חושבת פעמיים אם להיכנס לביקורת כזו בנושא טעון ארגונית, במרחק רב מהאנשים ומהמכונות. אם החלטתם שכן - כמה טיפים לביצוע ביקורת בפגישות ZOOM:

1. Ice Breakers - הנעת ביקורת באמצעות שיחת וידאו עשויה להיות אירוע מתוח יותר מהרגיל בשל השפעת המדיה והריחוק. כבר אי אפשר לשבור את הקרח באמצעות הכנת קפה ביחד במטבחון. כדאי לחשוב מראש על Ice Breakers שיתאימו לסיטואציה - שיתוף במשהו אישי או מצחיק ואפילו גיחה של אחד הילדים בסביבה עשויה להועיל...
2. הדגמת ניתוח נתונים ב-LIVE - באחת משיחות ההנעה שקיימתי לאחרונה, תיאר לי השותף לשיחה תופעה מסוימת. שאלתי אם יוכל להיכנס למערכת המידע וננתח את הנתונים יחד ב-LIVE. בשונה מפגישה פרונטלית, הרגשתי שותפה מכיוון שראיתי את התוצאות מקרוב על המסך שמולי.

מכיוון שביקשתי להקליט את הפגישה, הקלטה בהסכמה, יכולתי לשחזר מאוחר יותר את אופן הניתוח ואת התוצאות של כל שלב, ולבחון זאת מחדש תחת הנחות שונות.

מתברר שלפגישות בזום יש גם יתרונות ואנחנו נמשיך לגלות אותם בתקופה הקרובה...

## 3 ביקורת מרחוק – סימולציה על כדאיות השקעות

במאמר המרתק של אנה רוזנברג שפירו בגיליון מס׳ 10 מספטמבר 2019, ״שימוש בכלים טכנולוגיים וחדשניים בביקורת פנימית״, מדגימה המחברת כיצד מבצעים ביקורת באמצעות בניית סימולציה המדמה את החישוב ומריצים אותה על האוכלוסיה כולה (המאמר כולל גם התייחסות להסתמכות על נתוני המבוקר. מומלץ לעיין).

**ניתן לבצע ביקורת השקעות, הצטיידות ומכונות באמצעות סימולציה.**

בנייה של מודל כזה והרצת נתוני המכר והעלויות בפועל ביחס לכלל אוכלוסיית המכונות הנרכשות היא בעלת ערך רב, בין אם בארגון קיימת מתודולוגיה לבחינה (מראש) של כדאיות ההשקעות באמצעות מודל מוסכם וניתוחי רגישות של התחזיות ובין אם לאו.

בסיטואציה שלנו, גם אם לא נוסעים לחברת הבת ניתן להשתמש בנתונים שנשלפו על ידי המבוקרים להרצת סימולציה מדמה. אם יש מודל ארגוני, הפערים שיימצאו משמשים אינדיקטורים לסוגיות הטעונות הבהרה ולתיקונים הנדרשים במודל הקיים. אם לא קיים בארגון מודל, הסימולציה יכולה לשמש דוגמה לתועלת שצומחת מקיומו של מודל כזה.

## 4 קרוב ורחוק - מיקוד במשילות ויחסי מטה שטח

כחלופה נוספת לבדיקה שתוכננה, מוצע לבדוק את תהליכי העבודה של המטה מול חברת הבת בהתייחס לשני רבדים:

1. שגרות הבקרה הכלליות: אילו גורמים אחראים לבקרה שוטפת מטעם המטה? מה הסמכויות שלהם? כיצד הם מיישמים בפועל את הבקרה? מה מקומן של חבילות דיווח (נתונים תקופתיים שחברות בנות מעבירות לחברת האם)? מה החבילות כוללות ומה אינן כוללות? מי עורך בדיקות על הנתונים המסופקים בחבילות אלה, שואל שאלות ומבקש תגובות?
2. משילות וקבלת החלטות בנושא השקעות והצטיידות: מכיוון שבמקרה שתיארתי בפתיח, יש לנו מידע מוקדם על מערכת יחסים מתוחה על רקע ההשקעות, אפשר לבחור כדוגמה את המתואר בסעיף א׳, מספר מקרים ספציפיים של הצטיידות, ולנתח את תהליכי העבודה בהקשר של יחסי מטה ושטח. האם קבלת ההחלטות נערכת מתוך ראייה רחבה?

**לעיתים קרובות בבדיקה זו מתברר שישנם ממשקים ותחומים חשובים שמערך הבקרה וחבילת הדיווח אינם מכסים.**

ניתוח כזה של שגרות העבודה והמשילות יכול להביא ערך ותובנות ברמת חברות הבנות כולן, מכיוון שהתיקון נערך ברמת המטה.

## 5 הערכה השוואתית של בשלות החברות הבנות

במאמר החשוב של דני פרידמן, דרור בר משה ודוד ניסים בגיליון מס׳ 11 ממרץ 2020, ״כפרי בשל - מודל הבשלות בשירות הביקורת הפנימית״, הם מתארים את יתרונות השימוש במודל בשלות מבוסס COSO ככלי להערכת רמת הממשל התאגידי, ניהול הסיכונים ומערך הבקרות, המאפשר הערכה אובייקטיבית והשוואה בין תהליכים ובין יחידות.

אחת הדרכים ליישם את המודל מרחוק היא כשאלון להערכה עצמית (Control Self-Assessment) הנשלח לגורמים רלוונטיים, והם מתבקשים להעריך את רמת הבשלות ביחס לעקרונות הבקרה הפנימית. אפשר להתאים את העקרונות המפורטים במאמר לנושא ההצטיידות במכונות. דוגמה לעקרון בקרה פנימית שהותאם: ״הארגון בוחר ומפתח פעילויות בקרה על רכש מכונות חדשות והטמעתן כדי לתמוך ביעדי ההצטיידות שהוגדרו״. הוא ידורג על ידי המשיבים מ-1 (נמוך) ועד 5.

הערכה השוואתית בדרך זו מתאימה כשיש מספר חברות בנות והיא תלויה במהימנות התשובות לשאלון ההערכה העצמית.

בסיטואציה שלנו - בדיקה רוחבית של מרכיבי הבקרה הפנימית במספר חברות בנות בחו״ל, באמצעות סטנדרטים אחידים ובירי השוואה, מאפשרת התבוננות על חברות הבנות מזווית חדשה.

## סיכום

בשעת משבר אנחנו נדרשים להמציא את עצמנו מחדש. לא צריך ללכת רחוק! כתב העת שלנו מספק שפע רעיונות מגוונים איך להתמודד עם אתגרים, גם עם אתגרי הקורונה. זו הזדמנות לומר תודה גדולה לעורכת הנפלאה, לכותבים החרוצים, לצוות המערכת שנרתם למשימה, לסטודיו ולמעצבת ולכל מי ששולחים ידם במלאכה החשובה!



החל מגיליון זה, נבחר בכל שנה בגיליון ראש השנה, את המאמרים המצטיינים ביותר שהוגשו למערכת כתב העת בשנה החולפת.

# המאמרים המצטיינים לשנת 2019

**אני לא רובוט**
גלי גנה ומוריה צבעוני
ספטמבר 2019

**בבסיסו של עניין**
ארטור יעקובוב
ספטמבר 2019

**המסלול המהיר להבנת התרבויות השונות**
דוד אגרנט
מרץ 2019

**הקריטריונים על בסיס מאמרים נבחרים על ידי המערכת כמאמרים מצטיינים הינם:**

- איכות יוצאת דופן
- הצגת רעיונות ברורה
- רלוונטיות לשיפור המקצוע
- ישימות (פרקטיות)
- חדשנות

ברכות לזוכים, תוכלו לעיין במאמרים באתר הנשכה

# הערכת סיכונים בעולם שלאחר מגפה עולמית

**הביקורת הפנימית חייבת לכייל מחדש את מערך ניהול הסיכונים שלה בתגובה לסביבת סיכונים שונה לחלוטין**

**מאת:** ריק רייט* - **מאמר מתורגם**

ככל שמגפת נגיף הקורונה משנה את העולם, כך נאלצים מבקרים פנימיים להתמודד עם אותו עולם בדרכים שונות. אם לפני ההתפרצות עבדו המבקרים הפנימיים בהתאם לאותם כללי התנהגות ואותם תקנים והשתמשו בכלים דומים, כיום יש למבקרים עוד דבר במשותף: הצורך להתאים את עצמם לתנאי סיכון המשתנים בתכיפות.

הקורונה שינתה מן היסוד את פרופילי הסיכון של ארגונים רבים.

**הביקורת הפנימית צריכה להתאים את עבודתה לשגרה החדשה, ובו-בזמן גם לכייל את תוכנית הביקורת שלה מנקודת מבט על סיכון שונה לחלוטין.**

> הקורונה מנחיתה פגיעה בקנה מידה גלובלי ובעוצמה חזקה יותר מכל אירוע אחר שחוו רוב המבקרים אי פעם.

## תוכנית העבודה בסכנה

בואו נבדוק את השתלשלות האירועים. לקראת סוף שנת 2019 מבקרים פנימיים רבים כבר התחילו את תהליכי תכנון הביקורות והערכות סיכונים. עד החודשים הראשונים של שנת 2020, רוב מחלקות הביקורת הפנימית ברחבי העולם כבר בנו לפחות את השלד של תוכניות העבודה השנתית שלהם וחלקם כבר הגישו תוכניות פורמליות לוועדות הביקורת ולחברי ההנהלה. בחודשים הראשונים של שנת 2020, חלק מהמבקרים כבר התחילו לבצע את מטלות הביקורת.

הכול השתנה בחודש מרץ, כאשר נגיף הקורונה התחיל להתפשט ברחבי העולם ועסקים חוו את ההשלכות הראשוניות של צעדי הריחוק החברתי. מבחינה תפעולית, ארגונים רבים שינו את אופן התנהלותם העסקית. מבחינת ציות, במהלך ההתפרצות תעשיות שלמות קיבלו הקלות בדרישות הרגולטוריות ודרישות אחרות הושהו.

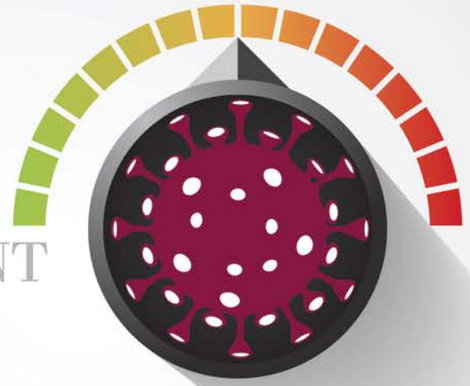
ככל שצעדים אלה התגברו, **מבקרים רבים שינו באופן דרסטי את תוכנית העבודה שלהם. ארגונים נתקלו בשיבושים רבים כל כך עד שכמעט היה בלתי אפשרי לבצע חלק ממטלות הביקורת או שפשוט לא היה טעם לבצען.**

במסגרת סקר בזק שערך ה-IIA בחודש אפריל 2020 (ראו גם סקר שבוצע בישראל בעמוד 8 לגיליון), רוב המשיבים דיווחו שעצרו או צמצמו את ההיקף של חלק ממטלות הביקורת, וכמעט מחציתם ביטלו כליל חלק מהמטלות.

ארבעה מתוך עשרה משיבים דיווחו שנאלצו להטיל על צוותי הביקורת משימות שאינן קשורות לביקורת. משיבים אחרים דיווחו על הוצאת צוותי ביקורת לחל"ת, על צמצומי תקציבים שהובילו לעצירת עבודת הביקורת, ועל צוותי ביקורת שמבצעים רק עבודות אדמיניסטרטיביות.








## תוכנית עבודת הביקורת הפנימית לאחר מגפה עולמית

תוכנית העבודה לפני המגפה הייתה מבוססת על פרדיגמת הסיכון הישנה.

**בעולם שלאחר המגפה, על מבקרים פנימיים ראשיים לחשוב אחרת לגבי הסיכונים העומדים בפני ארגוניהם ולבחון איך להקצות מחדש את משאבי הביקורת.**

להלן מספר שאלות שכדאי שמבקרים פנימיים ראשיים ישאלו במסגרת חשיבה מחדש על תוכניות הביקורת שלהם.

**איך נראה המצב הנורמלי החדש בארגון?**

אפילו ארגונים שנפגעו בצורה מינימלית מהקורונה עוברים שינויים מערכתיים בסביבת הסיכון שלהם (ראו "שאלות למבקרים פנימיים ראשיים" בסוף מאמר זה). נזקים כבדים עלולים להיגרם למוסדות ולמערכות שעליהם נשענים ארגונים רבים, ורגולטורים, מוסדות פיננסיים ושרשראות אספקה עלולים לחוות שיבושים במשך זמן רב. לא מן הנמנע שחלקם לא ישרדו את המשבר.

**האם תהליך הערכת הסיכונים שלי מספיק גמיש?**

השאלה הזו קריטית כאשר מבקרים פנימיים ראשיים מתחילים לקבוע סדרי עדיפויות בעניין הקצאה מחדש של משאבים כדי לטפל ברמות סיכון גבוהות יותר, הן בתחומי סיכון המסורתיים והן בתחומי סיכון חדשים ולא ידועים. הערכות סיכונים חייבות להיות גמישות ומסוגלות לנתח מצבים תוך כדי תנועה, מפני שהדינמיקה של הסיכונים עשויה להשתנות בכל עת בטווח הקרוב. על מבקרים פנימיים ראשיים לבחון תהליכי הערכות סיכונים מסורתיים ולייעל אותם.

**האם לצוות שלי עדיין יש את המיומנויות הנדרשות כדי לבצע הערכות סיכונים ותוכניות ביקורת?**

סביר להניח שבעולם שלאחר המגפה העולמית פרופילי הסיכון ישתנו, ובחלק מהארגונים - באופן דרמטי. מבקרים פנימיים ראשיים צריכים להעריך את כישורי הצוותים שלהם ואת היכולת של מחלקת הביקורת הפנימית לזהות סיכונים ולבצע משימות ביקורת שמתמקדות בסוגים חדשים של סיכונים. עליהם להתייחס לשאלות כגון:

איך השתנה הצוות במחלקת הביקורת הפנימית?

האם רמת המקצועיות בקרב העובדים השתנתה והאם חלו שינויים בכישורים?

האם נדרשים כישורים חדשים כתוצאה מהשינויים בפרופיל הסיכון של הארגון?

**האם לצוות שלי עדיין יש דפוס חשיבה אובייקטיבי?**

זמנים חסרי תקדים דורשים אמצעים חסרי תקדים, ובמהלך מצב החירום מבקרים פנימיים רבים נקראו לבצע מטלות שמעולם לא העלו על דעתם שיבצעו. מבקרים פנימיים ראשיים צריכים לבחון את האובייקטיביות של צוותיהם, ולבדוק אם מבקרים עסקו בפעילויות שלא קשורות לביקורת פנימית בתוך העסק, או שביצעו פעילויות שבמצב נורמלי היו נחשבות כמנוגדות לסטנדרטים המקצועיים.

## עולם חדש של סיכונים

העולם שונה עכשיו והסיכונים שונים. על מבקרים פנימיים לכייל את נקודת המבט שלהם על הסיכונים הטבועים העומדים בפני ארגוניהם עכשיו, כשתקופת ההתאוששות מתחילה.

מעבר חד מתקופה לתקופה אינו תופעה חדשה, אך הקורונה מנחיתה פגיעה בקנה מידה גלובלי ובעוצמה חזקה יותר מכל אירוע אחר שחוו רוב המבקרים אי פעם. יכולת התגובה של הביקורת הפנימית היא חיונית לא רק למידת התאוששות הארגונים שמשרתת הביקורת, אלא גם לאופן שבו הביקורת הפנימית מתאימה את עצמה מחדש לצרכים של בעלי העניין שלה.

> כיום יש למבקרים עוד דבר במשותף: הצורך להתאים את עצמם לתנאי סיכון המשתנים בתכיפות.

## שאלות למבקרים פנימיים ראשיים

על מנת להעריך את המצב בארגונם במהלך משבר הקורונה, כדאי שמבקרים פנימיים ראשיים ישאלו את השאלות הבאות:

- איך נראית מצבת כוח האדם בארגון כעת? האם בוצעו צמצומים או ארגון מחדש?
- האם בעלי העניין העיקריים השתנו? האם צפויים להיות לנו מבוקרים חדשים?
- האם צמצומים בכוח האדם או ארגון מחדש השפיעו על אופן הביצוע של בקרות פנימיות? האם יש צורך לבחון בעיות חדשות של הפרדת תפקידים או של בקרות שכבר אין מישהו שאחראי עליהן?
- אילו תהליכים השתנו באופן זמני או קבוע?
- אילו מערכות עברו התאמות זמניות או שונו באופן קבוע? האם במהלך ביצוע שינוים אלה בוצעו בקרות IT ראויות? אם לא, מהן ההשלכות לכך?
- אילו בקרות שונו כדי להתאימן למצבים עסקיים או לסיכונים יוצאי דופן?
- האם חלו שינויים בתפקידי מפתח, כגון אובדן של מומחיות בתחום ספציפי או אובדן של מנהלים המובילים תחומים אסטרטגיים?
- האם הארגון שינה את המיקוד האסטרטגי שלו בטווח הקצר או הארוך?
- האם השתנו מבני העלויות?
- האם התרחשו שינויים יסודיים במבני החוב וההון של הארגון? האם חלות אמות מידה פיננסיות חדשות או שונות?
- אילו אתגרים משפטיים או אתגרי ציות עומדים בפני הארגון (חשיפות לתביעות או שינויים בתשתית הציות)?
- האם צמחו הזדמנויות עסקיות חדשות? אם כן, האם זוהו הסיכונים הנלווים?
- האם השתנו יסודות הפעילות של היחידות עסקיות או האסטרטגיה שלהן?
- איך השתנתה הדינמיקה של ההמשכיות העסקית (שינויים בתשתיות מרכזיות, שינויים בלקוחות עיקריים)?
- איך השתנתה הדינמיקה של ניהול סיכונים עסקיים (סיכונים מרכזיים, מדדי סיכונים מרכזיים, תוכניות תגובה, תיאבון סיכון)?
- איך השתנתה הדינמיקה של החוק האמריקאי סרבנס-אוקסלי משנת 2002, לרבות שינויים מול מבקרים חיצוניים, הדינמיקה הרגולטורית, ושינויים בגורמים האחראים על בקרות?

> "הערכות סיכונים חייבות להיות גמישות ומסוגלות לנתח מצבים תוך כדי תנועה"

*"This article was reprinted with permission from the May 27, 2020 issue of Internal Auditor magazine, published by The Institute of Internal Auditors, Inc., and has been translated from English to Hebrew".

# חדשנות בעת משבר

## אתגרי המגפה הם הזדמנות ייחודית למבקרים הפנימיים להמציא מחדש את תפקידם בשרשרת הערך בארגון

**מאת:** אלנה דובינדה

אודיי גולוואדי* - **מאמר מתורגם**

הכלכלה העולמית נפגעה בצורה קשה ממגפת הקורונה שהתפשטה במהירות מפתיעה בעולם. המומחים מסכימים שלא מדובר באירוע חולף, ושעסקים ימשיכו לסבול מההשפעות השליליות של המגפה עוד הרבה זמן. הצורך החיוני "לשטח את העקומה" כדי להכיל את התפשטות הנגיף גרם לשיבושים משמעותיים, המלווים בירידות חדות בהיקפי העסקים ובהכנסות. ירידות נוספות צפויות לכל אורך שנת 2020 וגם ב-2021. כבר עכשיו ארגונים חווים אובדן לקוחות, משברי נזילות, שיבושים בשרשרת האספקה, צמצומים ופיטורים של כוח אדם.

בתגובה לאתגרים אלה, ארגונים בכל רחבי העולם נקטו יוזמות וביצעו צעדים מהירים. לדוגמה, ארגונים רבים הקימו צוותים ייעודיים לניהול המשבר תוך התמקדות בטיפול בצרכים המיידיים של לקוחות ועובדים. כמו כן, צוותי מנהלים בכירים מבצעים מבחני לחץ על תרחישים אסטרטגיים, פיננסיים ותפעוליים, ויש ארגונים שכבר התחילו להיערך לחידוש הפעילות העסקית לאחר המשבר. בהינתן הירידות הצפויות בתזרימי ההכנסות העיקריים, סביר להניח שמנהלים יתמקדו בצעדים ספציפיים במטרה להקטין את אובדן ההכנסות. במקביל, מנהלים ינסו לשפר רווחיות על ידי שמירה על מבנה עלויות תפעוליות רזה ככל האפשר, הרחבת היכולות הדיגיטליות, הקצאת משאבים באופן משתנה והגברת החוסן הארגוני.

סביר להניח שצמצומי כוח האדם (בין פיטורין ובין חל"ת) יפגעו בתהליכים עסקיים באופן מהותי ויחלישו בצורה ניכרת מנגנונים של בקרות פנימיות. אין ספק שמצב שבו כוח אדם מצומצם עובד מהבית במשך תקופה ארוכה ומקיים קשר פרונטלי מינימלי יגרום לארגונים להיות פגיעים. בנסיבות אלו, ארגונים צפויים לראות גידול חד ומתמשך במעילות ובהונאות, בפשעים פיננסיים ובמתקפות סייבר, ורמאים רבים ינסו לנצל את האוכלוסייה הפגיעה והלחוצה מאוד עקב המשבר.

**אתגרים אלה מחייבים תגובה חדשנית מצד הביקורת הפנימית ומהווים הזדמנות ייחודית עבור מבקרים פנימיים להמציא מחדש את תפקידם בשרשרת הערך בארגון.**

שאלנו מספר מבקרים פנימיים ראשיים (CAEs) במוסדות פיננסיים לגבי דרכי ההתנהלות במחלקותיהם מאז פרוץ המשבר. מספר גישות חדשניות, לרבות כאלה שמציעים מבקרים אלה, יכולות להוסיף ערך עבור הארגון ולעזור ללקוחות להבין את החשיבות של הביקורת הפנימית במהלך הימים הקשים האלה.





## יישום פתרונות ניהול משבר

**ועדות ביקורת ובעלי עניין מרכזיים סומכים על כך שהביקורת הפנימית תספק שירותי הבטחה רחבים וממוקדים ושירותי ייעוץ כדי להתגבר על האתגרים בעתיד הקרוב.**

מבקרים פנימיים ראשיים צריכים לעבוד בשיתוף פעולה עם ועדות הביקורת ועם חברי ההנהלה הבכירה בתכנון סדרה של פעולות אפשריות להפחתת סיכונים באופן מחושב, אבל גם גמיש בהתאם להתפתחויות. מבקרים פנימיים ראשיים שעימם שוחחנו ציינו שתפקידם כיום כולל השתתפות ישירה בוועדות ניהול משבר הקורונה ובצוותי ניהול משבר בארגוניהם. הם סייעו בגיבוש התגובות הארגוניות כדי לוודא שההודעות בנושא המשבר אכן נמסרות ללקוחות, לבעלי העניין ולציבור הרחב בצורה מתאימה ושקופה.

גורם מרכזי בקבלת החלטות אצל בעלי העניין הוא קצב החרפת הסיכונים ואיכות הניתוח של השפעותיהם. לכן מבקרים בעלי ניסיון בזיהוי סיכונים ובביצוע הערכות הוליסטיות יכולים לבצע הערכות טובות יותר של ההשלכות הטווח הקצר והטווח הארוך של החלטות בעת משבר.

בנוסף, מבקרים פנימיים ראשיים ציינו שהם הוסיפו לתוכנית העבודה בחינה של נושאים הקשורים בקורונה, לרבות לגבי בחינת פעילויות המבוצעות מרחוק ובחינת שינויים בתהליכים עסקיים. חלק מהבדיקות האלה בוצעו במהירות רבה - לפעמים תוך כמה ימים - על מנת לדווח ולהציף סוגיות מבעוד מועד.

## תמיכה בעובדים, בבעלי עניין ובלקוחות

המשבר מציף הזדמנויות רבות עבור מבקרים פנימיים לפעול כיועצים מהימנים ולסייע לארגון לשמור על פונקציות הליבה, לתמוך בלקוחות, לנהל את הסיכונים העיקריים ולשמור על חוסן. אחד המבקרים הפנימיים הראשיים ציין כי המשימה הראשונה של מחלקת הביקורת הפנימית שלו הייתה להתמקד בשמירה על בטיחות ושלום עובדי המחלקה, וכי הם יישמו במהירות נוהלי עבודה מהבית, אפשרו הסדרי שעות עבודה גמישות על מנת לאפשר חינוך ביתי, ותמכו בעובדים השוהים בבידוד עצמי. במטרה לתעדף את צורכי הלקוחות, מחלקות ביקורת פנימית רבות צמצמו משימות הבטחה מסורתיות והקלו על לוחות הזמנים להשלמת תיקונים לסוגיות שעלו בביקורת הפנימית, במטרה לתת למרחב תמרון בתחומים עסקיים כדי לשרת את הלקוחות. מחלקות ביקורת פנימית אחרות עשו הרבה מעבר, והפגינו גמישות ומחויבות לבעלי העניין שלהן, ונתנו כתף בצורות שונות, כגון ביצוע בדיקות טרומיות של תהליכי סגירת הדוחות הכספיים הרבעוניים, מתן דחיפה למאמצי תיקוף ולמאמצי תיקון אחרים, וסיפקו פעולות ניטור משופרות. בעוד שעבודות ביקורת חשובות ומוגבלות בזמן המשיכו להתקדם, ההיקף של ביקורות אלה נבחן על מנת להתמקד בסיכונים העיקריים.

מחלקות מסוימות בארגונים מבצעות רמות פעילות חסרות תקדים ומתמודדות עם אתגרים מבחינת משאבים, כגון מחלקות מערכות המידע הנדרשות לעמוד בדרישות תשתית גבוהות, לרבות הגברת יכולות עבודה מרחוק ויכולות דיגיטליות, שירות לקוחות ותמיכה תפעולית. ככל שעולה מספר העובדים הנעדרים עקב מחלות ומצבי חירום - או כאלה העובדים תחת הסדרי עבודה גמישים - או כאלה המאבדים ניידות עקב המגבלות על נסיעה ותחבורה ציבורית - כך גובר המחסור במשאבים.

לאחר מגפה עולמית, ארגונים יהיו זקוקים לתמיכה בגיבוש מחדש של תוכניות עסקיות ושל תחזיות דרישה, הכנסות, עלויות ורווחיות, בהערכת סיכונים מרכזיים ובבחינה מחדש של הנחות יסוד. מתן שירותי מומחים באופן זמני לעסק, יחד עם אמצעי הגנה ראויים, יגביר את הערך של הביקורת הפנימית. פעילויות מסוג זה עלולות לגרום לניגודי עניינים בעתיד ויש לבחון אותן בזהירות ולנהל אותן בהתאם.

**ניתן להשיג חיסכון משמעותי במשאבים באמצעות שיתוף פעולה מוגבר עם קווי ההגנה הראשון והשני – מבקרים חיצוניים ורגולטורים.**

יש בידי הביקורת הפנימית היכולת לסייע במתן ביטוי מדויק של הערכות סיכונים מקיפות, תוך דאגה לפעולות מתואמות כדי למנוע כיסוי כפול.

## מציאת דרכי עבודה חדשות

הביקורת הפנימית תצטרך להבין כיצד המגפה משפיעה על גישות עבודה, על שיתופי פעולה ועל יחסי הגומלין עם בעלי העניין. "הקורונה הבליטה את היתרונות של עבודה מרחוק ושל הפרודוקטיביות שאפשר להשיג בסביבת עבודה מרחוק", אמר אחד מהמבקרים הפנימיים הראשיים. "בה בעת, היא גם מבליטה את היתרונות של אינטראקציה פנים אל פנים, לא משנה כמה איתנה הסביבה הווירטואלית".

חשיבה על האתגרים וההצלחות של עבודה מרחוק תעזור בגיבוש יוזמות אסטרטגיות לטווח הארוך או אפילו באופן קבוע. מודל העבודה החדש הזה יחייב שימוש מוגבר בכלי אוטומציה, ומגעים תכופים עם צוותי הביקורת, עם לקוחות ועם בעלי העניין. בתרחיש הזה, הביקורת הפנימית צריכה להעריך את השפעת העבודה מרחוק על משימות ביקורת של ישויות ויחידות עסקיות הנמצאות במקומות שונים ועם יכולת מוגבלת לנהל אינטראקציות פנים אל פנים, ראיונות, סיורים וכו'. סביר להניח שתהיה הישענות מוגברת על תשתיות IT מבוססות ענן בסביבת העבודה הדיגיטלית והמרוחקת הזו. כבר היום אנו רואים עלייה בשימוש בשיחות וידאו, כמו זום, וובאקס וסקייפ, אולם פלטפורמות אלו גם עלולות להיות חשופות לסיכוני אבטחה. אם נתונים ורשומות המיועדים לבדיקה אינם מסופרתים או זמינים באופן אלקטרוני, מבקרים פנימיים יצטרכו לבחון אם ניתן לבצע נוהלי אימות אלטרנטיביים מרחוק, בהתחשב בהיעדר הגישה למסמכים או לנתונים הפיזיים. עליהם גם לבדוק אם הדבר גורם לירידה בכיסוי או בהיקף הביקורת וכתוצאה מכך לירידה ברמת ההבטחה שהיא מספקת.

## מודלים גמישים של תכנון וביצוע ביקורות

משבר הקורונה נותן הזדמנות לחשיבה מחודשת לגבי תהליכי תכנון הביקורת הפנימית. הוכח כי המודל המסורתי של כיסוי על פני מספר שנים ושל מחזורי ביצוע ארוכים הוא נוקשה מדי כדי להגיב לסביבה בלתי יציבה. לכן בעלי העניין ידרשו גמישות לגבי ההיקף, הכיסוי ואופן הביצוע, וכן לגבי העיתוי ושיטות אסקלציה. יישום גישה גמישה במודל תכנון וביצוע הביקורת יסייע בשמירה על ההתמקדות בסוגיות המרכזיות, כאשר התנאים משתנים בכל עת ובביצוע מהיר של תעדוף מחדש של משימות. תהליכי גילוי גמישים יכולים לסייע בהתייחסות מהירה להתפתחויות ולסיכונים חדשים. מטלות ביקורת קצרות בגישה שיתופית יותר, יאפשרו הסקה מהירה יותר של תובנות ברות ביצוע ופעולות תיקון מהירות. אחד מהמבקרים הפנימיים הראשיים בארגון גלובלי ציין שהוא משתמש בגישת ביקורת גמישה לכל אורך מחזור החיים של מטלות הביקורת על מנת לספק את אותה רמה של הבטחה בפחות זמן. ה-CAE הוסיף כי "ההשפעה של שיבושים במצבת כוח האדם על התרבות ועל סביבת הציות היא סיכון מהותי חדש העומד בפני הארגון."

**מבקרים פנימיים יצטרכו להגדיר מחדש את המתודולוגיה ואת תהליכי העבודה שלהם כדי להפוך אותם לגמישים יותר ומותאמים לתרחישים בלתי צפויים.**

> מספר חידושים ושיפורים מבוססי-צורך לטווח הקצר, המיושמים על ידי מבקרים פנימיים כתוצאה ישירה של המשבר, עשויים להישאר על כנם ולהפוך ל"מצב הנורמלי החדש"

### מתפתח קונצנזוס לגבי תעדוף מספר תחומים ראשונים לטיפול על ידי הביקורת הפנימית בסביבה שלאחר המגפה, לרבות:

- חוסן עסקי ותכנון המשכיות, במיוחד בכל הקשור לשילוב לקחים שנלמדו.
- גילויים והתחייבויות לציבור הנוגעים למשבר הקורונה.
- שיקולי בטיחות ובריאות העובדים, הלקוחות ובעלי העניין.
- בקרות על פשעי סייבר ואבטחת סייבר.
- אבטחת מידע בתנאי עבודה מרחוק.
- גילוי ומניעת הונאות ופשיעה פיננסית.
- כיול מחדש של תוכניות ויעדים עסקיים.
- אספקת מוצרים ושירותים דיגיטליים.
- תכנון תרחישים ומבחני לחץ.
- תחזיות הון, תזרים מזומנים ונזילות.
- ביטול הדרגתי של ויתורים והנחות שניתנו במהלך משבר הקורונה.
- הקטנת סיכונים גיאוגרפיים, סיכוני ערוצי אספקה וסיכוני ריכוזיות ספקים.
- סיכונים משפטיים וחוזיים וסכסוכים מסחריים.
- תביעות משפטיות עקב ההשפעות הכלכליות של המגפה.
- אינטגרציה של חוסן עסקי, היערכות למגפה עולמית, ומדדי ייחוס בניהול משברים בתוכניות תגמול לבכירים.
- כיול מחדש של מדדי תגמול מבוסס ביצועי העובדים.





> מספר גישות חדשניות, יכולות להוסיף ערך עבור הארגון ולעזור ללקוחות להבין את החשיבות של הביקורת הפנימית במהלך הימים הקשים האלה

מבקר פנימי ראשי סיפר איך הוא משתמש בדוחות בזק כדי לספק תובנות מהירות יותר להנהלה בתגובה לציפיות ולתיאבון גדול יותר של בעלי העניין לגמישות. מבקר ראשי אחר מיישם פתרונות חדשניים של פעילויות ביקורת מתמשכת - הבוחנות ומנטרות תהליכים הקשורים לקורונה בנוגע לשלמות, נכונות ודייקנות. מבקרים פנימיים ראשיים אחרים ציינו שהם החלו ליישם תהליכי ניטור פעילויות עסקיות משופרים על מנת לספק משוב על סיכונים בזמן אמת.

שימוש נרחב בניתוח נתונים - תוך מינוף בינה מלאכותית, לימוד מכונה ואוטומציה רובוטית של תהליכים - יהיה המפתח לתמיכה בגישה הגמישה של הביקורת הפנימית. "מבקרים פנימיים חייבים לקבל גישה לנתונים של ארגוניהם כדי לתפקד ברמה הגבוהה ביותר, וחלק מתוכנית הביקורת צריך להתמקד בהבטחת השלמות של אותם נתונים", אמר מנהל לשעבר של הביקורת הפנימית והציות בחברת ייעוץ גלובלית. "ניטור תמידי של נתונים יכול להניע שיחות עם המנהלים וההנהלה הבכירה במידה ומתגלות חריגות, וכך לקדם דו-שיח ומערכות יחסים טובות יותר".

מבקר פנימי ראשי אחר ציין את הערך שבנקיטת גישה גמישה יותר ומגיבה יותר. "החיוניות של הביקורת הפנימית מעולם לא הייתה גדולה יותר, לכן פיתחנו תהליך המאפשר דיווחים בתדירות גבוהה יותר לגבי הסטטוסים של משימות הביקורת וכדי להציף מחסומים פוטנציאליים לצוות ההנהלה הבכירה. בנוסף, ביצענו בדיקות הבקרות בזמן אמת, ושמנו את הדגש על אזורים בחברה בעלי סיכון גבוה, על מנת לספק הבטחה במועד שהתהליכים פועלים כמתוכנן. בדיקות אלו לוקחות בחשבון סיכונים במגמת עלייה - למשל, הן לוקחות בחשבון שעבודה מהבית עלולה להשפיע על סביבת הבקרה".

הסביבה תיצור מגמות חדשות מבחינת היקפים עסקיים, הכנסות, עלויות ומדדי סיכונים פיננסיים ותפעוליים אחרים. כתוצאה מכך, נוהלי ניתוח הנשענים על השוואות מול נתונים היסטוריים, וכן ניתוחי מגמות מבוססי תקציב או נתוני שנה קודמת, עלולים להיות לא מהימנים. כמו כן כדאי לשקול קיום "בקרות מינימליות" המקובלות בסביבות בקרה הנמצאות תחת לחץ אדיר ובתהליכים עסקיים הנמצאים בתהליך פיתוח וניטור.

## מבט קדימה

מספר חידושים ושיפורים מבוססי-צורך לטווח הקצר, המיושמים על ידי מבקרים פנימיים כתוצאה ישירה של המשבר, עשויים להישאר על כנם ולהפוך ל"מצב הנורמלי החדש". הסדרים גמישים לעבודה מרחוק עם פחות יחסי גומלין פנים אל פנים עשויים להמשיך, ומאגר הרבה יותר גדול של כישרונות יהיה זמין ללא המגבלה הגיאוגרפית של "נוכחות פיזית". צוותי הביקורת הפנימית יצטרכו לקחת בחשבון בתהליכי הערכות סיכונים את הפוטנציאל - נמוך ככל שיהיה - לאירועי "ברבור שחור" בעלי השפעה גדולה. באופן ספציפי, במספר מוסדות פיננסיים גלובליים יש התמקדות מוגברת בסיכונים פורצים או באיומים חיצוניים (כגון שינוי אקלים), שבדומה למגפת הקורונה מתפתחים כל הזמן והם קשים למדידה. כיום, יותר מתמיד, חשוב להתעדכן לגבי סיכונים אלה ולשקול איך לספק כיסוי ביקורת עבורם.

**מחלקות הביקורת הפנימית יכולות לסייע לארגונים לשפר את היכולות שלהם לחוש סיכונים ולזהות איתותים מהשוק בצורה טובה יותר, במיוחד תזוזות קריטיות בסביבה העסקית העלולות להשפיע על סיכונים.**

מבקרים פנימיים ראשיים אומרים שבעלי העניין ימשיכו לצפות למנהיגות חשיבתית וליוזמות מצד הביקורת הפנימית כדי לעזור לארגון להישאר בטוח אבל עדיין תחרותי. התמיכה והשותפות מצד הביקורת הפנימית, יחד עם בעלי תפקידים אחרים במהלך המשבר, עשויות להגביר את ההוקרה ההדדית על תפקידיהם של שני הצדדים ואת האמפתיה ביניהם, לצמצם מחלוקות ולהגביר את שיתוף הפעולה. כפי שאמר אחד המבקרים, "המצב יוצר הזדמנות ללחוץ, לפחות חלקית, על כפתור האיפוס של היבטים של התפקיד שכרגע אינם מתיישבים באופן מעשי עם הכינוי יועץ ושותף מהימן".

This article was reprinted with permission from the* June 15, 2020 issue of Internal Auditor magazine, published by The Institute of Internal Auditors, Inc., and has been translated from English to Hebrew.

# NEW NORMAL

## כיצד ליישם ולנהל עבודה מרחוק בצורה נכונה

**מאת:** שרון ויטקובסקי טביב | רו"ח, MA - שותפה BDO Israel,
ראש מגזר סיכונים (RAS) - סגנית נשיא ועורכת כתב העת

חני עמר | רו"ח משפטנית - שותפה BDO Israel, ראש קבוצת ביקורת פנימית

**איך אני יכול לנהל ולהבטיח דוחות איכותיים כשהעובדים בכלל לא מולי?**

זוהי שאלה שכולנו שואלים בחודשים האחרונים, כשנאלצנו להתנסות בעבודה מהבית, לצמצם את היקף הנוכחות הפיזית במשרדים, להתאים את עצמנו לסדרי עדיפויות חדשיםואף להוביל מהלכי עבודה וניהול חדשניים.

**האם אנחנו באמת בעלי הכישורים הנדרשים לצורך 'ניהול היברידי' (ניהול עובדים On-Site לצד עובדים מרחוק)?**

אם לא נסגל הרגלי עבודה מתאימים למודל החדש, המעבר של צוותים הרגילים לעבוד יחד, בצמידות, תוך הפריה, התייעצות והווי חברתי, לעבודה מרחוק, יכול לפגוע קשות בלכידות ולהביא לאי יעילות ואפילו לכשלים במישור המקצועי.

בכתובים הבאים נשתף בתובנות שהגענו אליהן בתקופה האחרונה הנוגעות ליישום ולניהול מיטבי של עבודה מרחוק, מוטיב מרכזי ב-New Normal שאליו כולנו מתרגלים בימים טרופים אלו.





## שינוי תפיסה -

## מדוד תפוקות ותוצרים במקום שעות עבודה

ניהול עובדים מרחוק או 'ניהול היברידי' הוכיח לנו במהירות כי השינוי הראשון שעלינו לעשות הוא לא בטכנולוגיות שבהן אנו משתמשים, לא בשעות העבודה, לא בצורת התקשורת בין הצוותים ועם המבוקרים, אלא לעשות שינוי תפיסתי, וזה השינוי הקשה ביותר.

הבנו שלא נוכל יותר למדוד ולהעריך את העובדים לפי מדדי תשומות (כגון היקף שעות העבודה או מספר השעות הנוספות), אלא לפי מדדי תפוקות. תפסנו כי כאשר העובדים לא לצידנו ומפריד בינינו הרבה יותר מקיר משותף, עלינו להבטיח יותר מתמיד שהם יוכלו לספק את התוצרים באיכות ובלוחות הזמנים הנדרשים, וכמובן תוך שמירה על כל הכללים המקצועיים.

חשוב לציין כי שינוי התפיסה תקף גם במצב עבודה רגיל, כלומר בעבודה פיזית משרדית, ולא רק במצב של עבודה מרחוק, אולם למדנו כי שינוי אופי העבודה אילץ אותנו לאמץ תפיסה זו באבחה אחת.

שינוי תפיסה זה מתיישב עם תורת ה-"Lean Auditing", המביאה אותנו לחשוב על התפוקות ועל הדיוק של התוצרים, ולא על התשומות שהשקענו.

שינוי התפיסה והמעבר לאופי עבודה שונה מחייב שינוי בשיטות הפיקוח והניטור, כך שגם הוא יהיה מבוסס על מדידת תפוקות, וכפועל יוצא מתחייב שינוי בשגרות התכנון של המשימות השונות בביקורת ושל המעקב אחר ביצוען.

**ככל שמדובר בעבודה מרחוק של חלק ניכר מהצוות או בחלק ניכר מהזמן, הבסיס לפיקוח וניטור אפקטיביים הוא תכנון מראש של משימות ותפוקות**

(ולא רק של נושאי הביקורת ולוחות הזמנים להשלמתם). לכן מומלץ להכין 'סידור עבודה צוותי' שיכלול משימות ברורות לכל אחד מהעובדים, תוך התייחסות לרכיבים הבאים:

(גם פה חשוב לציין כי שיטות ניהול ממוקדות תפוקות רלוונטיות גם במצב עבודה רגיל)

1. המשימות לביצוע ברמה יומית לפרק זמן של השבוע הקרוב, המשאבים הסבירים לכל משימה (שעות העבודה) וכן התפוקות או התוצרים של כל משימה, בדגש על כאלו הניתנים לכימות ולמדידה.
2. היקף התשומות הניהוליות שחברי הצוות יצטרכו על מנת להתקדם בעבודתם (שיחה עם המנהל, בדיקת תוצר ביניים לפני שיוכל להתקדם הלאה וכו').
3. זיהוי המשימות שתלויות במבוקר (צריך לקבל חומר ולשוחח עם המבוקר כדי שהמבקר יוכל להתקדם בעבודה על סמך החומר שקיים ברשותו).
4. ההבנה של 'הצמתים' הללו חשובה על מנת לזהות מראש היכן יכולה העבודה 'להיתקע'. כך לדוגמה: חשוב לתכנן בצורה נכונה את המשימות כך שלא ייווצר יום שבו כל חברי הצוות תלויים בפידבק מהמנהל בטרם יוכלו להתקדם בעבודה, כלומר להימנע מ"צווארי בקבוק", אלא לבזר את הצורך במשאבי הניהול על פני כל השבוע, ולהבטיח עבודה רציפה או יכולת התקדמות של חבר הצוות במשימות אחרות.

לצד תכנון נאות, ודאי שנדרשים גם ניטור ופיקוח הולמים. לכן חשוב לקבל מהעובדים משוב מהיר על העבודה שבוצעה: מה מתוך המשימות והתוצרים שתוכננו בוצעו בפועל, והאם זה קרה באיכות המצופה ובתשומות שהוגדרו לשם כך. על בסיס זאת יש לעדכן את תוכנית העבודה לימים הקרובים, ובמידת הצורך לנייד מטלות לעובדים אחרים.

## אימוץ שיטות ניהול חדשות ומתקדמות - בניית סידור עבודה



> "ניהול עובדים מרחוק או 'ניהול היברידי' הוכיח לנו כי השינוי שעלינו לעשות הוא שינוי תפיסתי, וזה השינוי הקשה ביותר. הבנו שלא נוכל יותר למדוד ולהעריך את העובדים לפי מדדי תשומות, אלא לפי מדדי תפוקות."

## שינוי שיטת תקשורת בין-אישית -

## זה שהעובד לא נמצא איתנו פיזית, לא אומר שלא יהיה 'סמול-טוק'

הימים הראשונים של ניהול מרחוק, ודאי של 'ניהול היברידי', הביאו את המנהלים לעומס מחשבות - איך מצליחים לשמור על קשר עם כולם בעולם וירטואלי? איך מגלים התעניינות דרך מסך ה-ZOOM, במיוחד כשלשיחה שותפים כל חברי הצוות? איך אני שומר על 'הטון הניהולי האישי' גם בתקופות שבהן לא פגשתי את העובדים שלי במשך שבועות רצופים?

במצבים כאלו, ומכיוון שכנראה עבודה מרחוק היא מגמה שתימשך גם בעתיד (בגלל משבר הקורונה או בגלל שינוי בהרגלי העבודה), עלינו כמנהלים לאמץ שיטות תקשורת ולכידות חדשניות.

**המנהלים והצוותים צריכים להיות מודעים יותר לצורך להישאר עמיתים טובים (חברותיים, אדיבים, משתפים בידע) כדי להבטיח שהצוות ירגיש בטוח ויוכל להיתרם ולתרום גם מרחוק,**

> עלינו כמנהלים לאמץ שיטות תקשורת ולכידות חדשניות

לפחות באותה המידה שזה בא לידי ביטוי בעבודה מקרוב.

שיטות אלו יכולות לכלול שיחות צוות בתחילת יום או בסופו, שבמסגרתן דנים במטלות שיש לכל אחד מהעובדים, שיתוף צוותי לגבי אתגרים וקושיות מקצועיות שעלו אצל עובדים והם מעוניינים לשתף ולהתייעץ, ושיחות הווי כלליות לגבי העבודה מול המבוקרים. ניתן גם לקיים שיחות שבועיות של 'הווי צוותי', דוגמת Happy Thursday או Happy Hour או 'הרצאת אורח שבועית' בשיחות וידאו.

חשוב לזכור שמשבר הקורונה האיץ את השימוש בכלים טכנולוגיים ידידותיים שהצוותים יכולים לעשות בהם שימוש (ZOOM, Face-Time, Skype, Teams ועוד רבים אחרים).

אין ספק שעבודה מהבית מטשטשת את הקווים שבין החיים המקצועיים לבין החיים האישיים ולמעשה כל ה-Work Life Balance מתערער. לא פעם חברי הצוות מרגישים לחץ נוסף בעבודה מרחוק בשל הרושם שהם מותירים בפני מי שחווה אותם עובד מרחוק (הנראות שלהם בווידאו), בשל סביבת העבודה הביתית שלהם, בשל הפרעות מצד ילדים או מצד בני משפחה שחולקים את אותה סביבת עבודה ועוד. שעות העבודה עוברות גם הן שיבוש (Disruption), ולא מעט מאיתנו מצאו עצמם מתלבטים לגבי מסגרת שעות העבודה שאנו מצפים לה מעובד.

כמנהלים עלינו להיות ערים למגבלות ולעודד את חברי הצוות לשתף אותנו בקשיים שהם חווים כדי שנוכל לסייע במציאת פתרונות, אך מנגד עלינו להציב גבולות משלנו, או לכל הפחות לערוך

## הגדרה מחדש של מסגרת העבודה -

## כבר לא 08:00 עד 17:00

תיאום ציפיות מלא באשר למסגרת שעות העבודה וזמינות הצוות.

לא משנה מה תהיה ההחלטה הניהולית לגבי שעות העבודה הנורמטיביות בעבודה מרחוק, שיכולות להיות פרטניות ביחס לכל אחד מחברי הצוות, חשוב לייצר מסגרת שעות חופפת בין המנהלים לבין הצוות, כך שתישמר מסגרת יום עבודה שבו כולם יתבקשו להיות זמינים וחברי הצוות יוכלו לפנות אל המנהלים והקולגות בשאלות והתייעצות, כפי שקורה גם בעבודה מהמשרד.

גם אם בשל האילוצים האישיים של כל עובד ישנה שונות בשעות העבודה, בטח כאשר אין מסגרות חינוך או מסגרות פורמליות אחרות מסודרות, חשוב להבטיח שלכל הפחות תהיה מסגרת עבודה חופפת של מספר שעות עבודה בודדות ביום.





## סביבת העבודה ואבטחת המידע -

## לא לכולם יש חדר עבודה מדוגם בבית...

בעבודה מרחוק אין לנו, המנהלים, יכולת להבטיח סביבת עבודה ותנאים פיזיים הולמים עבור כל אחד מהעובדים שלנו. "אין לי תשתית אינטרנט טובה בבית", "אין לי היכן לעבוד, הילדים רצים לי מול העיניים", "אין לי מצלמת וידאו במחשב ולא ניתן להשיג בחנויות", "מסך המחשב הנייד שלי קטן מדי", הם רק חלק מהמשפטים ששמענו בימים הראשונים של הסגר שהוטל בעקבות נגיף הקורונה, ומצאנו את עצמנו מטפלים ב'בעיות ת"ש' שהעלו העובדים.

על רקע סיכוני סייבר ואבטחת מידע, חשוב מאוד להבטיח כי ברשות העובד מרחוק יהיו כל התנאים הסביבתיים והטכנולוגיים הנדרשים על מנת לקיים עבודה רציפה, איכותית ומאובטחת, כמעט כמו במשרדים. לכן יש לוודא עם העובדים מרחוק שברשותם תקשורת אינטרנט בטוחה, טובה ורציפה, סביבה פיזית המאפשרת ריכוז וללא הסחות דעת, ציוד היקפי הולם וכו'. כמו כן, על הארגון להיערך כיאות בהיבטי אספקת ציוד היקפי ופתרונות טכנולוגיים, וכמובן שעלינו גם להגביר את מודעות העובדים להיבטי אבטחת המידע - להצפין את הכניסה למחשב הפרטי, לא לשמור עליו מידע, לא להשליך טיוטות וניירות עבודה לפח הביתי וכו'.

אחת מהתובנות החשובות ביותר היא שלא משנה אילו שגרות תסגלו לעצמכם כמנהלים בעידן של 'עבודה מרחוק' או 'עבודה היברידית', תדאגו שהדברים יהיו נהירים וידועים לכל הגורמים הרלוונטיים (העובדים והמנהלים כאחד).

**צוותים שרק לאחרונה עברו למצב של עבודה מרחוק עומדים בפני אתגרים חדשים שעשויים לערער את נורמות העבודה והתקשרות של הצוות, את טיפוח המורל ואת הרגשת השייכות והחונכות.**

הגדרות לא ברורות דיין של המצופה מהמנהלים ומהעובדים בעת עבודה מרחוק יחריפו את התחושות הללו ויגבירו את אי הוודאות.

אנחנו כמבקרים פנימיים בוחנים כמעט בכל מטלת ביקורת את קיומם של מדיניות ונהלים ברורים והולמים לנסיבות העניין. 'נאה דורש, נאה מקיים' - עגנו כתורה שבכתב את העקרונות ושגרות העבודה והניהול המצופות בעת עבודה מרחוק. הקפידו שתורה זו תנוסח בצורה ברורה ובשפה פשוטה על גבי מסמך מדיניות או נוהל עבודה. מומלץ שמסמך המדיניות או הנוהל יתייחסו גם להיבטים שאליהם התייחסנו במאמר זה.

## עיגון העקרונות לעבודה מרחוק ונוהלי העבודה במסמך ברור

## תורה שבכתב ולא שבעל-פה

> אין ספק שעבודה מהבית מטשטשת את הקווים שבין החיים המקצועיים לבין החיים האישיים ולמעשה כל ה-WORK-LIFE BALANCE מתערער

האתר
לשירותכם

WWW.THEIIA.ORG.IL

תוכלו למצוא בו

- תקינה ומידע מקצועי ממוין לנושאים לפי קטגוריות -
- חדשות ועדכונים על חידושים במקצוע -
- בלוגים ודעות בנושאים שונים -
- כתבי עת קודמים לקריאה דיגיטלית -
- קורסים וערבי עיון -
- כנסים בארץ ובחו"ל -

לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA ISRAEL-INSTITUTE OF INTERNAL AUDITORS


# עקרונות ו'טיפים' לעבודה מרחוק ולניהול מרחוק:

## מראה וניהול ישיבות

'כאילו אתה במשרד' (להתלבש, להתגלח/להתאפר בהתאם להרגלים לפני כן, לשבת על ה-...).

ישיבות - לא לאחר ואם אתה יוזם הפגישה אף תקדים (אף אחד לא אוהב להמתין מול מסך).

הקלטת ישיבות - להודיע מראש.

התייעלות בפגישות עם לקוחות - לנסות לשמר את 'תרבות הוידאו' גם אחרי המשבר.

## שגרות יומיות לצוות

גיבוש ערוצים לתקשורת שוטפת עם העובדים (Microsoft Teams, ווטסאפ, תיבת דוא"ל ייעודית וכו').

שיחות עבודה צוותיות קבועות (VC של תחילת יום/סוף יום).

שיחות ניהול קבועות לסקירת תכנון מול ביצוע, הצפת בעיות וכו'.

פגישות הווי צוות קבועות (VC שבועיות / Happy Thursday Happy Hour...).

## סביבת העבודה

תשתית אינטרנט וציוד מחשוב טובים שיאפשרו עבודה רציפה.

סביבת עבודה פיזית נוחה ונקייה מהסחות דעת (שולחן וכסא, ילדים ברקע, מטלות בית וכו').

הקפדה יתרה על אבטחת מידע פיזי ולוגי (paperless, נהלי גריסה וכו').

הגדרה ברורה של נהלי שמירת החומר ברשת/ בתיקים ולא בפרטי.

## לסיכום,

אין ספק שעבודה מרחוק לעולם לא תהיה זהה לעבודה מקרוב, מה שעבד במסגרת המשרד לא תמיד יעבוד מרחוק. לצד זאת, ברור לנו כיום שלא כל האמצעים והשגרות של עבודה במשרד הם הכרחיים, ולא אחת גם גילינו שעבודה מרחוק או עבודה היברידית מביאה להתייעלות בעבודה.

במאמר זה ביקשנו לשתף מהניסיון שנצבר ומהתובנות שאליהן הגענו תחת ההבנה שאין פתרון קסם לניהול אפקטיבי של עבודה מרחוק. המפתח להצלחה הוא 'לעבוד לאחור' - להגדיר בבירור את התוצאות שהיינו רגילים אליהן או ציפינו להן בעבודה במשרד, ולגבש את מתכונת העבודה שתבטיח שגם בעבודה מרחוק נגיע לאותן התוצאות (או לתוצאות טובות יותר...).



## מסגרת העבודה

הגדרה ברורה של מסגרת שעות העבודה.

תיאום ציפיות לגבי שעות זמינות הצוות.

## שינוי תפיסה

מעבר מתפיסה של ניהול עובדים מקרוב ומדידה תשומות לתפיסה של ניהול מרחוק ומדידת תפוקות, או לכל הפחות, 'ניהול היברידי'.

## מעקב ביצוע

מעקב הדוק על בסיס יומי אחר ביצוע המשימות בפועל - שיחות/דיווח מפורט של העובד.

עדכון מסמך התכנון לאור הביצוע בפועל.

## תכנון

להכין 'סידור עבודה' מפורט - משימות, תוצרים/תפוקות לכל משימה, הערכת שעות/ לוחות זמנים ברורים לכל עובד ולפרק זמן של יום-יומיים מראש (אקסל, משימות באאוטלוק...).

לקחת בחשבון צרכים/תלות של העובד במבוקרים/במנהל וכו', ולזהות מראש צווארי בקבוק.

לתכנן מסגרת שעות עבודה חופפות של הצוות והמנהלים לצורך התייעצויות ונושאים שיעלו אד-הוק.

# הונאות ומעילות בישראל

## תמונת מצב ומבט לעתיד על רקע משבר הקורונה

מאת: שי מדינה | רו"ח CFE, LLM, שותף ומנהל מחלקת הביקורת החקירתית
בפאהן קנה ניהול בקרה בע"מ

### הסקר

סקר עבירות צווארון לבן שערכה מחלקת הביקורת החקירתית בפאהן קנה ניהול בקרה, בדק מספר ארגונים שבחלקם התרחשו אירועי הונאות ומעילות במהלך השנים 2018-2019. הסקר בחן פרמטרים שונים כדוגמת ניתוח סוגי המעילות, מגזרי הפעילות שאליהם משתייכים הארגונים שבהם בוצעו המעילות, פרופיל מבצעי המעילות, הקשר בין הפרופיל לאופן הטיפול, וכימות הנזק שנגרם לארגון. הסקר הקיף חברות וארגונים מובילים במגזר העסקי, ובהם גופים ממשלתיים, רשויות מקומיות, מלכ"רים, וחברות ציבוריות ופרטיות מענפים שונים: מסחר, תעשייה, נדל"ן, פיננסים, היי-טק וכדומה. הסקר מעלה מסקנות ותחזיות לעתיד אודות ריבוי המעילות שעוד נכונות להיחשף במהלך 2020, בייחוד לנוכח השפעות משבר הקורונה המתמשך.

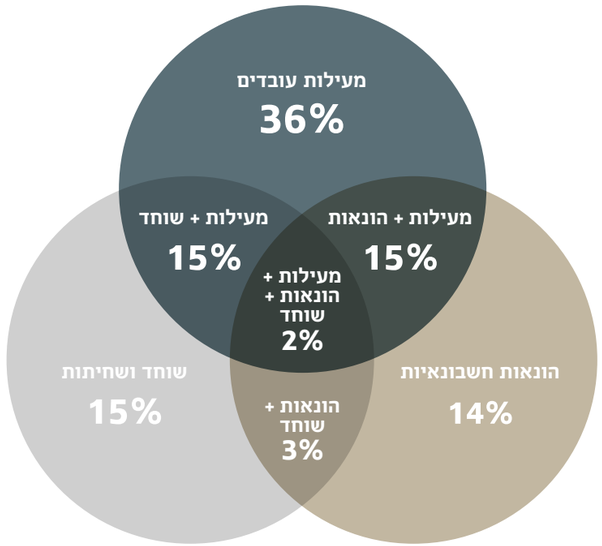
בעקבות אירועי הקורונה מובאים בסוף הניתוח עוד דגשים רלוונטיים.

להלן עיקרי הסקר:

## סוג המעילה

מקרי המעילות שנבדקו סווגו לשלושה מאפיינים עיקריים:

**מעילות עובדים** - הונאות של גורמים פנימיים (לעיתים בשיתוף פעולה עם גורמים חיצוניים), הפוגעים בנכסיו ובמצבו הכספי של הארגון.




**הונאות חשבונאיות** - הונאות המבוצעות על ידי הנהלת הארגון כלפי גורמים חיצוניים. הונאות מסוג זה כוללות מצגים מעוותים בכוונת זדון על מצבו הכספי של הארגון, במטרה להונות את ציבור המשקיעים ו/או גורמים הנמצאים בקשר עסקי עם הארגון.

**שוחד ושחיתות** - שימוש לרעה של בעל תפקיד/מקבל החלטות בסמכויותיו על מנת להשיג טובות הנאה או רווח אישי.

**הסקר מעלה כי מעילות עובדים מהוות 68% מהאירועים שנבדקו, כאשר מחציתן בוצעו בשילוב מעשי שחיתות והונאות חשבונאיות.**

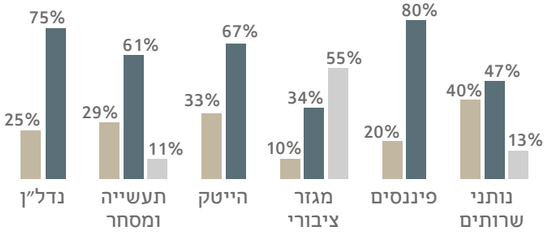
ב-35% מכלל האירועים שנבדקו עלו חשדות למעשי שוחד ושחיתות.





## התפלגות סוג המעילה לפי מגזר פעילות

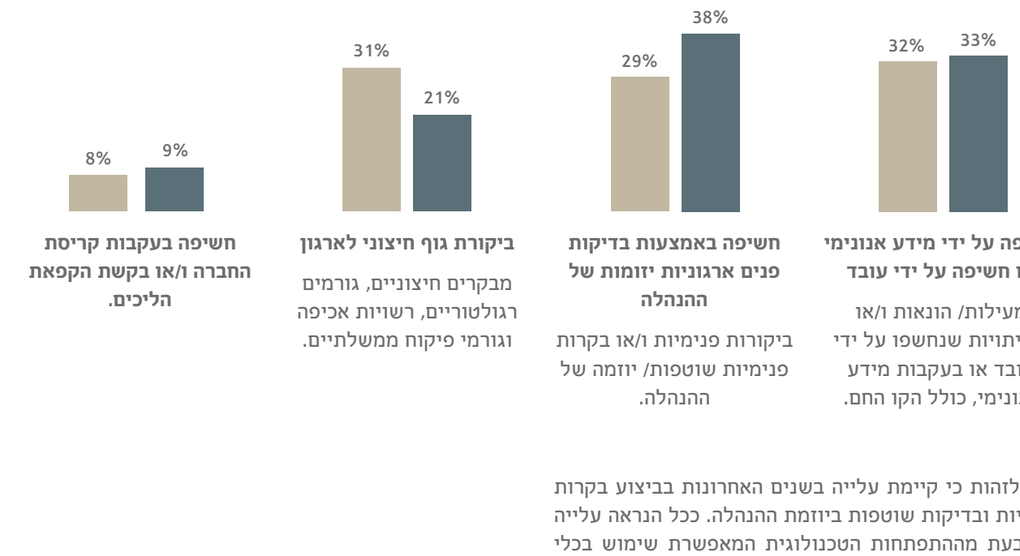
| המגזרים שהובילו במקרי שוחד ושחיתות | המגזרים שבהם בלטו מעילות העובדים | המגזרים שהובילו בתחום הונאות חשבונאיות |
|---|---|---|
| המגזר הציבורי 55% | פיננסי 80% (בוצעו על ידי עובדים) | נותני השירותים 40% |
| נותני השירותים 13% | נדל"ן 75% | היי-טק 33% |
| התעשייה והמסחר 11% | ההיי-טק 67% | התעשייה והמסחר 29% |
| | התעשייה והמסחר 61% | |




בשנים האחרונות חלה עלייה בשיעור המקרים שבהם עלו החשדות למעשי שוחד ושחיתות. נתון זה אינו מעיד בהכרח על עלייה במספר העבירות מסוג זה, אלא על עלייה במספר המקרים שנחקרו ונחשפו ביחס לשנים קודמות. ייתכן כי העיסוק התקשורתי הרב בעבירות מסוג זה גרם גם כן לעלייה במספר המקרים שנחקרו ונחשפו.

## אופן איתור המעילה

הסקר התייחס לארבע קטגוריות שבהן נחשפו המעילות:




**חשיפה על ידי מידע אנונימי או חשיפה על ידי עובד**

מעילות/ הונאות ו/או שחיתויות שנחשפו על ידי עובד או בעקבות מידע אנונימי, כולל הקו החם.

**חשיפה באמצעות בדיקות פנים ארגוניות יזומות של ההנהלה**

ביקורות פנימיות ו/או בקרות פנימיות שוטפות/ יוזמה של ההנהלה.

**ביקורת גוף חיצוני לארגון**

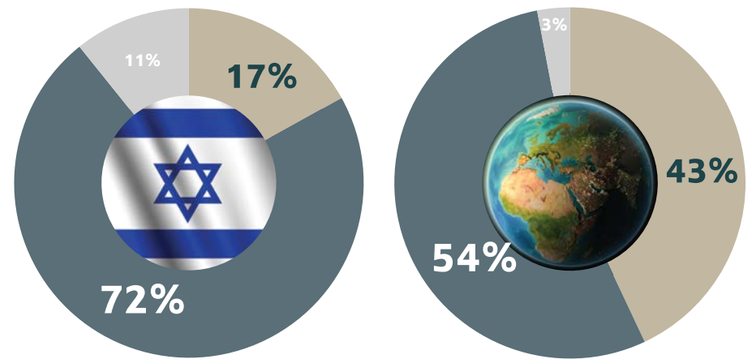
מבקרים חיצוניים, גורמים רגולטוריים, רשויות אכיפה וגורמי פיקוח ממשלתיים.

**חשיפה בעקבות קריסת החברה ו/או בקשת הקפאת הליכים.**

ניתן לזהות כי קיימת עלייה בשנים האחרונות בביצוע בקרות פנימיות ובדיקות שוטפות ביוזמת ההנהלה. ככל הנראה עלייה זו נובעת מההתפתחות הטכנולוגית המאפשרת שימוש בכלי בקרה פנים ארגוניים מתקדמים יותר. כיום נראה כי ארגונים רבים מחליטים להשקיע משאבים ביישום בקרות ממוחשבות, במטרה למנוע ולצמצם את הסיכון להתרחשותן של מעשי הונאות ומעילות העלולות להסב נזק משמעותי לארגון.

## פרופיל מבצע המעילה

פרופיל המועל מגלה כי השנה, בדומה לשנים קודמות, את מרבית ההונאות והמעילות בישראל מבצעים מנהלים ובעלי חברות ו/או גורמים בכירים:72% ממבצעי המעילות בשנים 2018-2019 הם עובדים בכירים בארגון ו/או בעלי מניות ושותפים בחברות (לעומת 73% בשנים 2016-2017).

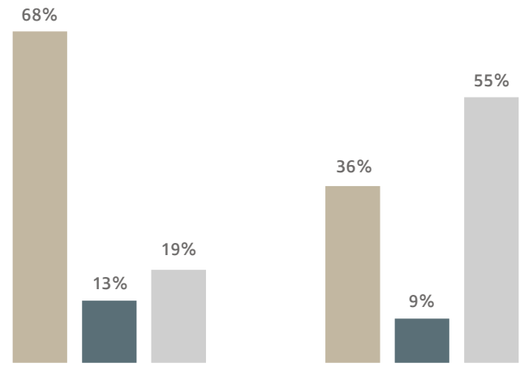



עובדים זוטרים ● גורמי חיצוניים ● עובדים בכירים ובעלי הארגון (בעלי מניות ושותפים)

## הקשר שבין היקף הנזק לפרופיל מבצע המעילה

הסקר מגלה כי קיים מתאם בין פרופיל מבצע המעילה לבין היקף הנזק.

**במרבית המעילות שביצעו עובדים זוטרים היקף הנזק הכספי עומד על מתחת ל-500 אלפי ₪, ואילו ברובן המכריע של המעילות שביצעו גורמים בכירים בארגון, היקף הנזק הכספי עומד על סכום של מעל מיליון ש"ח.**







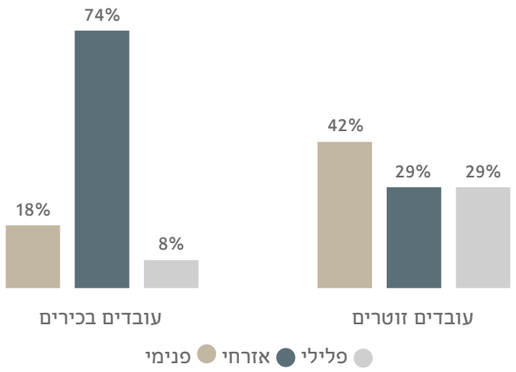

## הקשר שבין פרופיל המבצע לאופן הטיפול במעילה

הסקר העלה כי מרבית המעילות שביצעו עובדים זוטרים טופלו בארגונים בהליך פנימי

**42%**

לעומת זאת, רוב המעילות שביצעו גורמים בכירים בארגון טופלו בהליך אזרחי

**74%**

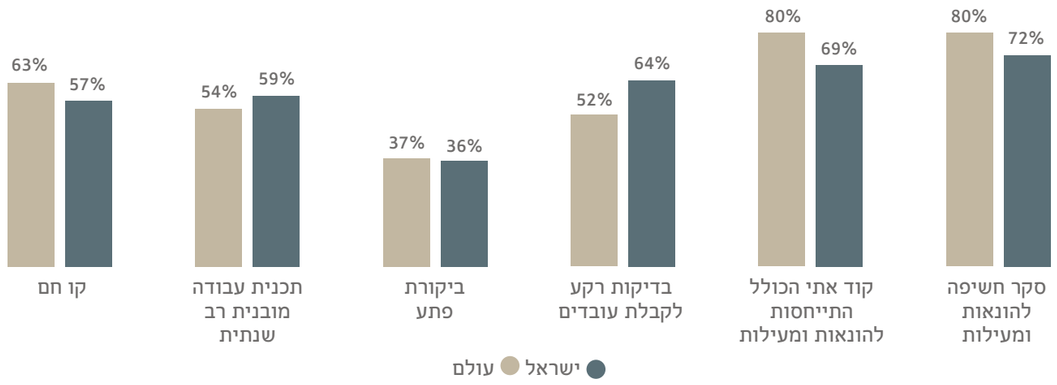



**במרבית המעילות שביצעו גורמים בכירים בארגון, הארגונים פועלים על פי ההנחה כי ניתן יהיה להשיב את הכסף או את חלקו מאותם גורמים ולכן פונים להליך האזרחי.**

לעומת זאת, מעילות שביצעו גורמים זוטרים בארגון, מטופלות בדרך כלל בהליכים פנימיים בשל ההבנה כי הסיכוי להשיב את כל הסכום שנגנב אינו גבוה, קל וחומר אם ייפתחו הליכים משפטיים נגד מבצע המעילה.

בעולם מתקיימת מגמה הפוכה לישראל, כאשר חלק ניכר מאירועי המעילות (44%) שביצעו גורמים זוטרים בארגון מטופלים בהליך הפלילי. הפנייה להליך הפלילי מבוצעת בדרך כלל כאשר קיים אינטרס ציבורי מובהק, והארגון סבור שיש ערך מוסף לפנייה לרשויות האכיפה ובחלק מהמקרים אף בסיוע לקידום התיק גם בהליך האזרחי.

## שימוש באמצעים למניעת מעילות




ישראל היא אחת המדינות החברות בארגון ה- OECD, וחברות ישראליות נדרשות לעמוד ברגולציה מחייבת. לכן הן מטמיעות כלי בקרה הנפוצים כיום בעולם כולו. בעוד שבעבר ארגונים הסתפקו בביצוע סקר סיכוני הונאות ומעילות, הרי שכיום ארגונים מבינים כי הדרך הנכונה להתמודדות עם האיומים המשתנים היא באמצעות תוכנית עבודה מודולרית, המאפשרת למקד בקרות ובדיקות חכמות בתהליכי עבודה ובאזורים שזוהו כבעלי סיכון גבוה למעשי הונאות ומעילות.

## מגפת הקורונה
## השלכות עתידיות על חשיפת מעילות בארגונים

על רקע מגפת הקורונה והמשבר הכלכלי העמוק הפוקד את המשקים, ניתן לזהות עלייה במספר מקרי ההונאות והמעילות המתפרסמים באמצעי התקשורת הן בארץ והן בעולם. השאלה המתבקשת היא מדוע דווקא בתקופות קשות נחשפות יותר פרשיות מסוג זה, והאם קיים קשר בין מעילות לבין משבר כלכלי. נראה כי התשובה לכך נמצאת בכמה מישורים:

- התקופה הקשה מחייבת צעדים ארגוניים מהותיים ואגב כך גוברת ההסתברות לחשיפה. לדוגמה, לאחרונה התפרסמו ידיעות בדבר חשדות על מעילה בסך מיליוני שקלים שביצעה לכאורה מנהלת חשבונות ותיקה בחברת פרסום חוצות. לפי הפרסומים, בשל מגפת הקורונה נאלצה הנהלת החברה להוציא את מרבית עובדיה לחל"ת, ובהם גם את העובדת החשודה. בעקבות בדיקות פנימיות שערכה הנהלת החברה במהלך תקופת החל"ת, עלו החשדות כנגד העובדת בדבר מעילה שהתרחשה לכאורה במשך מספר שנים.
- **בתקופות משבר נוטים מנהלי החברות לבדוק את התהליכים העסקיים בחברה כדי למזער נזקים. לעומת זאת, בתקופות שפע המנהלים נוטים לעסוק בעיקר בצמיחה וביצירת הזדמנויות עסקיות חדשות, ופחות מתמקדים באיתור ומניעת פרצות במערכי הבקרה.**

לדוגמה, אתי אלון מעלה בכספי הבנק למסחר במשך שנים ובהיקף של מאות מיליוני שקלים. המעילה נחשפה רק מספר חודשים לאחר המשבר הכלכלי של 2001 והביאה עם חשיפתה לקריסתו של הבנק. דוגמה נוספת היא ההונאה הפיננסית של ברנרד מיידוף, המהווה את אחת מהונאות הפונזי הגדולות בהיסטוריה. ההונאה נחשפה בעיצומו של המשבר הכלכלי העולמי אך התבצעה במשך מספר שנים קודם לכן. ההסבר לכך הוא שבתקופות שפל בורסאי מקורות המימון נעצרים, ובהונאות פירמידה מסוג פונזי, המתאפיינות בשימוש בכספי משקיעים חדשים על מנת לממן תשואות למשקיעים הוותיקים, הדבר גורם לקריסתה של הפירמידה שנבנתה.

- תקופות שפל ומשבר מתאפיינות גם במספר רב של סכסוכים עסקיים בין שותפים. במקרים כאלה הצדדים משתמשים בכל הכלים המשפטיים העומדים לרשותם, ולכן לא פעם גם מתעוררים חשדות לגבי טוהר המידות של השותפים. כל עוד העסקים שגשגו לא נשאלו שאלות ולא צפו חשדות, אך בתקופת משבר נשאלות השאלות הקשות ולעיתים גם מאותרות פעולות "חריגות" שבוצעו בעבר.

> אין זה מן הנמנע כי בסיומו של ה"צונאמי הכלכלי" שהביא עימו משבר הקורונה, יתגבר קצב חשיפת הפרשיות של מעשי הונאות ומעילות מסוגים שונים, שייתכן שכלל לא היו נחשפות כל עוד השווקים היו בתקופת שפע וגאות.

כאמור, ההיסטוריה מלמדת אותנו כי

**חלק ניכר ממעשי הונאות ומעילות נחשפים ביתר שאת בעיתות משבר,**

והתחקות אחר הפעולות "החריגות" מגלה שהן החלו דווקא בתקופות של צמיחה כלכלית. אין זה מן הנמנע כי בסיומו של ה"צונאמי הכלכלי" שהביא עימו משבר הקורונה, יתגבר קצב חשיפת הפרשיות של מעשי הונאות ומעילות מסוגים שונים, שייתכן שכלל לא היו נחשפות כל עוד השווקים היו בתקופת שפע וגאות.

**בהקשר הזה ראוי לציין כי חברות שבהן קיימים מערך ביקורת ומנגנוני בקרה ופיקוח שוטפים, צולחות תקופות של שפל ומשבר בצורה טובה יותר מאשר חברות אחרות.**

> על רקע מגפת הקורונה והמשבר הכלכלי העמוק הפוקד את המשקים, ניתן לזהות עלייה במספר מקרי ההונאות והמעילות המתפרסמים באמצעי התקשורת הן בארץ והן בעולם.




# תואר שני במשפטים בהתמחות בלימודי ביקורת פנימית

משפטנים (LL.M)
משפטים ללא משפטנים (M.A.)

אוקטובר 2020
המכללה למנהל (ראשל"צ)

הטבות מיוחדות לחברי הלשכות המקצועיות

"מלגה" בסך של 2,000 ₪ מטעם לשכת המבקרים הפנימיים IIA ישראל ללימודי תואר שני במשפטים – M.A. או LL.M. – עם התמחות בביקורת פנימית

חברות חינם (בתקופת הלימודים) בלשכת המבקרים הפנימיים IIA ישראל

השתתפות ללא תשלום ב-2 ערבי עיון (או וובינרים) של לשכת המבקרים הפנימיים IIA ישראל

לפרטים נוספים והרשמה:
לשכת המבקרים הפנימיים IIA ישראל
טל' | 054-2391957
דוא"ל | OFFICE@THEIIA.ORG.IL

# שוד ושבר

## ביקורת פנימית על תהליך ניהול משברים

מאת: דני פרידמן | CIA, CISA, CRISC - המבקר הפנימי, אמדוקס

דרור בר משה | רו"ח, LLM, CIA, CISA, CRISC, CFE CSX-F, CRMA - סגן המבקר הפנימי, אמדוקס, חבר ועדת ביקורת - לשכת המבקרים הפנימיים IIA ישראל

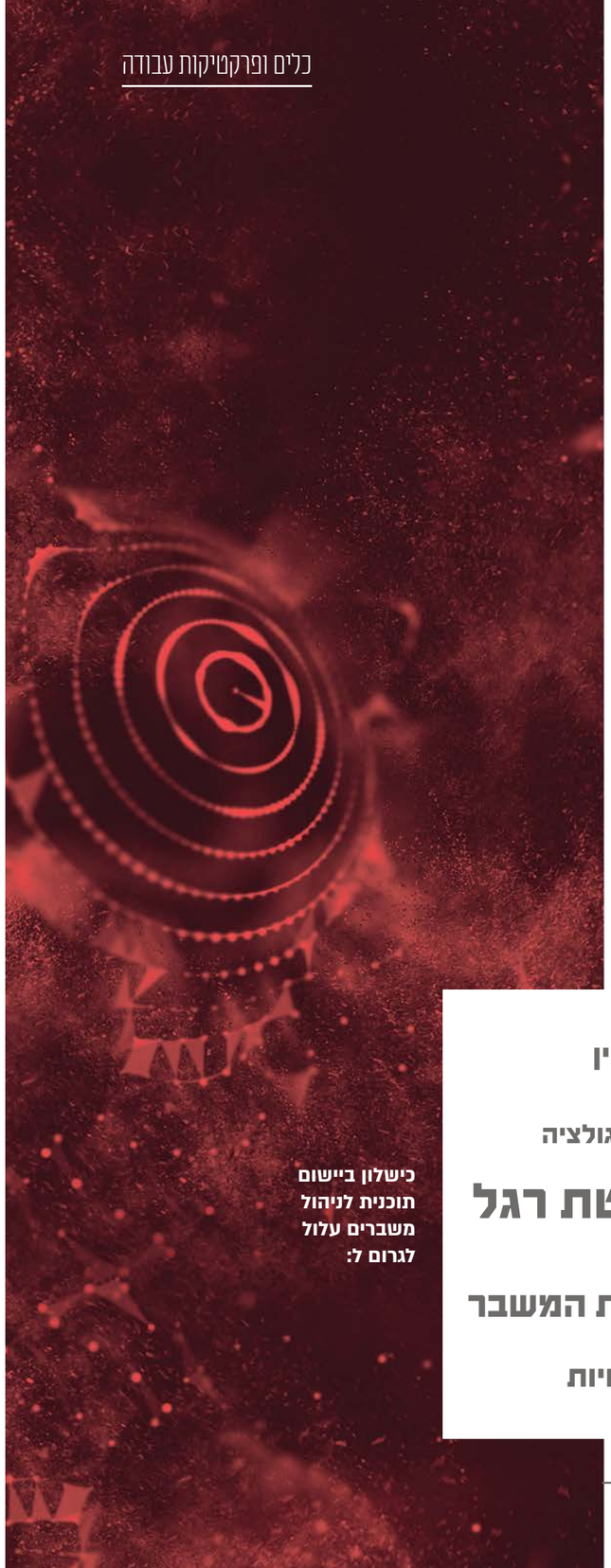
מגוון האיומים שבפניהם עומדים כיום ארגונים הולך ומתרחב. יחד עימם גדלה ההסתברות להיווצרותם של שיבושים/משברים שעלולים לשבש את מהלך העסקים הרגיל עד לכדי איום ממשי על המשך קיומם.

**בסקר שפורסם כמה חודשים לפני משבר הקורונה COVID-19 שבוצע ע"י דלויט, Global Risk Management Survey**

**23% מהמשיבים הציבו את הסיכון לאירוע משברי כסיכון השישי בדירוג הסיכונים שבפניהם עומד הארגון.**

**בסקר נוסף של דלויט, Staying Relevant – 2020 Hot Topics for Internal Audit in Financial Services,**

**סווג הנושא "חוסן תפעולי" (Operational Resilience) כנושא השני בחשיבותו לבדיקה על ידי הביקורת הפנימית.**








## מהו משבר?

משבר הוא אירוע או סדרה של אירועים בלתי צפויים היוצאים משליטה ומשבשים באופן מהותי את מהלך העסקים של הארגון.

זהו אירוע שלרוב יקבל הד תקשורתי רחב מאוד, השפעותיו השליליות תורגשנה בטווח המיידי, ולפיכך יהיו במוקד תשומת הלב של בעלי המניות. מסיבה זו התוכניות וההכנות של הארגון להתמודדות עם משברים הן בעלי חשיבות עליונה להנהלה הבכירה, לבעלי המניות ולמחזיקי עניין אחרים (כמו לקוחות וספקים, מוסדות פיננסיים וכדומה).

משברים מאופיינים לרוב בעיתוי ובאופן שהם מופיעים:

**משברים בדרך כלל מתרחשים במפתיע, אינם בשליטת הארגון, דורשים תגובה מיידית, וכל טעות בקבלת החלטות עלולה להיות בלתי הפיכה,**

כלומר לארגון ולתדמיתו עלול להיגרם נזק לזמן ארוך ובמקרים קיצוניים גם יש איום לשרידותו.

כאן טמון ההבדל המהותי בין "משבר" לעוד אירוע של "המשכיות עסקית" - מונח המוכר לנו זה מכבר. נדגיש כי אירוע מקומי ומוגבל בהיקפו שנהגנו לשייך לאירוע DR או BCP איננו משבר. עם זאת, ככל הנראה גם אירוע נקודתי של המשכיות עסקית ועימו כשל בניהול, עלול להפוך למשבר אם הוא לא מטופל כיאות.

ישנן מספר מתודולוגיות לניהול משברים. המובילות שבהן הן תקן ניהול משברים של מכון התקנים הבריטי (BS 11200 : 2014 Crisis Management - Guidance and Good Practice) וכן סיפרו של Otto Lerbinger, "The Crisis Manager", שנחשב לגורו בתחום.

> "הפרקטיקה של ניהול משבר "על הדרך", לאחר שהוא פורץ, הוכחה כדרך שגויה. אומנם קשה לתכנן מראש מענה ותוכניות לכל סוגי "תסריטי אסון", אולם ניתן לבנות תבניות כלליות עם עקרונות פעולה המתאימים לרוב המשברים."

## סוגי משברים

על פי הספרות והפרקטיקה המקובלת בניהול משברים, נהוג לחלק את עולם המשברים ל-7 קבוצות עיקריות:

**אסון טבע**

למשל: רעידות אדמה, הוריקנים, סערות, התפרצות הר געש, שיטפונות, צונאמי, בצורת, התפרצות מחלות.

**משבר טכנולוגי**

למשל: דליפת חומרים מסוכנים (כמו דליפת נפט לים), תאונות תעשייתיות, כשלי תוכנה.

**עימות**

למשל: חרם, אולטימטומים, חסימות, כיבוש מבנים, התנגדות או אי ציות למשטרה.

**זדון או חבלה**

למשל: חבלה של מוצרים, חטיפות, שמועות זדוניות, טרור, פשעי רשת וריגול.

**פשעים ארגוניים**

למשל: הונאה, סילוף, הטעיה, רמייה, התנהלות הנהלה פסולה.

**אלימות**

למשל: אלימות של עובד או עובד לשעבר כלפי עובדים אחרים.

**שמועות**

למשל: מידע כוזב המופץ על ארגון ו/או על מוצריו וגורם נזק נרחב למוניטין של החברה.

## ניהול הסיכון

היכולת לנהל משברים קובעת בסופו של דבר את מידת עמידותו של הארגון. ארגון בעל יכולת עמידות גבוהה יהיה חסין יותר במהלך המשבר.

חוסן ארגוני מחייב ניהול אפקטיבי של משברים שיש להתכונן לקראתו מראש. הפרקטיקה של ניהול משבר "על הדרך", לאחר שהוא פורץ, הוכחה כדרך שגויה. אומנם קשה לתכנן מראש מענה ותוכניות לכל סוגי "תסריטי אסון", אולם ניתן לבנות תבניות כלליות עם עקרונות פעולה המתאימים לרוב המשברים.

**ברור שהמאמץ הנדרש להתאמת משבר ספציפי למסגרת הבנויה מראש הוא קטן לאין ערוך מאשר לבנות מהיסוד, עם פרוץ המשבר, את כל מסגרת המענה.**

בנייה מראש של מענים סבירים דורשת גישה צופה פני עתיד וראייה שיטתית היוצרת מסגרות, תבניות, תוכניות הכשרה, תרגול ותחזוקה שוטפת.

פיתוח יכולת ניהול משברים צריכה להיות פעילות ממוסדת/קבועה ופרופורציונאלית לגודלו ויכולתו של הארגון. הדבר רלוונטי לכל ארגון ללא קשר למיקום, גודל, סוג, ענף או מגזר.

פרקטיקה לפיתוח יכולת ניהול משברים כוללת בדרך כלל ארבעה שלבים: זיהוי, הכנה, תפעול וחזרה לשגרה. שלבים אלה כוללים את האלמנטים הבאים:

- מיפוי סיכונים וסוגי המשברים הפוטנציאליים.
- ניתוח הפגיעה הפוטנציאלית בפעילות.
- פיתוח ותחזוקה של תוכניות לתרחישים מזוהים.
- מעקב אחר בעיות מתהוות.
- עריכת תרגילים ועדכון התוכניות.
- קביעת צוות לניהול משברים.
- תקשור.
- נקיטת פעולות חזרה לשגרה.
- הערכת ההשפעה לטווח הארוך.
- עריכת סקירה שלאחר המשבר ושינוי תוכניות בהתאם.

מניסיוננו, לרוב הארגונים ישנה תוכנית המשכיות עסקית לטיפול במשבר שמקורו באסון טבע (פגיעה בתשתיות פיזיות-לאומיות או ארגוניות או שתיהן), ולחלק מהארגונים אף קיימת תוכנית לטיפול במשבר שמקורו באירוע סייבר (פגיעה בתשתיות המידע), אך המציאות של המאה ה-21 הוכיחה שישנם משברים אחרים שלא כרוכים דווקא בפגיעת תשתיות פיזיות או דאטה. הנה כי כן התוכניות להמשכיות עסקית דורשות מחשבה ורענון.

> "סיכון של התפרצות משברים הוא סיכון מהותי וקיומי, וצריך להיות חלק מניהול הסיכונים התאגידי"

**לדוגמה, בעידן של רשתות חברתיות השולטות על חלק נכבד מחיינו, ראוי להדגיש במיוחד את נושא הפגיעה במוניטין ואת הצורך בהיערכות לתגובה ארגונית – תגובה תקשורתית פנים ארגונית וחוץ ארגונית.**

בהקשר הזה ראוי להזכיר את המשבר התדמיתי-תקשורתי שאליו נקלעה חברת התעופה יונייטד איירליינס בשנת 2017, כאשר רופא שקנה כרטיס טיסה במיטב כספו הורד מהטיסה לאחר שבטיסה היה אובר-בוקינג. הרופא נבחר בהגרלה וסירב להתפנות מהמטוס. הוא נגרר בכוח החוצה ובתוך מספר שניות התפרסמו ברשתות החברתיות סרטונים שבהם נראה הרופא נגרר מהמטוס בכוח כשפניו מדממות. האירוע היה דרמטי - ניהול המשבר בכלל וניהול ההד התקשרותי בפרט לא יכול היה להיות קלוקל יותר: ההצהרות הראשוניות של המנכ"ל לתקשורת היו הרסניות, דבר שהפך משבר נקודתי לחמור יותר והביא אותו לראש מבזקי החדשות בכל העולם. מניית החברה כמובן צנחה בעקבות האירוע.

מנגד, האירוע הטראגי של אייר-אסיה, שבו מצאו את מותם 162 אנשים בהתרסקות, מוזכר במאמרים רבים כדוגמה להתנהלות תקשורתית טובה בזמן משבר. מנכ"ל החברה בעצמו השתמש במדיה החברתית כדי לתקשר עם הציבור ולמזער סיכון של הפצת מידע שגוי. ה"ציוצים" שלו גילו מלכתחילה חמלה ודאגה ומינפו יחסי אמון. ראוי לציין כי לחברה הייתה אסטרטגיה למדיה חברתית שפותחה מבעוד מועד, ולמנכ"ל היו חשבונות/פרופילים פעילים מאומתים במדיה החברתית.

ואם במגזר התעופה עסקינן, ניתן גם לציין משבר מסוג אחר שאליו נקלעה חברת בואינג. ניתן לסווג משבר זה כמשבר טכנולוגי, שבו מהנדסים וטייסים התלוננו שהם מתקשים "להשתלט" על מטוס ה-737 מקס, והזהירו מקטסטרופה ובעייתיות של מערכת הבטיחות. כל זה לא מנע מבואינג להשיק בחופזה את המטוס. מותם של 346 אנשים בשתי התרסקויות גרמו למשבר החמור ביותר בחברה מאז הקמתה ב-1916. המנכ"ל הודח, המניה קרסה, ואמון הציבור בחברה שנחשבה לגאוותה של ארה"ב נפגע בצורה אנושה.

ראוי לציין כי היום יש חברות בין-לאומיות גדולות הנותנות שירותי ניהול משבר. ניתן להתקשר עם חברות אלה עם קרות המשבר (עלויות גבוהות) או בתשלום חודשי/שנתי למקרה שנכפה משבר (בעלות נמוכה יותר).





## ביקורת פנימית על תהליך ניהול משברים

הדוגמאות שתיארנו לעיל, ועוד עשרות מקרים שהתרחשו לאחרונה, בעיצומו של עידן הקורונה, מאפשרים לנו להבין את גודל הסיכון שטמון באי היערכות של הארגון להתמודדות עם משברים.

לפיכך זוהי הזדמנות בלתי רגילה למבקרים הפנימיים בארגונים השונים להביא ערך להנהלה הבכירה ולדירקטוריון בנושא כה מהותי וקיומי לארגון.

כנושאים אופציונליים לתוכניות עבודה שנתיות, אנו מציעים לציבור המבקרים לכלול נושאים אלו:

1. הערכת הממשל התאגידי של ניהול משברים, כולל היערכות ובניית מסגרת ומבנה ארגוני לניהול משברים, פיקוח ותרגול.
2. בדיקת ניהול משברים מבוסס סיכונים, כולל סקר סיכונים תקופתי וזיהוי תרחישי משבר אפשריים.
3. בחינת תוכנית לניהול סיכוני משברים - בנייה מראש של הנהגת משבר, הערכת אירוע ראשונית, ניהול כוח אדם, בניית ערוצי דיווח פנים ארגוניים, תקשורת ודיווח.
4. בדיקת תרגול התוכנית לניהול משברים.
5. בחינת הערכה ותחזוקה של תוכניות ניהול משברים.

## סיכום

כפי שנוכחנו לדעת במשבר הקורונה, סיכון של התפרצות משברים הוא סיכון מהותי וקיומי, וצריך להיות חלק מניהול הסיכונים התאגידי. סיכונים אלה נתמכים גם בסקרים שונים שבוצעו בעולם עוד לפני משבר הקורונה.

חשוב שהארגון ייערך מראש על מנת לתת מענה לסוגי משברים מגוונים.

תרגול מעת לעת של התוכנית הוא קריטי להצלחה גבוהה יותר ומהירה יותר בעת משבר.

מודעות לסיכון היא צעד ראשון וחשוב. הַראו שהנושא הוא באג'נדה של הביקורת הפנימית. שוחחו עם ההנהלה ועם עדת הביקורת אודות סיכון זה, ושתפו ועדכנו את ההנהלה לאורך הדרך. זוהי הזדמנות לביקורת הפנימית להוסיף ערך משמעותי.

# להמחיש בתרחיש – על היתרונות שבבדיקת ערנות

## (בדיקת פתע)

מאת: אסף גלעדי | רו"ח, CISA, בנק לאומי

מוטי שנורמכר | CISA, Bsc - ביקורת מערכות מידע, בנק לאומי

**הסבירו לנו שחשוב לתחקר נתונים, הפכו אותנו ליועצים, תמצתו לנו את הדוחות וצמצמו ממצאים. אז מה עוד אפשר לחדש במקצוע הביקורת הפנימית?!**

בתקופה שבה אנו נדרשים יותר מהרגיל להתמקד רק בסיכונים המהותיים, ולצמצם ככל שניתן את מרכיב ההפרעה לפעילות השוטפת של המבוקרים, עלינו להמציא את עצמנו מחדש ולמצוא דרכים להשקיע את משאבי הביקורת בצורה יעילה, דיפרנציאלית, ובאזורים שיגדילו את ערכי התוצרים וההשפעה שלנו בארגון.

כולנו מכירים את הדרך ה"קלאסית" להערכת סביבת הבקרה ובחינת תהליכי עבודה, הנעשית באינטראקציה מול המבוקרים על ידי שימוש בטכניקה של תשאול (שיחות, פגישות ומיילים) ופעילות עצמאית של סקירת חומרים ונתונים. תהליך ביקורת המתבסס ברובו על טכניקות אלה עלול לעיתים להקשות על קבלת תמונה מלאה המגובה בעובדות, ואף לגרום להסקת מסקנות והערכות העלולות להיתפס כסובייקטיביות.

## אז מה אנחנו מציעים?

**אחת הדרכים להתמודד עם אתגר זה היא "ירידה לשטח". לא מדובר בשיטה חדשה, אך המטרה היא להגביר את השימוש בטכניקה של "בדיקת ערנות" או בשמה הפחות ידידותי "בדיקת פתע".**

אפשר לשלב בדיקת ערנות כמעט בכל ביקורת, ובהמשך המאמר נציג רעיונות ודוגמאות מניסיוננו.

## מה נרוויח מזה?

קודם כל, נחזק את היכולת להגיע למסקנות אובייקטיביות. על הדרך, נוכל לאתגר את אפקטיביות הבקרות באופן בלתי ניתן לערעור, נפחית התנגדויות וויכוחים, נצמצם "הפרעה" על ידי הפחתת הבדיקות והאינטראקציה עם המבוקרים, ונקבל תחושת נוחות מתוצרי הבדיקות. אם באמצעות בדיקת ערנות נגיע למסקנה שבקרה מסוימת אינה פועלת כמצופה או אינה פועלת כלל, נוכל לקדם ביעילות את מטרת הביקורת מבחינת הערכת סביבת הבקרה, ולפנות משאבים לבדיקות נוספות. במקביל, נוכל להעביר באופן מיידי למבוקר את תוצאות הבדיקה על מנת שיוכל לטפל בהמלצות בהתאם לרמת החומרה. וכמובן איך אפשר בלי הנהלת הארגון וועדת הביקורת? גם הם מרוויחים מהתהליך, שכן נוכל להציג בפניהן תמונת מצב מוחשית של סביבת הבקרה בנושא הנבדק.

## איך זה יתבצע בפועל?

על מנת לבצע את משימת הביקורת בצורה האפקטיבית ביותר ולהעריך את אופן התמודדות הארגון עם הסיכון "בזמן אמת", על המבקר לעבור מספר שלבים:

**1**

לסקור את הבקרות הקיימות בארגון בתהליך הנבדק.

**2**

לזהות בקרות חסרות.

**3**

להגדיר את התרחישים המהותיים שהוא ירצה לבדוק.

**4**

לבצע בדיקות ערנות לאתגור הבקרות בתרחישים שהוגדרו.

## קצת המחשות?

**בביקורת בנושא דלף מידע**, מטרת הביקורת הייתה לבחון את תהליכי העבודה והבקרות לצמצום סיכוני דלף המידע. בהנחה שהארגון הגדיר סט של בקרות כמענה לתרחישי דלף שונים, משימתנו היא להעריך את אופן התמודדות הארגון עם סיכון זה. בתהליך הקלאסי יסקור המבקר את מדיניות הארגון בנושא, את נוהלי העבודה, תהליכי הגדרת בקרות, תהליכי טיפול בהתראות, תחזוקה שוטפת ועוד. סקירה זו בהחלט עשויה לתרום להסקת המסקנות בנוגע לתהליך בכללותו אך האם היא תספיק לקבלת מענה לשאלה: **"האם הארגון אכן מוגן מתרחיש דלף מסוים?"** - כנראה שלא.

לעומת זאת, באמצעות בדיקת ערנות המבקר יבצע אתגור מוחשי של הבקרות בכך שינסה לשלוח מידע רגיש אל מחוץ לארגון. ומה ניתן יהיה להסיק מכך?

- אם הוגדרו בקרות והמידע נחסם - הבקרות הקיימות אפקטיביות.
- אם הוגדרו בקרות והמידע יצא - הבקרות הקיימות אינן אפקטיביות והארגון לא מוגן בתרחיש זה.
- אם לא הוגדרו בקרות - לארגון קיימת חשיפה לדלף מידע ועליו לנהל את הסיכון בגינו.

> "נוכל לאתגר את אפקטיביות הבקרות באופן בלתי ניתן לערעור, נפחית התנגדויות וויכוחים, ונקבל תחושת נוחות מתוצרי הבדיקות"

**דוגמה נוספת היא בביקורת סייבר** שבמסגרתה נבקש לבצע ניסיונות חדירה למערכות הארגון מתוך חצרות הארגון. נתחבר באמצעות כלים שונים אל נקודות התקשורת או למצלמות הרשת הפזורות בארגון, ונסה לעקוף את מנגנוני הבקרה הקיימים. גם בבדיקה זו יש להגדיר מראש את המטרות שנרצה להשיג (מעבר בין סביבות עבודה בארגון, חדירה למערכת מסוימת וכו'), ולבחון את רמת ההקשחה (FireWall, מדיניות סיסמאות וכו') הקיימת בארגון.

כמובן שחוץ מלהסיק מסקנות על רמת ההגנה, נוכל גם לבחון בזמן אמת את אפקטיביות מערך הניטור בהקפצת התראות בתרחישים שונים. אם התגלו חוסרים - תוצאות הבדיקה יעזרו בעדכון ההתראות.

## בדיקות ערנות רלוונטיות לרוב עולמות התוכן של המבקרים

- ניתן לאתגר בקרות עסקיות ולבצע פעולות יזומות מעל סף הבקרות שהוגדר.
- ניתן לאתגר בקרות טכנולוגיות על ידי התחברות לארגון מאתר של ספק מאושר ולבחון את שרשרת האבטחה, או לחילופין לבצע תרגיל יזום של אירוע חירום/סייבר ולבחון את מודעות העובדים המהווים, במרבית המקרים, את החוליה החלשה ביותר בשרשרת האבטחה בארגון.
- ניתן לאתגר בקרות תפעוליות או לזהות חשיפות בהיבטים רכים יותר, כמו נגישות, שירות וחוויית לקוח על ידי שליחת לקוח/עובד סמוי לארגון, ביצוע האזנות לשיחות מוקלטות, או צפייה בהקלטות מצלמות האבטחה על פעילות העובדים באתרים רגישים.

מרבית הבדיקות ניתנות לביצוע באופן עצמאי או בסיוע יועץ מומחה, אך לעיתים יידרש, ואפילו מומלץ, לפעול בשיתוף פעולה עם גורם נוסף מתוך הארגון שיתבקש להקפיד על דיסקרטיות לצורך שמירה על אפקטיביות הבדיקה.

## לפני שרצים להעיר את כולם - בואו ננהל גם אנחנו את הסיכונים

**בעת שימוש בבדיקות ערנות, חשוב מאוד ליישם תהליך של "ניהול סיכוני הבדיקה" ולהביאו לידיעת הנהלת הגוף המבקר ואישורו.**

תהליך זה נועד לצמצם את ההשלכות האפשריות של הצלחת הבדיקה (ומהצד השני כישלון הבקרה) והסיכונים שעלולים להיווצר. כך למשל, בדוגמה על אתגור בקרות דלף מידע, אם המידע יצא מחוץ לחצרות הארגון, נוצר מצב שבו מידע רגיש של הארגון "מסתובב" ברשת הציבורית או באמצעי נתיק (DOK) ששימש להוצאת המידע. בדוגמה של ניסיונות חדירה למערכות הארגון, בעת אתגור של בקרה המונעת/מנטרת חיבור רכיב זר לרשת, עלול להיגרם נזק על ידי "הדבקת" הרשת הארגונית או אף חסימתה.

מה חשוב לכלול בתהליך ניהול סיכוני הבדיקה? - זיהוי ומיפוי מראש של הסיכונים תוך בחינת כלל הנושאים שעלולים "להשתבש", הגדרת תוכנית הפחתה מתאימה ויצירת מנגנון של עצירה מיידית בעת הצורך. דרך נוספת לצמצם את הסיכונים היא באמצעות שיתוף רמה בכירה של היחידה המבוקרת. כך ניתן לרתום את המבוקר לתהליך שבו הוא מקבל הזדמנות להיות שותף בבדיקה, ואנו זוכים בשיתוף פעולה בקבלת תוצאות הבדיקה וביישום המלצות הביקורת.

## והתיעוד - לנצח יישאר

היבט חשוב לא פחות בבדיקות מסוג זה הוא התיעוד. על מנת להציג למבוקר את תוצאות הבדיקות שביצענו (וכן - גם קצת להשוויץ 😊), **חשוב לאסוף תיעוד מסודר לאורך כל אחד מהתרחישים הנבדקים.** לדוגמה: ריכוז הקבצים שאנו מעוניינים להדליף מחוץ לארגון, צילומי מסך של הוצאת המידע וקבלתו מחוץ לארגון, הודעות שהתקבלו בגין תרחישים שנחסמו ו/או שנוטרו על ידי מרכז הבקרה, צילום תמונות/סרטונים של הציוד שאנחנו מחברים וכו'. כך נוכל להעביר למבוקר תמונה מדויקת ומבוססת עובדות של מצב סביבת הבקרה לגבי החשיפות והסיכונים הנבדקים באופן שיצמצם התנגדויות ויהפוך כמעט כל ויכוח להסכמה.

## אז מה היה לנו?

גילינו שעל ידי שימוש מושכל בטכניקה של "בדיקות ערנות", הכולל הכנת תרחישי בדיקה, שיתוף גורמים רלוונטיים, ניהול סיכונים אפשריים ותיעוד מסודר - ניתן להגביר לאין ערוך את אפקטיביות הבדיקות המבוצעות במסגרת הביקורת. בשיטה זו ניתן לספק יתרון משמעותי על פני טכניקות בדיקה אחרות ולהציג הוכחות חד-משמעיות המקלות על קבלת הממצאים על ידי הגורם המבוקר.

# פיילוט לאוטומציה רובוטית של תהליכים

**מבקרים פנימיים בחברת הובלת מטענים לוקחים RPA למבחן דרכים**

מאת: ריק רייט* - **מאמר מתורגם**

אוטומציה רובוטית של תהליכים robotic process automation - RPA מקבלת תשומת לב רבה לאחרונה עקב יכולתה לייעל תהליכים ולשפר יעילות. בפשטות, RPA היא אוטומציה באמצעות רובוטים וירטואליים (בוטים) של משימות מבוססות-מחשב שבאופן מסורתי מבוצעות על ידי אנשים. בוטים של RPA מורכבים מתוכנות שמבצעות פעולות חזרתיות באופן זהה לאנשים שמבצעים אותן.

RPA תופס תנופה בעולם העסקי ככלי לאטמט משימות חזרתיות סטנדרטיות המחייבות מינימום של שיקול דעת או חשיבה אנושית. הטכנולוגיה משחררת לאנשים זמן משמעותי לבצע עבודה שהיא בעצם אנושית יותר - משימות המחייבות מידה רבה של מחשבה אינטלקטואלית ואנליטית.

טכנולוגיית RPA בסיסית קיימת כבר כמה עשורים. לדוגמה, סוגים שונים של "מאקרו" בגיליונות אלקטרוניים קיימים זמן רב ומאפשרים למשתמשים לאטמט משימות בסיסיות והקשות בקלידים באמצעות קליק בעכבר. היום, הפיתוחים של בוטים ל-RPA הרבה יותר מתוחכמים. בוטים אינם קשורים למערכת אחת או לבסיס נתונים אחד והם מסוגלים לשלוט בנתונים בלתי מובנים (unstructured data). למשל, בוט יכול "לגרד" מידע מצילום מסך על פי מילת מפתח, צירוף מילים או מיקום של מסך.

היכולות החזקות של טכנולוגיה זו מאפשרות שימוש ב-RPA עבור יישומים רבים, מאיטמוט של התאמות חשבון לביצוע של משימות ביקורת. בהתחשב ביכולות אלו, מחלקת הביקורת הפנימית ב-YRC Worldwide (YRCW), חברת הובלה המתמחה בהובלת מטענים ובשירותים לוגיסטיים עבור חברות שילוח בצפון אמריקה, השיקה תוכנית פיילוט ליישום טכנולוגיית ה-RPA. הפיילוט הצליח ונתן אור ירוק לתוכנית יישום פורמלית ולפריסה של RPA בעתיד.

> "RPA תופס תנופה בעולם העסקי ככלי לאטמט משימות חזרתיות סטנדרטיות המחייבות מינימום של שיקול דעת או חשיבה אנושית"

## התנופה לעבר RPA

מחלקת הביקורת הפנימית ב-YRCW מונה 17 עובדים ומחולקת לשתי קבוצות - קבוצה אחת מתמקדת בציות רגולטורי, במתן הבטחה מבוססת סיכון במוקד העורפי ובשירותי ייעוץ; הקבוצה השנייה מתמקדת בציות ובסקירות תפעוליות עבור יותר מ-300 המסופים למטענים ברשת YRCW. פיילוט ה-RPA של מחלקת הביקורת הפנימית התמקד בתחום הביקורת הפנימית עבור המסופים.





לכל אורך הדרך, הנהלת YRCW דרשה דבר אחד מצוות הביקורת הפנימית: לספק כיסוי ביקורת רחב יותר עם אותו מספר עובדים. בלקיחת האתגר הזה על עצמם, ראשי הביקורת, השואפים לחדשנות, יצאו למשימה אסטרטגית - ליצור את "הביקורת הפנימית של העתיד בנושא הטרמינלים". ביקורת פנימית בנושא טרמינל כוללת בדיקות הבטחת איכות (בדיקות ציות) ובדיקות תצפיתיות, במטרה להעניק הבטחת ציות רגולטורי ותפעולי תוך שימוש בתוכניות ביקורת סטנדרטיות כדי לספק מדידה עקבית של ביצועי הטרמינלים למטענים.

למחלקת הביקורת הפנימית של YRCW מוניטין מוכח של גידול שנתי בכיסוי של הביקורת הפנימית. אולם משנה לשנה נעשה קשה יותר לשמור על ההרחבות האלה.

**מטרת אסטרטגיית "הביקורת של העתיד" היא לא רק להרחיב את הכיסוי של הביקורת, אלא גם להגביר את תרומתה של הביקורת הפנימית על ידי הוספת תכולות לסל השירותים שלה.**

ראשי הביקורת ראו את הפוטנציאל של RPA בהקשר זה כרכיב חיוני באסטרטגיה של הביקורת הפנימית. איטמוט של חלקים של תוכנית הביקורת הסטנדרטית בנושא המסופים יכול לשחרר משאבים יקרי ערך של צוות הביקורת ולאפשר לו להתמקד בשירותים בהם לביקורת ערך מוסף.

> "איטמוט של חלקים של תוכנית הביקורת הסטנדרטית בנושא המסופים יכול לשחרר משאבים יקרי ערך של צוות הביקורת ולאפשר לו להתמקד בשירותים בהם לביקורת ערך מוסף"

## היערכות לאוטומציה

כהכנה ליוזמת "הביקורת של העתיד" ולרכיב ה-RPA שבה, בחנה הנהגת הביקורת הפנימית של YRCW מספר גורמים. בשלב הראשון הם בחנו את היכולות של הצוות, במיוחד המיומנויות הטכנולוגיות והאנליטיות שלו. על אף שכלים של RPA הופכים להיות יותר ויותר ידידותיים למשתמש, כישורים בפיתוח יישומים עשויים לשפר את היכולות של ה-RPA באופן משמעותי. אומנם המבקרים הפנימיים ב-YRCW השתתפו בהשתלמויות כדי לשדרג את הכישורים הטכנולוגיים שלהם במסגרת תוכניות הפיתוח האישיים שלהם, אך הם לא רכשו את הכישורים הרצויים בכתיבת קוד או כאנליסט עסקי כדי לסייע ביישום ה-RPA.

כדי להשיג את הכישורים האלה, הנהגת הביקורת הפנימית הגדירה מחדש משרת אנליסט אחת (שהייתה לא מאוישת באותה עת) והוסיפו לדרישות התפקיד כישורים ב-RPA, שליטה ב-SQL או כישורים אחרים בכתיבת קוד, וניסיון בשיפור תהליכים וכאנליסט עסקי - הכול בנוסף על הרקע הנדרש בביקורת פנימית. למועמד שהתקבל בסוף לתפקיד אומנם לא היה ניסיון ספציפי ב-RPA, אך הרקע והכישורים שלו העידו על עקומת למידה מהירה.

לפני השקת היוזמה, ראשי הביקורת הפנימית היו צריכים להגדיר תפקידים גם עבור חברי הצוות הקיימים. הם הטילו על ראש הפרויקט את המטלות של לימוד העקרונות הבסיסיים של RPA ושל הדרכת יתר חברי הצוות לגבי התכונות העיקריות, הכלים והדרישות. מאמץ זה הוביל ליצירת נייר עמדה שכלל הגדרות של המשימות המתאימות ביותר להעברה ל-RPA, זיהוי הדרישות למשאבים העיקריים, והקביעה אם החזון של ראשי הביקורת הפנימית הוא אכן ריאלי. בנוסף, נייר העמדה הציג תיאור כללי של RPA, מידע על היתרונות הצפויים, אופן הפעולה של RPA, תצורות אפשריות של בוטים, יכולות ושימושים נפוצים, סיכונים, ספקי RPA מובילים וכלים. המסמך תרם לידע הבסיסי של הצוות ולהבנה של היכולות והמגבלות של הטכנולוגיה. ההבנה המשותפת הזו אפשרה לצוות לשתף פעולה באופן אפקטיבי יותר בבניית הנימוקים בעד השימוש ב-RPA לצרכים עסקיים וכן את התוכנית ליישום היוזמה.

## הוכחת היתכנות

מצויד במחקר המוצג בנייר העמדה, צוות הביקורת הפנימית החל לעבוד על הוכחת היתכנות כדי לקבוע את הערך הפוטנציאלי של ה-RPA בכל הנוגע לתוכנית הביקורת בנושא המסופים. התהליך כלל את קביעת השלבים המתאימים להמרה ל-RPA והצגת תחומי ההתייעלות הפוטנציאליים. הצוות זיהה שלבים הכוללים בדיקות הבטחת איכות של המערכת ובדיקות אחרות הקשורות למערכת מול שלבים תצפיתיים שלא יהיו מתאימים לאוטומציה.

בנוסף, חברי הצוות בנו אומדן של רמת המאמץ הנוכחית הנדרשת כדי להשלים את שלבי הביקורת, ודירגו את השלבים בהתאם דרגות קושי - קל, ממוצע או קשה. שלבים שהוגדרו כממוצע או קשה לביצוע סומנו כמועמדים פוטנציאליים להעברה ל-RPA. שלבים הקשורים לעסקאות או שלבים המחייבים את המבקר להיכנס למספר מערכות סומנו כמועמדים האופטימליים להעברה ל-RPA. ככל שהשלב הוגדר כקשה יותר לביצוע וכצורך יותר זמן, כך הוא סומן כמועמד טוב יותר ל-RPA. הניתוח - שהציג תמונה של החיסכון בזמן הפוטנציאלי שניתן לכימות - אישר בסופו של דבר שיש ל-RPA את הפוטנציאל להגדיל באופן משמעותי את היעילות של ביקורת פנימית בנושא טרמינלים. הניתוחים והדיונים המשותפים בתהליך הוכחת ההיתכנות נתנו אור ירוק להמשיך לתוכנית קידום הפרויקט ולפיתוח תוכנית פיילוט.

## קידום יוזמת ה-RPA

מצויד בהוכחת ההיתכנות, ראשי הביקורת התחילו לקדם את יוזמת ה-RPA בקרב בעלי העניין העיקריים. קידום היוזמה היה שלב חשוב, מאחר שמשאבי הזמן הנדרשים כדי ליישם RPA באופן מלא עלולים להשפיע על כיסוי הביקורת בטווח הקצר ולחייב השקעות פיננסיות בהמשך.

בעלי העניין העיקריים במאמץ קידום היוזמה כללו את היררכיית הדיווח של הביקורת הפנימית (כלומר ועדת הביקורת וסמנכ"ל הכספים). נוסף על כך, היה חשוב מאוד לקבל תמיכה ממחלקת מערכות המידע ב-YRCW, מפני שהתועלות הצפויות מהטרנספורמציה הזו מחייבות גישה ישירה לנתונים של החברה.

על מנת להשיג את הסכמת ותמיכת בעלי העניין, היה על צוות הביקורת הפנימית לגרום להם להבין הן את התועלות בטווח הארוך והן את השפעות יוזמת ה-RPA בטווח הקצר. מאמצי קידום היוזמה כללו פגישות קצרות כדי להסביר את ה-RPA ויתרונותיו לבעלי העניין. רוב בעלי העניין הכירו את RPA בהקשר של תהליכים עסקיים, אך לא העלו על דעתם את יתרונותיו בהקשר של תהליכי הביקורת הפנימית בנושא המסופים. במהלך הפגישות הציג צוות הביקורת הפנימית את התוצאות של הוכחות ההיתכנות ואת הצעת הערך הניתנת להשגה מיישום ה-RPA. מאחר שנייר העמדה והוכחת ההיתכנות הציגו את ערכה של היוזמה בצורה חותכת, קידום היוזמה היה בעצם פעולה פורמלית בלבד ויוזמת ה-RPA קיבלה תמיכה ואישור להתקדם ללא תנאים.

### מיומנויות בפיתוח בוטים

התחלת השימוש ב-RPA אינה מחייבת מיומנויות מיוחדות. רוב כלי ה-RPA כוללים סוגים של ממשק משתמש גרפי טיפוסיים עם פונקציות של point and click המסייעות למשתמשים מתחילים להתחיל מיד.

כל בעל ניסיון בתוכנות בסיסיות כמו אקסל יכול לפתח בוטים בסיסיים. אולם ידע טכני, כמו כתיבת קוד, יכול להיות שימושי מאוד כשמבקשים לפתח בוט מתוחכם יותר, במיוחד אם יוזמת ה-RPA צפויה להיות מורכבת יותר.

כלים מתקדמים יותר של RPA מאפשרים גם כתיבת קוד בהתאמה אישית באמצעות SQL או בשפות קוד אחרות. אנשים בעלי מומחיות כאנליסט עסקי או בכתיבת קוד יכולים להוסיף ערך משמעותי לפרויקטים לפיתוח בוטים מורכבים.

## הפיילוט של הבוט

השלב האחרון בהוכחת ההיתכנות כלל פיתוח של בוט כפיילוט. הפיתוח כלל כמה שלבים:

- זיהוי כלי RPA מתאים.
- בחירת שלב בתוכנית הביקורת הפנימית בנושא המסופים כמועמד מתאים ל-RPA.
- פירוט המשימות הנדרשות כדי להשלים את שלב הביקורת.
- פיתוח הלוגיקה של בוט ה-RPA.
- בדיקה, איתור וטיפול בבעיות ושכלול הבוט.
- הדגמת ביצועי הבוט.

המחסום הראשון העומד בפני מחלקות הביקורת הפנימית בבואן להפעיל פיילוט של RPA, הוא בחירת כלי ה-RPA. והשכנוע לבצע השקעה פיננסית בכלי שייתכן שלא יוסיף ערך הוא לא דבר של מה בכך, במיוחד עבור מחלקות קטנות של ביקורת פנימית בעלות משאבים פחותים. למרבה המזל, כלי RPA מבוססי אינטרנט זמינים ממספר ספקים המציעים גרסה בסיסית המאפשרת למשתמשים לנסותם בחינם. מחלקת הביקורת הפנימית של YRCW בחרה באפשרות זו עבור הפיילוט שלה. לאחר בחינה והתנסות במספר כלים חינמיים, היא בחרה כלי אחד עם מוניטין מבוסס שנראה כמסוגל להתאים לפיילוט.

הצוות בחר שלב ביקורת בפיילוט שכלל מספר משימות ביקורת ידניות: כניסות למספר מערכות, ניווט למסכי אפליקציה שונים, ליקוט רשימות ושדות נתונים ספציפיים כדי לזהות מדגם של פריטים לבדיקה, וכן ניתוח הנתונים המדגמיים בגיליון אלקטרוני כדי לקבוע את תוצאות הבדיקה. נוסף על כך, בהתחשב בתחומי ההתייעלות המשופרת הצפויה מהבוט, המבקרים יכלו להחליף דגימה שיפוטית בבדיקות של כלל האוכלוסייה.

אחרי שהגדיר את גישת הבדיקה החדשה, צוות הביקורת החל בפיתוח הבוט. התהליך כלל רישום של כל אחת ממשימות הביקורת, שלב אחרי שלב, בכלי ה-RPA. במובנים רבים, הפיתוח היה דומה להגדרות של מאקרו בתוכנת גיליון אלקטרוני - המבקרים לכדו משימות, כגון קליקים בעכבר, הקשות בקלידים, שמות משתמשים וסיסמאות, ואטמטו אותן באמצעות הכלי.

## תוצאות הפיילוט

פרויקט הפיילוט הפיק תובנות בעלות ערך רב אודות פיתוח בוטים, כגון המורכבויות בתהליכים שאנשים לוקחים כמובנות מאליהן בעת ביצוע בדיקות. לדוגמה: הצוות הכיר בערך שבגישה ישירה לנתונים לעומת גישה עקיפה המתבצעת באמצעות לכידת מסך. חלק מהשלבים בתהליך פיתוח הבוט כללו השגת גישה למסכי מעבד מרכזי ו"גירוד" הנתונים הנדרשים מהם. אולם מסכי אפליקציה מסוימים מכילים רק תמונות ואין בהם נתונים של ממש (כלומר גרפיקה עבור ממשק המשתמש).





### תחשבו לפני שאתם מבצעים אוטומציה

אין זה רצוי שמבקרים פנימיים יתחילו בפרויקטים לפיתוח בוטים בפזיזות או ללא תכנון ותמיכה ראויים. מחלקות ביקורת פנימית השוקלות יישום של RPA צריכות לקחת בחשבון את הנקודות הבאות:

- יש לבצע הוכחות היתכנות (לרבות פיילוט) כדי לוודא שהמהלך מציע ערך גבוה מספיק ומצדיק את יוזמת ה-RPA.
- אפשר להשתמש בכלים בסיסיים חינמיים ובמיומנות בסיסית כדי להתחיל את הפרויקט, אבל כלים מתקדמים יותר ויכולת כתיבת קוד עשויים להיות חיוניים כדי להשלים את הפרויקט.
- גישה ישירה לנתונים מוסיפה ערך מעריכי.
- שותפות עם מחלקת מערכות המידע או עם מחלקות אחרות המשתמשות ב-RPA מאפשרת לביקורת הפנימית למנף מומחיות בנושאים פנים-ארגוניים ולהקטין את הוצאות הפיתוח.
- האיכות והקיימות של התוכנית מחייבות פיקוח צמוד על ממשל ה-RPA.

אנשים מסוגלים "לקרוא" תמונות בקלות, אך לכלים של RPA יש יכולות קריאת תמונות ברמות שונות. הבוט של הפיילוט לא הצליח לזהות נתונים המוצגים כתמונה (אינפוגרפיקה), וזה גרם לבעיות בשלב זה של משימות הביקורת. בכל פעם שהבוט נתקל במשימה כזו (זיהוי נתונים בתוך אינפוגרפיקה) הוא נכשל או נתקע, והמצב חייב התערבות ידנית על מנת להשלים את המשימה. כאשר הבוט השיג גישה ישירה לנתונים, הוא הצליח להמשיך בעיבודים של משימות הביקורת עד לסיומם. אולם בעת הפיילוט גישה ישירה לחלק מהנתונים לא היתה אפשרית.

כתוצאה מכך, הפיילוט של הבוט הפיק תוצאות חיוביות אך לא שלמות. משימת הביקורת שנבחרה עבור הפיילוט היא משימה שמבקר יכול להשלים באופן ידני בתוך שעה-שעתיים בדרך כלל. הבוט של הפיילוט השלים את המשימה בערך בתוך דקה - עד לנקודה שבה הוא נתקל באינפוגרפיקה שעצרה את פעולתו. בנקודה זו נדרש המבקר לבצע עיבודים ידניים במשך 20 דקות נוספות.

למרות העבודה הידנית, האוטומציה סיפקה חיסכון משמעותי בזמן. לו קיבלה הביקורת גישה ישירה לנתונים, הבוט היה מצליח להשלים את מלוא שלב הביקורת ביעילות משופרת עוד יותר - בשתי דקות או פחות. גילוי זה הבליט את החיוניות של גישה ישירה לנתונים לצורך פיתוח בוטים לקראת יישום עתידי של ה-RPA. הודות לתמיכה הנוספת שהוענקה על ידי מחלקת מערכות המידע, צוות הביקורת הפנימית השיג בסופו של דבר גישה ישירה לנתונים הנדרשים והשלים את הפיילוט של הבוט.

צוות הביקורת הפנימית ביצע השוואה בין תוצאות העבודה של הבוט לבין תוצאות העבודה הידנית על מנת לוודא תוצאות עקביות. הצוות מצא שתוצאות הפיילוט היו באיכות גבוהה יותר (בדיקה מלאה של אוכלוסייה מול בדיקה מדגמית) וביעילות גבוהה יותר באופן משמעותי (כ-90 שניות מול שעה-שעתיים להשלמת משימת הביקורת).

## איך ממשיכים

לאחר תיקוף הפוטנציאל של הבוטים להגדלת יעילות הביקורת הפנימית, מחלקת הביקורת הפנימית של YRCW מוכנה להשיק תוכנית פורמלית ליישום ה-RPA. התוכנית מתעדפת משימות ביקורת עבור פיתוח בוטים ותשקול את השלכות ממשל ה-RPA. התוכנית תתייחס להרבה מהשיקולים הנדרשים בכל סביבת פיתוח IT, לרבות סטנדרטים של פיתוח, ניהול שינויים ובדיקות משתמש.

הנהגת הביקורת הפנימית גם תצטרך להחליט על כלי ה-RPA שיהיה מתאים לאחר הפיילוט, ובמידת הצורך לגבש נימוקים עסקיים שיצדיקו ויבטיחו מימון לפרויקט. כמו כן, עליה לשקול כיצד לפרוס מחדש את צוות הביקורת לאחר שהיעילות המשופרת של תהליך ה-RPA יתחיל להבשיל.

## כלי שינוי

כמו רוב הכלים הטכנולוגיים, כלי ה-RPA אינו פתרון של one-size-fits-all. מודל היישום שלו ופוטנציאל הערך שלו יהיו שונים בכל ארגון וארגון. בסופו של דבר, הערך שב-RPA הוא באיטמוט של פעילויות סטנדרטיות המבוצעות בתדירות גבוהה.

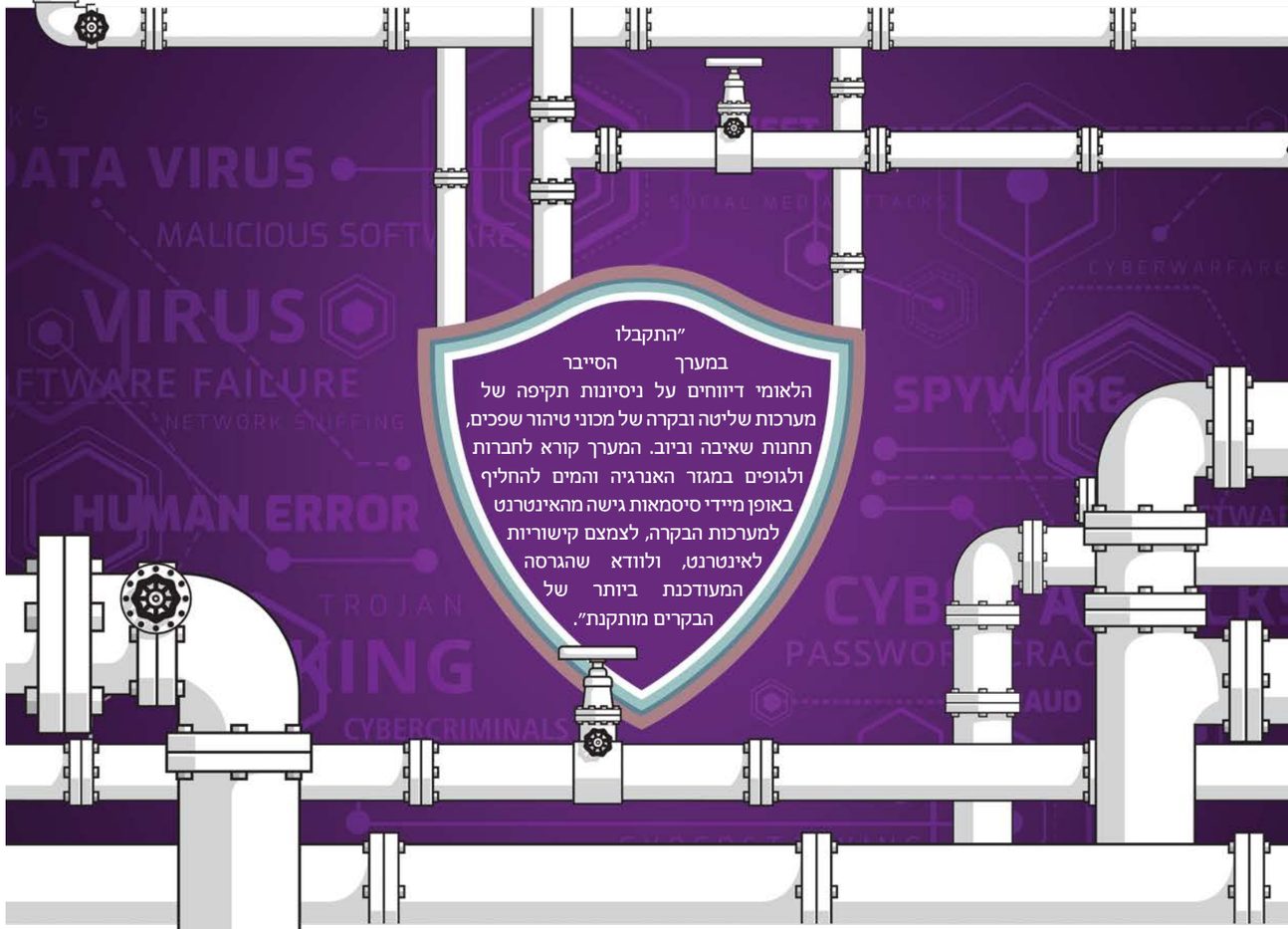
**למחלקות ביקורת פנימית שתוכניות הביקורת שלהן מכילות התקשרויות משמעותיות שחוזרות על עצמן להבטחת ציות, תהיה הצדקה טובה יותר ליישום ה-RPA מאשר למחלקות שתוכניותיהן מכילות שיעור גבוה יותר של פרויקטים תפעוליים ושל שירותי ייעוץ.**

עבור מחלקות ביקורת פנימית שבהן יישום ה-RPA הוא הגיוני - זה יכול לשנות את שם המשחק

*This article was reprinted with permission from the April 09, 2020 issue of Internal Auditor magazine, published by The Institute of Internal Auditors, Inc., and has been translated from English to Hebrew."

# מהם סיכוני OT בארגון, ואיך נדרש לבקר אותם?

מאת: רפאל גולוב | CIA, CIRSC, CISA CISM,
ניהל את יחידת הגנת הסייבר של הרשות הממשלתית למים ולביוב




תקיפת תשתיות מים וביוב, כפי שתוארה בפרסום, בוצעה על מנת לשבש את הספקת המים לצרכנים ואת הקליטה והעיבוד של השפכים. כלומר, התקיפה כוונה כנגד מה שמכונה בשפה המקצועית "טכנולוגיה תפעולית" (TECHNOLOGY OPERATIONAL – OT).

מטרת מאמר זה היא לספק למבקר הפנימי, למנהלי הסיכונים ולהנהלה בארגון, אשנב לסיכונים האפשריים הנובעים מהשימוש ב"טכנולוגיה תפעולית" (OT) בארגונים, וכן להמליץ על כיווני ביקורת כדי לוודא שהרציפות התפקודית של הארגון לא נפגעת.





בהתאם להגדרה שמציע מכון המחקר GARTNER,

**"טכנולוגיה תפעולית" היא "חומרה ותוכנה אשר מזהות או גורמות לשינוי באמצעות ניטור ו/ או בקרה ישירים על ציוד תעשייתי, נכסים, תהליכים ואירועים".**

## טכנולוגיה תפעולית כוללת שתי קבוצות משנה עיקריות:

**מערכות בקרה תעשייתיות**

ICS - INDUSTRIAL CONTROL) (SYSTEMS
מסוגים שונים, שתהליכי הייצור במפעלים תעשייתיים מושתתים עליהן. מערכות אלו משמשות לניטור ובקרה וכן בגופי תשתיות: תחנות כוח, מתקני מים וביוב, תשתיות גז ודלק, מערכות תחבורה, נמלים ועוד.

**מערכות ניהול לבניין**

BMS - BUILDING MANAGEMENT) (SYSTEMS). מדובר במשפחה רחבה של רשתות ומערכות, כגון מיזוג, תאורה, ביטחון ובטיחות, מעליות ועוד.

> "OT עלול להביא להשלכות בטיחותיות וסביבתיות מחרידות. פקודה לפרוק מכל אמוניה עלולה לגרום למאות הרוגים."

## משמעות התממשות איומי הסייבר בסביבת ה-OT

ההבדל המהותי בין מערכות ה-IT (Informational Technology) לבין OT הוא בכך שבעוד שהמערכות מהסוג הראשון מאחסנות, מעבדות ומפיצות מידע ברמת ערכיות שונה, מערכות ה-OT מנהלות תהליכים פיזיים.

אירוע סייבר בסביבת ה-IT בדרך כלל עלול לפגוע בסודיות, בשלמות ובזמינות המידע הארגוני ולגרום לנזק כלכלי, תדמיתי ורגולטורי. לעומת זאת, אירוע סייבר בסביבת ה-OT עלול להביא להשלכות חמורות בהרבה. המונחים שבהם נהוג להשתמש בסביבת ה-OT הם יציבות התהליך (RELIABILITY), איכות הייצור, בטיחות העובדים (SAFETY) ונזק סביבתי (מומלץ לעיין במסמך "ניהול סיכוני סייבר בסביבת OT - מדריך לדירקטוריון" שפורסם בחודש מרץ 2020 על ידי מערך הסייבר הלאומי).

**פגיעה ביציבות התהליך עלולה לשבש או אפילו להפסיק לחלוטין שירות חיוני, כגון הספקת החשמל**

(לדוגמה, התקיפה הרוסית בתחנת כוח אוקראינית בשנת 2015). כמו כן, אירוע סייבר בסביבת ה-OT עלול להביא להשלכות בטיחותיות וסביבתיות מחרידות. כך למשל, פקודה לפרוק מכל אמוניה עלולה לגרום למאות הרוגים.

תקיפת סייבר במערכות ניהול של בניין עלולה לגרום לשיבושים תפעוליים משמעותיים. כך לדוגמה, השבתת מערכת מעליות במגדל משרדים תקשה על עובדים ולקוחות להגיע ליעדם. השתלטות על מערכת בקרת כניסה תאפשר לתוקף להכניס גורמים לא מורשים למתחם לצורך פעילות זדונית.

כתוצאה מכך, אם הארגון עושה שימוש בטכנולוגיה תפעולית, המבקר הפנימי בארגון מחויב לוודא שתהליך ניהול הסיכונים בהקשר הזה מתנהל בצורה נאותה.

## חולשות הגנת סייבר אופייניות בתחום ה-OT

מערכות בקרה תעשייתית רבות סובלות מחולשות הגנת סייבר חמורות. המשמעותיות שבהן:

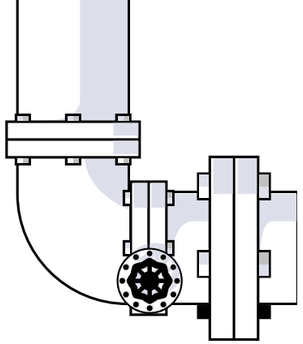
1. חלקן פותחו והוטמעו לפני תחילת "עידן הסייבר" ולכן עושות שימוש ברכיבים, בתוכנות ובפרוטוקולי תקשורת שיש בהם חולשות הגנת סייבר מובנות. לדוגמה, פרוטוקול תקשורת נפוץ בסביבת ה-OT הוא MODBUS שפותח בשנת 1979. ניצול החולשות המובנות בפרוטוקול זה מאפשר לתוקף לבצע תקיפה מסוג man-in-the-middle לצורך שיבוש תהליכי הייצור, בעוד שמפעיל המערכת יוזן במידע כוזב בנוגע לתקינות התהליך (לדוגמה: "Man-In-The-Middle Attack Against Modbus TCP illustrated with Wireshark" Gabriel Sanchez SANS Institute).
2. בחלק מרשתות הבקרה חסרה סגמנטציה, כלומר לנוזקה או לתוקף שיצליח לחדור בנקודה כלשהי לרשת יהיה קל להגיע לכל יעד בתוכה (לדוגמה: Top 10 Cybersecurity Vulnerabilities and Threats for Critical Infrastructure and SCADA/ICS).
3. עמדות מפעיל רבות (HMI - Human Machine Interface) עדיין מריצות מערכות הפעלה מיושנות מסוג XP WINDOWS ששדרוגן יגרום לשיבוש פעילות תוכנת הבקרה.
4. מערכות בקרה תעשייתית נועדו במקור לשמש ישויות המופרדות הן מרשת המחשוב הארגונית והן מרשת האינטרנט. במהלך השנים, כתוצאה מצרכים עסקיים ותפעוליים וכחלק מתפיסת המהפכה התעשייתית הרביעית, INDUSTRY 4.0, חוברו רשתות בקרה תעשייתית רבות הן לרשת הארגונית (IT) והן לרשת האינטרנט. עם זאת, לעיתים במערכות בקרה תעשייתיות לא בוצעה הקשחת רכיבים כנדרש (בקרים, מתגים, עמדות מפעיל), וכן לא קיימות יכולות ניטור הרשת (IDS - Intrusion Detection System) או בקרת הגישה לרשת (NOC או NAC).
5. היעדר ממשל OT נאות בארגון. במפעלים רבים, בשונה מהנורמה הקיימת באשר ל-IT, לא קיים מיפוי תהליכי עבודה ונכסים מפורט באשר לסביבת ה-OT, תפעולה ואחזקתה. למשל, לא ברור באילו בקרים ופרוטוקולי תקשורת נעשה שימוש, או לא ידועה הקישוריות הקיימת בין רשתות הבקרה לרשת הארגונית ולאינטרנט. יותר מזה, ייתכן כי הארגון לא מודע לחיבור הספקים לרשתות הייצור שלו לצורך תמיכה וניטור.
6. מודעות הסגל התפעולי וגורמי שרשרת האספקה לסיכוני הסייבר הנלווים לשימוש בטכנולוגיה תפעולית יכולה להיות נמוכה מאוד, מפני שגם אנשי אבטחת המידע בארגון מגבילים את תחום עיסוקם בסביבת ה-IT בלבד.

## הבסיס הנורמטיבי להגנת סייבר על מערכות ה-OT

בשנים האחרונות בישראל (ובעולם) חל גידול משמעותי בנפח מעורבות הרגולטור בנושא הגנת הסייבר בתחום ה-OT בארגון. כך, לדוגמה, אגף שוק ההון, ביטוח וחיסכון במשרד האוצר פרסם בשנת 2016 חוזר בנושא ניהול סיכוני סייבר בגופים מוסדיים שבו נכתב: "הערכת הסיכונים תתייחס בין היתר למערכות OT ולסביבות פיתוח ובדיקות, העשויות להכיל מידע רגיש או לגלם חשיפות למערכות הגוף המוסדי כולו".

המשרד לאיכות הסביבה פרסם בינואר 2020 מדריך סייבר בנושא "עמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה". מדריך זה כולל דרישה לניהול נאות של סיכוני הסייבר בסביבת ה-OT ברשימת התנאים לקבלה ותיקוף מחדש של היתר הרעלים.

למשרד האנרגיה ולרשות הממשלתית למים ולביוב קיימים נהלים מחייבים שקובעים סטנדרט הגנה נדרש בנוגע לרשתות הבקרה של יצרני החשמל וספקי המים והביוב.



> "מתקפות הסייבר הולכות ומתפתחות גם לטכנולוגיות תפעוליות שמשמשות לניטור ובקרה של תהליכים תפעוליים, תעשייתיים, יצרניים ופיזיים בארגון"





## המלצות לביקורת ניהול סיכוני ה-OT בארגון

כצעד ראשון, יש לקבל הבנה בסיסית בנוגע לשימוש בטכנולוגיות תפעוליות בארגון, ובכלל זה:

1. הכרת היקף השימוש של הארגון המבוקר ב- ICS Industrial Control Systems וב- BMS Building Management Systems.
2. הבנת רמת הקריטיות של התהליכים המנוהלים על ידי המערכות הללו ורמת הסיכון השורשי הגלומה בתהליכים הללו.
3. מיפוי בעלי התפקידים הרלוונטיים לתפעול מערכות אלו ולמנגנוני הגנת הסייבר המוטמעים בהן. מומלץ לברר ולבחון האם קיים ניהול נכסים נאות: מיפוי רכבים ותרשימי רשתות, פירוט קישורים הדדיים וחיצוניים, רשימת גורמי שרשרת אספקה רלוונטיים, רשימת מורשים לגישה מרחוק, נהלים לעדכון רכיבים, הקשחה ועוד.
4. בחינה האם מתקיים תהליך סדור לניהול סיכוני סייבר בסביבת ה-OT, ובחינה האם קיימת תפיסה לניהול אירוע סייבר ברשתות ה-OT ולהתאוששות ממנו. חשוב מאוד לוודא כי תפיסה זו עולה בקנה אחד עם התפיסה הארגונית הכללית להמשכיות עסקית.
5. בחינה האם נערך סקר סיכוני סייבר בסביבת ה-OT, ואם בוצע - נדרש לבדוק מהו סטטוס יישום ההמלצות שעלו בו לשיפור רמת הגנת הסייבר הכוללת בארגון (בדגש על התחומים המשותפים לסביבת ה-IT).
6. בחינה האם סגל התפעול מודע לסיכוני הסייבר האפשריים.

לאחר שלמבקר הפנימי ישנה הבנה בסיסית בנוגע לשימוש בטכנולוגיות תפעוליות בארגונו, מומלץ לתכנן ביקורת ייעודית מקיפה בנושא, בדגש על העמידה ברגולציה הרלוונטית. מומלץ להיעזר במתודולוגיות ייעודיות (הנגזרות לרוב מהנחיות המפורטות במדריך NIST Special Publication 800-82 Revision 2"Guide to Industrial Control Systems (ICS) Security") ולהשתמש בכלים טכנולוגיים תואמים שחלקם שונים מסביבת ה-IT. כך למשל, בסביבת ה-OT לא מקובל לבצע סריקות רשת אקטיביות, ולכן מנתחים לרוב את הקלטת התעבורה במצב "offline".

## לסיכום

מתקפות הסייבר הולכות ומתפתחות גם לטכנולוגיות תפעוליות שמשמשות לניטור ובקרה של תהליכים תפעוליים, תעשייתיים, יצרניים ופיזיים בארגון. לכן על הארגון והמבקר הפנימי להכיר ולזהות את השוני ואת ההשפעות של איומי סייבר על הסביבה הפיזית לעומת סביבות אחרות, לדעת מהם הסיכונים ולהבין איך לנהל אותם ולהתגונן מפניהם.


# פורום
## "שולחן עגול"
## למבקרים פנימיים ראשיים

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

**להרשמה** למפגש שמועדו יקבע בקרוב
יש לפנות ל**אינה גולדרביטר**
לשכת המבקרים הפנימיים בישראל
**טלפון: 03-5116617 | office@theiia.org.il**

* החברות בפורום מוגבלת למבקרים פנימיים ראשיים בלבד. בפורום כ- 100 חברים המשמשים כמבקרים פנימיים ראשיים בארגונים המובילים בישראל.

# לכל מתקפה תשובה

## הפרקטיקה של ניהול אירועי סייבר

מאת: רם לוי | מייסד ומנכ"ל קונפידס

באוקטובר 2016 הותקפה חברת תשתית ה-DNS האמריקאית DYN במתקפת מניעת השירות הגדולה בהיסטוריה. ההתקפה בוצעה על ידי עשרות אלפי רכיבי IoT, והאירוע השפיע על עשרות שירותים ובהם כאלה המסופקים על ידי חברות כמו Amazon, PayPal, Twitter, Netflix, Soundcloud, Airbnb, Reddit. אחת הסיבות המרכזיות שבעטיין החברה הצליחה לטפל באירוע הזה בתוך שעות ספורות הייתה מוכנות מראש. לדבריהם, "אנו מתאמנים ומתכוננים לתרחישים מסוג זה על בסיס קבוע. אנו מתרגלים תסריטים מתגלגלים (playbooks) ועובדים בשיתוף פעולה עם גורמים מקצועיים כדי להתמודד עם תרחישים כאלה". זו דוגמה נדירה בנוף מתקפות הסייבר שבה הארגון המותקף מצליח לבלום התקפה ללא נזק משמעותי, הודות למוכנות מראש.

**מרבית התקיפות שמצליחות תופסות את הארגונים המותקפים עם המכנסיים הווירטואליים למטה, מה שגורר השלכות חמורות ביותר, בעיקר מבחינה עסקית.**

דוגמה לכך היא במקרה של התקיפה שביצעה צפון קוריאה על Sony Pictures. בין השלכות האירוע ניתן למנות את התפטרות מנכ"לית החברה, איימי פסקל, עלות של למעלה מ-41 מיליון דולר בשיקום ה-IT של הארגון, תביעות ייצוגיות והסדר טיעון עם עובדי החברה שהתכתבויות פנימיות שלהם נחשפו בהתקפה. למרבה הצער, Sony Pictures רחוקה מלהיות לבד בסירת אי-המוכנות למתקפת סייבר.

מקרה נוסף הוא של המתקפה הרוסית נגד אוקראינה, הידועה בשם NotPetya, מתקפה שהתפשטה לנכסים הדיגיטליים של החברות הגדולות בעולם והפכה להיות המתקפה היקרה וההרסנית בהיסטוריה. המתקפה פגעה בעשרות חברות בין-לאומיות מהגדולות בעולם, כגון Merck, Mondelez, DHL, DLA Piper וחברת הספנות הדנית הגדולה בעולם A.P. Moeller Maersk. נשיא חברת הספנות, שהנזק שהסבה לה המתקפה נאמד ביותר מ-300 מיליון דולר, אמר בפורום הכלכלי העולמי שהחברה הייתה "בינונית בכל הקשור להגנת הסייבר, בדיוק כמו חברות רבות אחרות... זו הייתה קריאת השכמה עבורנו לא רק להשתפר, אלא להפוך את הסייבר ליתרון תחרותי שלנו... הגיע הזמן להפסיק להיות תמימים בנוגע לנושא להגנת הסייבר... התלות בדיגיטל הולכת וגדלה, ומכאן הדחיפות הגבוהה... לא ניתן עוד להסתמך רק על חוסן אנושי".





## על סיכוני סייבר וארגונים

כל ארגון חשוף לסיכוני סייבר. בתחום הזה אין חסינות. בשנים האחרונות, ובחודשים האחרונים בפרט, אנו עדים לעלייה דרמטית בכמות תקיפות הסייבר ובאיכותן. ניתן לייחס מגמה זו להשפעות מגפת הקורונה שהאיצה את העבודה מרחוק, וכפועל יוצא הגדילה את משטח התקיפה הפוטנציאלי. בהקשר הישראלי - גם המתיחות הגוברת עם איראן מעלה את סיכון הסייבר של חברות ישראליות.

עם התפתחות מרחב הסייבר והתלות בתפקודו התקין, על ארגונים להיערך באופן אחר ולהתייחס לסיכוני סייבר כחלק חשוב ועקרוני מתהליך ניהול הסיכונים שלהם. היות שהסיכונים הם רבים ומגוונים וקצב התפתחות וגילוי החולשות הוא מהיר מאוד (כ-300 חולשות חדשות מתגלות בכל שבוע בממוצע), מדובר בתהליך מורכב שצריך להיעשות באופן שוטף.

הדבר חשוב במיוחד בגלל הסיבה הבאה: אירוע סייבר הוא אירוע שנגרם כתוצאה מתוקף (לרוב חיצוני) שמפתיע את הגוף המותקף. הדבר מייצר מצב הדומה למלחמה. מתקפת סייבר מכניסה את הגורם המותקף לתנאים של "ערפל קרב". פירוש הדבר הוא שבמקרים רבים לא ברור למותקף מה בדיוק התרחש, מיהו התוקף ומה הוא מבקש, ולכן כמעט תמיד הטיפול באירוע יתבצע בתנאים של מידע חסר ועלול לתפוס את הארגון במצב של הפתעה. משמעות הדברים היא שכל ארגון נמצא בסיכון משתנה לחוות אירוע סייבר, ולכן כל ארגון זקוק לתוכנית תגובה לאירוע סייבר המותאמת לו.

כאשר אירוע מתרחש במרחב הסייבר, הוא מתגלגל בקצב כה מהיר עד שרובנו איננו יכולים לתפוס זאת. לכך מתווספת העובדה שאירוע סייבר מאופיין בחוסר ודאות, דבר שמגביר את רמות החרדה ומשפיע מבחינה פסיכולוגית על יכולת קבלת ההחלטות.

ההשלכה החמורה ביותר של אירוע סייבר היא אובדן עסקאות בעקבות אובדן האמון של הלקוחות. שיקום קשר עם הלקוח הוא דבר שצורך זמן וכסף רב. בהקשר הזה קיים מתאם בין משך זמן הגילוי של ההתקפה לעלויות השיקום. עלויות השיקום של סקטורים תחת רגולציה (כגון בנקאות, ביטוח ורפואה) אף גבוהות יותר, בין היתר בגלל חובת דיווח, קנסות רגולטוריים, והחשיבות הקריטית של שיקום המוניטין, המצריך עלויות גבוהות במיוחד.

רגע, עוד לא סיימנו עם החדשות הרעות. חברות רבות מתקשות במציאת אנשי מקצוע טובים בתחום הגנת הסייבר, ולכן נאלצות להשקיע כספים רבים יותר לאחר שאירוע התרחש במקום למנוע אותו או לכל הפחות לצמצם את האפשרות שיתחולל.

**אבל יש גם חדשות טובות. פגיעה קשה ממתקפת סייבר איננה גזרת גורל. בארגונים שבהם הסדירו מבעוד מועד את הטיפול באירועי סייבר, מינו גורם אחראי לנושא, השקיעו בהעלאת המודעות, תרגלו באופן קבוע תרחישים ומענה להם ונקטו אמצעים רלוונטיים נוספים – עלויות הטיפול והשיקום נמוכות יותר.**

> מתקפת סייבר מכניסה את הגורם המותקף לתנאים של "ערפל קרב"

## מכאן עולות שתי מסקנות:

1. אפשר להקטין את זמן הגילוי והתגובה למינימום האפשרי. עם זאת, חשוב לזכור שבניית יכולת ניטור טובה אינה זהה לכושר תגובה איתן.
2. אפשר להגדיל את כושר התגובה והחוסן הארגוני, בעיקר סביב היבטים שאינם קשורים באופן מובהק לטכנולוגיה, כגון יח"צ, דוברות, ביטוח, עבודה מול רשויות, הרתעה ומודיעין, כל זאת במטרה לצמצם את הסיכונים והחשיפות לאחר אירוע סייבר למינימום האפשרי.

אי לכך, יש לדאוג מבעוד מועד לתוכנית (ארגונית) של מענה אפקטיבי מוקדם ככל הניתן למתקפה. לכן המפתח להתמודדות מבוסס על כלל האצבע שמלמדים בצבא: תרגול. קשה באימונים, קל בקרב. גם בסייבר - תרגול ומדידה הם המפתח למוכנות לתקיפה.

## אך מהו אותו מענה?

בהכנה להתמודדות עם מתקפת סייבר קיימים חמישה שלבים: זיהוי נכסים להגנה, הגנה על הנכסים, איתור מתקפות, תגובה והתאוששות.

באירוע "מוצלח", שלבי התגובה והתאוששות נחלקים לשניים: תגובה טקטית, שלרוב תהיה טכנולוגית, ותגובה אסטרטגית, שבה יידרש הארגון כולו להגיב, מהדירקטוריון ומטה.

שלבי התגובה לאירוע סייבר מוגדרים במספר מדריכים ותקנים של ארגונים, אם כי אני, באופן אישי, מוצא שבנק ישראל עשה את העבודה הטובה ביותר בתחום במסמך "ניהול בנקאי תקין 361":

### זיהוי (DETECTION)

1 בירור ראשוני לגבי קיומו של אירוע סייבר וגיבוש מהיר ככל האפשר של דפוס הפעילות הדרוש בארגון לשלב הבא אחריו.

### ניתוח (ANALYSIS)

2 בירור מקיף ומעמיק, ככל האפשר באותה נקודת זמן, לגבי אירוע הסייבר, לצורך: (א) קבלת החלטות ברמה האופרטיבית, (ב) גיבוש רשימת חלופות של דפוסי פעולה אפשריים לבלימת התקיפה, (ג) החלטה על דרך הפעולה העיקרית לשלב הבא של הכלה.

### הכלה (CONTAINMENT)

3 (א) השגת שליטה ראשונית באירוע לצורך הכלתו ועצירת החמרתו והשגת יעדיו, (ב) ביצוע תהליך השתלטות על מהלך התקיפה, וביטול או מזעור של וקטור הנזק לארגון.

### הכרעה (ERADICATION)

4 נטרול רכיבי התקיפה שמצויים במערכות של הארגון, תוך שאיפה לבטל או למזער, ככל שניתן, את הנזק שכבר נגרם.

### התאוששות (RECOVERY)

5 חזרה לרמת התקינות של פעילות הארגון טרום אירוע הסייבר, וחזרה לתפקוד מלא של כל פעילות שהושבתה, הוגבלה או הופרעה על ידי האירוע.



בפרקטיקה, שלבים אלה צריכים להיות מעוגנים בנוהל שאושר על ידי ההנהלה (ואף הדירקטוריון) ומתורגל לפחות פעם בשנה. עקרונות לנוהל כזה יכולים לכלול:

1. מעבר משגרה של "עסקים כרגיל" לשגרת חירום, הכוללת מחזוריות של תכנון, הכנה, ביצוע והערכה של התגובה לאירוע.
2. הקמת צוות ניהול משבר וחדר מצב, כולל מבנה של צוות תגובה רזה המאפשר פעולה מהירה.
3. קביעת שעון לחימה, הכולל זמני עדכון, תכנון והחלטות הנהלה.
4. מתן סמכות לדרגים בשטח ל"יוזמות ממושמעות", כדי לאפשר התאוששות מהירה על פי הכוונה של ההנהלה.
5. תוכנית לשמירת הכשירות הארגונית להתאוששות ממשבר סייבר.
6. הבנת הסביבה הרגולטורית וחובות הדיווח.
7. הגדרה והכשרה מראש של אדם אחד בחברה, שישמש כתובת לניהול משבר סייבר מול התקשורת.
8. תקשורת שקופה עם בעלי עניין מרכזיים, וכן בפניות והודעות לעובדים, לספקים, ללקוחות, ובעלי מניות.
9. רכישת פוליסת ביטוח סייבר. בהקשר הזה אביא את דבריו של שי סימקין, ראש תחום סייבר בקבוצת "האודן" העולמית: "הפייק ניוז הגדול ביותר הוא שהביטוח אינו מכסה דבר. מדובר באחד הביטוחים המשתלמים ביותר".

## החלטות מנכ"ל באירוע סייבר

כאשר אירוע סייבר מגיע עד לרמת המנכ"ל, יש מספר החלטות שכדאי שיקבל:

1. הכרזה על אירוע סייבר, כולל רמת החומרה שלו, והפעלת גופי ניהול רלוונטיים.
2. מה קרה? - נרטיב ארגוני אחיד.
3. הגדרות נחוצות - חומרת האירוע, דחיפות, המענה הנדרש, תחומי אחריות, שותפי סוד.
4. בירור חובת ההודעה לרגולטורים וגורמי אכיפה ולו"ז/סדר ההודעות.
5. אפיון הגורם התוקף (המערכת היריבה) והפעולות שיש לנקוט מולו.
6. עקרונות לניהול המשבר - קביעת אחריות חברי ההנהלה, מינוי צוותי חירום, הגדרת סמכויות, תקציבים וכו'.
7. עדכון ויידוע לקוחות - אופן הטיפול במשבר ומהן הפעולות להמשך.
8. צעדים שהמנכ"ל בעצמו הולך לבצע (כגון שיחות עם לקוחות, תקשורת, גורמים לאומיים וכו').
9. עקרונות דוברות ודיווח חיצוני.





## בואו נדבר הגנה - הצעה למודל הכנה ארגונית למשבר סייבר

אלה האתגרים שלאורם חברת קונפידס פיתחה מודל של הכנה ארגונית למשברי סייבר.

התוכנית, שמורכבת משלוש רמות בשלות, דואגת לכך שכל יחידה בתוך הארגון תהיה בשלה מספיק לנהל את ההיבטים תחת אחריותה.

המודל מסייע לגורמים העסקיים בארגון להתכונן למשבר, כל אחד בתחום שתחת אחריות, ומטרתו לסייע לכל יחידה בארגון לגבש את נוהלי החירום הפנימיים שלה ולהביא אותה לרמת בשלות בצורה שיטתית ובהתאם לנוהל התגובה התאגידי.

| Maturity Level | Basic | Advanced | Mature |
|---|---|---|---|
| Manual Contact information List | 1 | | |
| Unit Team membership (including backup and escalation) | 1 | | |
| Communication Plan | 1 | | |
| Unit representative at Situation Room | | 1 | |
| Required report (regulation, authorities, etc…) | | 1 | |
| SLA Definition (Customers, Suppliers) | | 1 | |
| Alternative Manual Documents | | 1 | |
| Alternative Side Systems | | 1 | |
| Critical process mapping | | 1 | |
| Unit BIA | | 1 | |
| Define the unit representative (that will communicate with other units) in crisis event (including backup) | | 1 | |
| Units War room (define the units war room in case of crisis and the equipment needed: Phone, Fax, Printer etc.) | | 1 | |
| Alternative Communication available (Fax, Printer, Gmail etc.) | | | 1 |
| Testing of communication system | | | 1 |
| Integration with Adjacent units in process (For receiving and transfer information, documents) | | | 1 |
| Unit indicate response Procedure | | | 1 |
| Emergency task tracking (responsible, monitoring, reporting) | | | 1 |
| Unit periodic drill | | | 1 |
| Procedure for moving to an alternative site | | | 1 |

איור 1: מטריצת המוכנות הארגונית של קונפידס

התהליך נעשה על פי השלבים הבאים:

**בסיסי** שלב זה כולל הגדרת גורמים חיוניים בכל יחידה לתגובה לאירוע, דרכי התקשורת איתם, וכתיבת נוהלי עבודה תומכים לאור הנוהל הארגוני.

**מתקדם** שלב זה כולל הגדרת חדר מצב יחידתי, ומיפוי התהליכים הקיימים העסקיים בכל יחידה וכוללים: ממשקי עבודה עם יחידות משיקות בארגון, מערכות תומכות וספקים, הגדרת התהליכים שיש להם צורך במתן מענה מיידי (הן בתהליכים חלופיים, הן במערכות והן בכוח אדם ואתר תומך), טפסים ידניים ומערכות חלופיות שיש לעבוד איתן בעת משבר.

**בשל** שלב הכולל תרגול של כל עקרונות העבודה, לרבות עם מערכות חלופיות, אינטגרציה עם יחידה אחרות, מעבר לאתר חלופי, ועדכון נוהלי עבודה קיימים לאור התרגולים.

## לסיכום

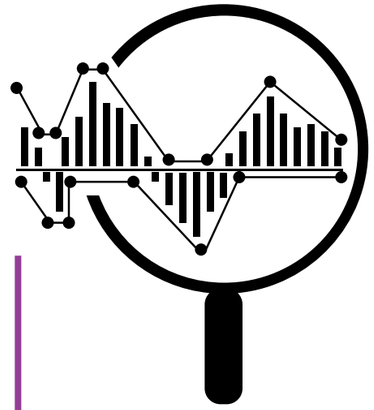
אירוע סייבר הוא אירוע מורכב, אפוף אי ודאות, ובמקרים מסוימים אף אירוע מכונן בחייו של ארגון.

כל חברה היא ייחודית ומיוחדת, הסיבות שהיא מותקפת (היגיון התוקף) הן יחודיות לה (ולפעמים לה בלבד), והפעולות שנעשו כדי למנוע אירוע ולהתמודד עימו לאחר שהתרחש תלויים, בין היתר, בתרבות הפנימית של הארגון, באנשים המאיישים את התפקידים השונים, ברגולציה, בקשב של ההנהלה, בתקשורת הבין-אישית הפנים ארגונית, בקשר עם גורמי חוץ במשאבים הקיימים ועוד.

משמעות המורכבויות הללו היא שבדיוק כמו אסטרטגיה עסקית, כל חברה זקוקה לתפיסה ייחודית של הגנת סייבר, שאותה תאמץ, תתרגל ותאתגר. במילים אחרות, בגזרת הסייבר כל ארגון זקוק לאימוץ אסטרטגיה כפולה: הגנה פרואקטיבית, מניעתית, והגנה רטרואקטיבית, בדיעבד. זו הדרך לנצח.

# ביקורת ANALYTICS – מאקסל ועד DATA SCIENCE

מאת: אסף קורן | CISA, CRISC, שותף בחברת סקאודיט בע"מ



**המידע הרב הנצבר ומנוהל בארגונים כולל נתונים על הזדמנויות עסקיות, תקלות, מעילות, יעילות תהליכים ועובדים, וכן נתונים נוספים. באמצעות שיטות וכלים המקובלים בעולם ה-Data Science ניתן להשתמש במידע העצום שנאגר גם לחיזוי בעולמות ה-Big-Data. אך עולה השאלה: האם גופי הביקורת הגיעו לעולמות אלו בביקורת ה-Analytics?**

סביבת מערכות המידע בארגונים הולכת והופכת מורכבת ותלויה במערכות מידע. בנוסף על שכבות מערכות המידע הסטנדרטיות המנהלות את התהליכים העסקיים המסורתיים (רכש, הכנסות, שכר, מלאי), מתווספים עוד ועוד כלים ותהליכים ממוכנים מעולמות שונים כגון דיגיטל (אתרים, אפליקציות, סמארטפונים), אנרגיה, תמונה, וידאו ועוד.

היקפי המידע המנוהלים בארגון כיום הם עצומים ובדאטה חבוי מידע עצום.

כמה נתונים מרתקים שמסבירים את גודל התופעה (על פי - IDC International Data Corporation):

**עד סוף שנת 2020,** כמות האינפורמציה החדשה שתיווצר בשנייה אחת תעמוד על

## 1.7 מגה בייט לאדם

ההיקף המצטבר של כמות המידע שאנו מייצרים ומשכפלים מדי שנה גדל מ-4.4 זטה-בייט בשנת 2013, ל-44 זטה-בייט בשנת 2020 (כמות מידע המקבילה ל-44 טריליון ג'יגה-בייט), **ואילו בשנת 2025 כמות המידע תסתכם ב-**

## 180 זטה-בייט

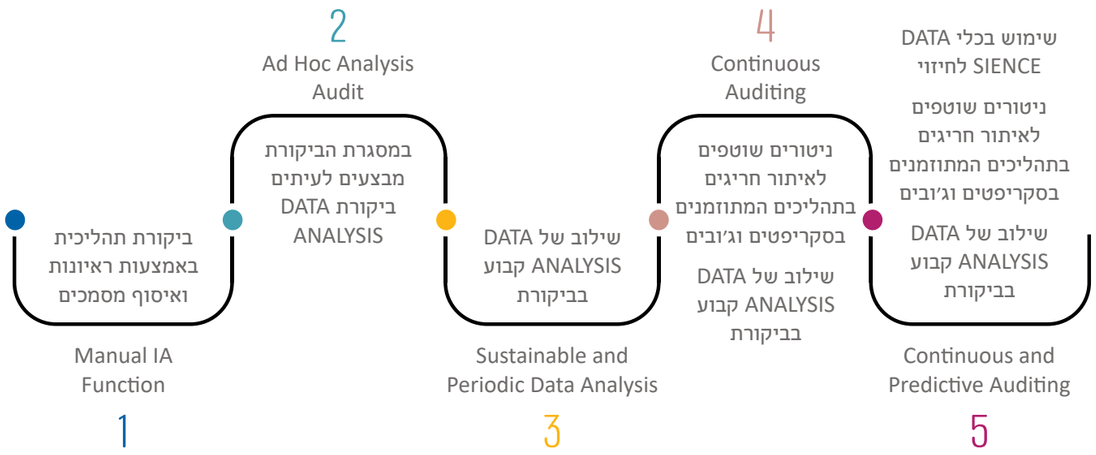
הנתונים הללו כוללים מידע על הזדמנויות עסקיות, תקלות, מעילות, יעילות תהליכים ועובדים, וכן נתונים נוספים. באמצעות מודלים סטטיסטיים ומתמטיים מתקדמים המקובלים בעולם ה-Data Science וכן בעולמות הידע הנפוצים כיום, ניתן להשתמש במידע העצום שנאגר גם לחיזוי בעולמות ה-Big-Data, כגון איתור לקוחות העומדים לנטוש, איתור מראש של תקלות העומדות להתרחש ואירועים נוספים.





## התייעלות באמצעות DATA ANALYSIS

מודל הבשלות בביקורת Analytics מגדיר שלבי התפתחות של שימוש ב- Analytics ותחקור נתונים כחלק מתהליך הביקורת השוטף. ככל שעולים ברמת הבשלות, השימוש ב- Analytics הופך לתדיר יותר, מקצועי יותר ובעל תוצרים ויזואליים יותר. לאור זאת, יכולת זיהוי הסיכונים והחריגים עולה, ובהתאם יעילות הביקורת הפנימית גוברת.




### שלב 1

Manual internal audit function

מבקרים (יחידות ביקורת) שעורכים ביקורת תהליכית קלאסית, ללא שימוש כזה או אחר בכלי Analytics המיועדים לביקורת (כגון ACL, Arbutus, IDEA) או לניתוח נתונים כגון SQL. הביקורת מסתמכת בעבודתה על פגישות, שאלונים, מעבר על נהלים ומסמכים. לעיתים נעשה שימוש באקסל לשימוש ניתוח נתונים פשוט יחסית, אך לא מעבר לכך. נציין כי מרבית הארגונים שבהם קיימת יחידות ביקורת המונות יותר ממבקר אחד נמצאים בשלבים מתקדמים יותר.

### שלב 2

Ad Hoc Analysis Audit

מבקרים/יחידות ביקורת שבאופן נקודתי משתמשים בכלי Analytics בעבודות ביקורת ספציפיות. במקרים רבים מדובר ביחידות ביקורת ללא יכולות Analytics המפעילות אחת לתקופה קבלן משנה לביצוע בדיקות אלו. יחידות ביקורת רבות נמצאות בשלב זה.

> "קיימת חשיבות רבה לאופן הצגת נתוני ביקורות ה- ANALYTICS באמצעות ויזואליזציה של הנתונים ניתן לראות את התמונה הכללית ולאתר מגמות בנקל"

### שלב 3

sustainable and periodic data analysis

שלב שבו מתקיים שילוב קבוע של ביקורת Analytics. בדרך כלל ביחידות ביקורת שבהן קיים צוות ביקורת מערכות מידע או גורם המתמחה בכלי Analytics המיועדים לביקורת (כגון ACL, Arbutus, IDEA) או כלים אחרים כגון SQL.

ביקורות Analytics בשלב זה הן חלק בלתי נפרד מעבודת הביקורת, וניתן לשלב בהן תחקור של הנתונים. שלב זה נפוץ בעיקר ביחידות ביקורת הפועלות בבנקים, בחברות ביטוח או בגופים אחרים בעלי יחידות ביקורת גדולות. קיימת חשיבות רבה לאופן הצגת נתוני ביקורות ה-Analytics באמצעות ויזואליזציה של הנתונים ניתן לראות את התמונה הכללית ולאתר מגמות בנקל. כיום, רוב משרדי ראיית החשבון יודעים לתת מענה ברמה זו או ברמה הקודמת עבור לקוחות יחידות הביקורת הפנימית שלהם.

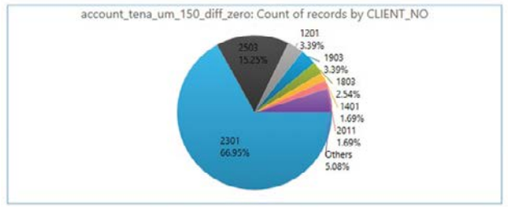
בדוגמה הבאה ניתן לראות תוצרי ביקורת שערכנו בתחום השכרת נכסים, שבמסגרתה ניסינו לאתר פערים בין סכומי חיוב בפועל של דיירים בנכסים מושכרים, לבין סכומי החיוב שנקבעו בחוזי ההשכרה. באמצעות בדיקות Analytics והצגה ויזואלית של הנתונים, זיהינו במהירות את הנכסים הבעייתיים לפי השלבים הבאים:

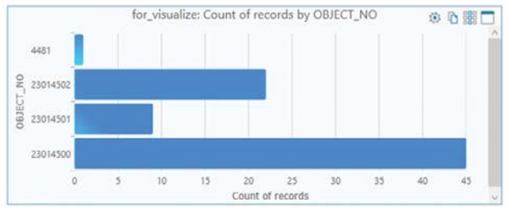
1. התמקדות בחברות שבהן קיימים חיובי חסר.

2. ניתוח כמותי של סכומי הפערים בין החוזה לבין חיוב בפועל.

3. זיהוי הנכסים הבעייתיים ומנהל הנכס הבעייתי.

באמצעות הצגה ויזואלית של הנתונים ניתן היה לאתר פערים בין סכומי החיוב בפועל לבין הסכומים שנקבעו בחוזי ההשכרה, וכן לאתר את מנהל האזור שקיימים אצלו אי סדרים בחיובים וכדומה.




כיום מרבית יחידות הביקורת בישראל אינן משלבות בקרות אנליטיות מתמשכות הדוגמות את בסיסי הנתונים ומציפות חריגים/אנומליות לצורך ביצוע של הערכה שוטפת של הסיכונים והבקרה, אך בתקופת משבר הקורונה ניתן היה להיווכח כי מודל זה בא לידי ביטוי באופן מעשי.

בעוד גופי ביקורת הנמצאים בשלבים 1-3 לא עסקו בביקורת ובבקרה במהלך המשבר, הרי שביחידות אחרות שבהן הוגדרה בקרה מתמשכת (שלב 4 ומעלה), התקבלו לאורך התקופה חיווים על חריגים / הפרות / חשדות למעילות. כך שבמקרים אלו הביקורת הייתה יעילה ואפקטיבית יותר לארגון, והיא חלשה על מערך הסיכונים דווקא בתקופה שבה הסיכונים גברו בצורה משמעותית.

כלי ה-Analytics המיועדים לביקורת (IDEA-ו ACL, Arbutus) כוללים יכולות תזמון ודיווח של הבדיקות, מה שהופך אותם לכלי Continues Control Monitoring (CCM) מתקדמים. בכלים אלו קיימים connectors לסוגים שונים של בסיסי נתונים, עליהם ניתן להגדיר פרוצדורות מתוזמנות של בדיקות הניתנות להצגה בדוחות, בגרפים ובכלים ויזואליים, ואף ניתן להוציא לגביהם התראות במייל או הודעות טקסט.

## שלב 4

Continues Auditing

במרץ 2015 פרסמה לשכת המבקרים הפנימיים העולמית (IIA) את הנחיית ביקורת GTAG3 בנושא ביקורת מתמשכת. בתקציר המנהלים של התקן נרשם בין היתר:

"A continuous audit approach allows internal auditors to fully understand critical control points, rules, and exceptions. With automated, frequent analyses of data, they are able to perform control and risk assessments in real time or near real time. They can analyze key business systems for both anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk. Finally, with continuous auditing, the analysis results are integrated into all aspects of the audit process, from the development and maintenance of the enterprise audit plan to the conduct and follow-up of specific audits."

פתרונות אלה החלו לצוץ לפני כעשר שנים. מודלים מתקדמים כיום כוללים לוחות ניהוליים המספקים תמונה כללית של רמת הבקרה והחריגים עם אפשרות לבצע Drill down על מנת לאתר את החריגים, כך שבכל נקודת זמן גוף הביקורת (או הבקרה) מעודכנים.

## שלב 5

שילוב כלי Data Science

בעולם העסקי, חברות וארגונים מטמיעים כלים ויכולות של Data Science על מנת לאתר לקוחות העומדים לנטוש, לאתר מעילות, לחזות מגמות וכדומה. מנגד, בעולם הביקורת שימוש בכלים אלה אינו נפוץ בישראל ובחו"ל.

Data Science (מדע נתונים) הוא תחום הכולל שיטות מדעיות, תהליכים, אלגוריתמים ומערכות. מדע הנתונים הוא "הרעיון לאחד נתונים סטטיסטיים, ניתוח נתונים, למידה של מכונה ושיטות קשורות כדי להבין ולנתח תופעות בפועל". מדע זה משתמש בטכניקות ובתאוריות מתחומי המתמטיקה, הסטטיסטיקה, מדעי המידע ומדעי המחשב, ובמיוחד מתתי-התחומים של כריית נתונים, למידת מכונה, מאגרי מידע וויזואליזציה.

למידת מכונה היא ענף של בינה מלאכותית, שבה הבינה נוצרת באמצעות למידה מתוך מאגרי נתונים גדולים. ניתן לחלק את למידת המכונה לשתי קבוצות עיקריות: למידה בלתי מונחית (Unsupervised Learning) ולמידה מונחית (Supervised Learning). ההבדל המרכזי בין השיטות הוא שבלמידה בלתי מונחית האנליסט אינו מתייג את הנתונים ואינו מלמד את מודל הנתונים מראש. המודל מוצא את הקשרים בין הנתונים על פי מודלים סטטיסטיים ומתמטיים בעצמו.

בלמידה מונחית (Supervised Learning) מתבצע תהליך של תיוג הנתונים ולימוד של מודל הנתונים, כך שבהתאם לתיוג זה המודל יציג את התוצאות. למשל, מודל על בסיס נתונים גדול של מידע מטויב על נתוני לקוחות הכולל תיוג של הרשומות של הלקוחות שעזבו. בהתאם לדפוס שתויג, המודל יאתר לקוחות בעלי פוטנציאל גבוה לנטישה.

דוגמאות נוספות: ניתוח ה-DATA הקיים ברשת האינטרנט, ומתוכו ללמוד על איתנותם של ספקים ולקוחות; ניתוח של הענף שבו הארגון פועל, של חברות שקרסו וחברות שהמריאו; וכן ניתוח מרכיבי הכישלון וההצלחה וכדומה.

נציין כי פרויקטי Data Science הם מורכבים ועתירי משאבים ולכן עדיין אינם נפוצים בארגונים העסקיים בארץ וכנגזרת בעולם הביקורת. גם בעולם השימוש בכלים אלו במסגרת הביקורת הוא נדיר. אנו צופים כי בעתיד המבקרים ישדרגו את ניתוחי הנתונים באמצעות שילוב טכניקות Data Science. לדוגמה, באמצעות למידה בלתי מונחית (Unsupervised Learning) על נתוני כרטיסי אשראי הכוללים מידע, כגון שעת ביצוע הפעולה, מיקום, סכום, נתונים על הלקוח וכדומה, ללא תיוג המציין אם הפעולה תקינה או לא תקינה. התכונות של הנתונים לעיל יכולות לשמש כדי לזהות אנומליות או כדי למיין את הנתונים לקטגוריות שמהן ניתן יהיה להסיק בנוגע לפעולות חריגות החשודות כמעילות.

שימוש ברובד ה-Data Science יכול לקבע את מעמדו של המבקר כיוזע הפועל לקדם את הארגון. אך עוד בטרם יבצע המבקר שימוש ברובד זה, חשוב לראות כי הארגון עצמו פועל למימוש היתרונות של רובד ה- Data Science ולבקר תהליכים אלו.

**ארגון הפועל באמצעות כלים אלה יאתר סיכונים אסטרטגיים בצורה יעילה יותר.**

נציין כי קיימות חברות שירותים המספקות ניתוחי Data Science תוך הבטחת סודיות המידע. יש בכך פתרון לחברות וארגונים שאינם ערוכים לפרויקטים אלו בהיבט התשתיתי או הפיננסי. ייתכן שדרישת הרגל של עולם הביקורת בתחום ה-Data Science.

# הדחף לשינויים בביקורת הפנימית

**מאת:** גלית ויזר | רו"ח, MBA, מבקרת פנימית ראשית ומנהלת חטיבת הביקורת בבנק מזרחי טפחות
דירקטורית ויו"ר משותף פורום המגזר הפיננסי - לשכת המבקרים הפנימיים IIA ישראל

רותי רובין | MBA, מנהלת מחלקת ביקורת סיכונים פיננסיים ויחידות מטה בנק מזרחי טפחות

את המאמר על הדחף לשינויים בביקורת הפנימית כתבנו לפני משבר הקורונה, על רקע התפיסה המקובלת בשנים האחרונות, ולפיה היכולת של הביקורת להסתגל ולקדם שינוי היא רכיב הכרחי לצורך ביקורת חדשנית ומתקדמת.

החשש היה דווקא מסטגנציה וחוסר מוטיבציה לבצע שינויים ושיפורים, ומחוסר רצון לצאת מאזור הנוחות שעלול לפגוע באפקטיביות הביקורת. המאמר נועד לקדם יוזמה לשינוי, גם אם הוא לא נכפה עלינו.

כולנו ידענו שהיכולת להתאים את עצמנו לשינויים וגמישות הביקורת הן חשובות. ידענו, אבל לא הבנו עד הסוף. שום דבר לא הכין אותנו למשבר הקורונה, שבה כלל העסקים במשק נקלעו למצב חירום. מרבית תשומת הלב הופנתה לשימור רציפות תפקודית, ובבנקים ניתן דגש על מתן שירות ללקוחות במוקדי שירות, בחדרי העסקאות ובסניפים. בתקופה זו נדרשה הביקורת להתאים את עצמה במהירות למצב החדש ולבחון את מקומה בעת חירום.

בתקופה זו עלו שאלות כמו האם הביקורת צריכה להמשיך בפעילותה הקלאסית, הכוללת הפקת דוחות ביקורת וניהול מעקב אחר יישום המלצותיה, או שמא היא נדרשת להתאים את פעילותה ולעבור לפעולות חשובות יותר לארגון, כגון סקירת הבקרות והאפקטיביות שלהן על רקע השינויים בתהליכי העבודה ובפעילות בתקופת המשבר.

הביקורת היא אורגן חי. תפקידה הוא לספק מענה לצרכים משתנים בסביבה חיצונית משתנה ולפי דרישות של בעלי עניין שונים. היא נדרשת להיות בתנועה ולהתאים את עצמה תוך שמירה על מטרותיה ועקרונותיה. בעת משבר הקורונה נדרשה הביקורת להקפיא את פעילותה לרגע, כדי לאפשר לבנק להתמודד ולהתאושש ולחזור לפעילות באופן מותאם אחר למגבלות הקורונה.

השינויים בביקורת הפנימית לא התחילו עכשיו. במהלך עשרות שנים חוותה הביקורת שינויים רבים בסביבתה הארגונית, העסקית, הרגולטורית והטכנולוגית, כמו גם שינוי בצרכים של בעלי העניין, ובהם ההנהלה והדירקטוריון.

**למרות זאת, ביצוע שינויים כחלק משגרת החיים של הביקורת בימים כתיקונם נותר אתגר, בין היתר בשל התשומות שנדרש להשקיע בשינוי, הסיכון לפגוע בקיים, והיציאה מאזור הנוחות הכרוכה בכך.**

לעומת זאת, השינויים בתקופת הקורונה שתוארו לעיל אומנם לא היו פשוטים, אך היו כרוכים בפחות היסוסים והתחבטויות מפני שהם נכפו מחוסר ברירה.

כדי להביא ערך אמיתי, הביקורת חייבת ללמוד את השינויים באופן מתמיד ולפעול בין היתר כ"סוכן שינוי", הן לגבי עצמה והן לגבי הארגון בכל "תנאי מזג אוויר".

במאמר זה נציין את ההיבטים העיקריים שבהם חל שינוי בביקורת הפנימית ושהביאו להתפתחותה במהלך העשורים האחרונים. הדברים נכונים לכלל הארגונים ולבנקים בפרט.

**על פי התיאוריה של המדען דניאל וולפרט, המוח דרוש אך ורק כדי לאפשר תנועה, כלומר שינוי. במחקר שבו בדק את האיצטלן, ייצור תת-ימי המנווט את דרכו באוקיינוס הגדול, הוא מצא שכאשר האיצטלן בוחר בסביבה המיטבית עבורו, הוא קובע בה את מושבו עד סוף חייו, ומוחו נעלם.**

## אילו שינויים חלו בביקורת בשנים האחרונות?

בעשורים האחרונים חלו שינויים מהותיים בפעילות הארגונים בענפים השונים, שינויים שמקורם בהתפתחויות רגולציה ובתקנים חדשים שפורסמו על ידי גופים מקצועיים מובילים בעולם.

בעקבות המשבר העולמי במהלך 2008-2009 חוזקו הבקרות, ובענפים מסוימים (לרבות ענף הבנקאות) ניתנה הנחיה לגיבוש מסגרת לניהול סיכונים הכוללת שלושה קווי הגנה ולהקמת מעגל בקרה שני. בנוסף נדרשה הביקורת להעריך את אפקטיביות הבקרות וניהול הסיכונים בארגון ולהתייחס לנושאים ולידע שלא נדרשה להם בעבר.

אם כן, הביקורת נאלצה להגדיר את מקומה מחדש בארגון, לחדד את גבולות הגזרה, ולקבוע ממשקי עבודה עם יחידת ניהול הסיכונים.

תקופת המשבר הנוכחי חידדה את חשיבות תפקיד הביקורת בעת הזו. לאור החשיפה ההולכת וגוברת של סיכונים שאליהם חשוף הארגון בעת משבר, כאשר יחידות עסוקות בהישרדות תוך נוכחות מצומצמת של עובדים ותחת מגבלות הקורונה, קיים צורך אמיתי בהפניית משאבים לניהול הסיכונים. לפיכך החלטנו להגביר את מעורבות הביקורת בניהול הסיכונים, בדגש על סיכוני מעילות והונאות וסיכוני סייבר. המטרה היא לוודא כי אפקטיביות הבקרות נשמרת גם במקרים שבהם חל שינוי מהותי בתהליכי העבודה או בסביבה העסקית.

**המשברים שאירעו וההתפתחויות הרגולטוריות שהגיעו בעקבותיהם הביאו את הביקורת הפנימית למספר התפתחויות משמעותיות.**

## תפיסת הביקורת בארגון

לאורך שנות קיומה של הביקורת חל שינוי בתפיסת הביקורת בארגון ממצב של קיום ביקורת כחובה חוקית לתפיסת הביקורת כגורם חיוני המצמצם סיכונים לארגון ולגורמי הנהלה החשופים לדרישות רגולציה ולאחריות אישית.

לפיכך, קיימת חשיבות רבה לתפיסת הביקורת בארגון ולמיצובה כפונקציה משמעותית וחיונית עבור ההנהלה והדירקטוריון.

> הביקורת היא אורגן חי. היא נדרשת להיות בתנועה ולהתאים את עצמה תוך שמירה על מטרותיה ועקרונותיה.

ביקורת שנתפסת כעניינית, אובייקטיבית ובלתי תלויה על ידי המבוקרים, תוכל לקיים את תפקידה טוב יותר ולהביא ערך משמעותי יותר לארגון. לצורך כך, הביקורת נדרשת להציג תמונה מאוזנת של הפעילות הנבדקת ולציין נקודות לשיפור, תוך התייחסות לפעולות מהותיות שנמצאו תקינות.

מגמה זו מתחזקת בשל הצורך במתן ציון והערכה כוללת (כפי שנדרש מהביקורת הפנימית בבנקים בהתאם להוראת ניהול בנקאי תקין 307), המחייבים הסתכלות כוללת על פעילות היחידה או הישות הנבדקת.

על מנת לספק מענה לשינויים אלה, נדרשת אבולוציה בתחומים הבאים:

## פרופיל המבקר

כבר היום, על מנת לתת מענה לצורכי הביקורת, המבקר הפנימי נדרש לקשת יכולות ולכישורים רבים ומגוונים, כמו יכולת למידה וניתוח לוגי ותהליכי, תקשורת בין-אישית, יכולות כתיבה והבחנה בין עיקר לטפל, וכן ידע וניסיון בתחומים המבוקרים, כגון כספים, מערכות מידע, פעילויות מטה תומכות ועוד.

בעקבות שינויים שחלו בשנים האחרונות, מלבד סט הכישורים והיכולות הללו, המבקר נדרש גם לכישורי שליפה וניתוח נתונים, לרבות יכולות שליפה וניתוח נתונים ממספר מקורות מידע, חשיבת BI ושליטה בכלים טכנולוגיים מתקדמים לביצוע תחקורים. מגמה זו צפויה להתעצם בשנים הקרובות.

אתגרים אלה יחייבו את הביקורת לשים דגש על קליטת מבקרים המשלבים יכולות בין-אישיות המאפשרות תקשורת פתוחה ועניינית עם הגורמים בארגון, ראייה מאוזנת וחסרת משוא פנים, וידע מקצועי. בו-בזמן נדרשת הכשרת כלל המבקרים לידע בנושאים טכנולוגיים, והנגשת השימוש בכלי תחקור לכלל המבקרים ביחידה.

> האם הביקורת צריכה להמשיך בפעילותה הקלאסית, או שמא היא נדרשת להתאים את פעילותה ולעבור לפעולות חשובות יותר לארגון?

## שיטת ביצוע הביקורת

### ביקורות בין צוותיות

יחידות הביקורת מחולקות בהתאם להתמחותן בסיכונים השונים או על פי סוג הפעילות (כגון ביקורת סניפים, מערכות מידע). על מנת לייצר תמונה כוללת של ניהול הסיכונים בנושא, עולה בשנים האחרונות הצורך בעבודה צוותית המשלבת מספר מיומנויות שונות לתוצר אחד.

מדברים יותר ויותר על עבודה בתצורת Agile. שינוי זה דורש שיתוף פעולה ותיאום תוך כדי תנועה, ויוצר אתגרים הנוגעים לתיאום זמנים, לתיאום הבדיקות, לכתיבת הדוח ועוד. כדי להתמודד עם השינוי הזה נדרשת הגדרה של שיטת עבודה עדכנית לתהליך הביקורת, והדרכת המבקרים והמנהלים לעבודה משותפת.

### כלים טכנולוגיים

סקר מוקדם שכולל איסוף חומרים לפגישה ראשונית, יהווה התחלה טובה לביקורת. אז למה צריך לשנות? אנו חיים בסביבה עתירת נתונים, ולרוב יש לנו גישה ישירה ועצמאית לנתונים שמאפשרים לנו לקבל מידע רב באמצעות זיהוי חריגים וניתוח אנומליות שיכולים להוות לידים כבר בשלב הראשון לביקורת.

**לשימוש בכלים טכנולוגיים יש מגוון יתרונות, ובהם:**

- כיסוי רחב יותר.
- מעבר מבדיקות מדגמיות לבדיקות אוטומטיות, המאפשרות לבחון היקף גדול יותר של נתונים ואף אוכלוסייה שלמה.
- ביצוע בדיקות נתונים בכלים ממוכנים המותאמים לצורכי הביקורת, עשוי לייעל את עבודת הביקורת ולהפחית את היקף המשאבים הנדרש.
- זיהוי קשרים או אנומליות יכול לחשוף ליקויים שגם המבוקר אינו מודע להם, ושלא יעלו בשיחות או בבדיקות מדגמיות.

עם זאת, קיימות גם מגבלות לשיטה זו:

- זמן ומומחיות בביצוע שליפות ממוקדות ומדויקות לצורך הבדיקה.
- תלות בגורמי BI.
- סיכון שלא נגלה בדרך זו ליקויים שהיינו מגלים בבדיקות תיקים ובשיחות.

> "הביקורת חייבת ללמוד את השינויים באופן מתמיד ולפעול בין היתר כ"סוכן שינוי""

## לפיכך, ההתמודדות עם השינוי תחייב אותנו לבצע התאמות:

- גיוס אנליסטים מומחים לשליפות נתונים. צפוי כי מספר העובדים בתחום זה יגדל משמעותית בשנים הבאות.
- כאמור, נדרשת הכשרת מבקרים לתחומי ה-BI, SQL, ו-SAS, על מנת להפחית את התלות בגורמים השולפים את הנתונים, ולשם יצירת מבקרים בעלי ידע מקצועי הכולל ידע בשליפת נתונים.

חשוב להדגיש שלצד ההיערכות לשינויים, יש לשמר את היתרונות של הביקורת המסורתית ולזכור שתקני הביקורת שלא השתנו במהותם, מהווים בסיס טוב ורלוונטי גם היום. לאור זאת, שילוב של ביקורות חדשניות באמצעות שליפות נתונים, לצד הביקורות המסורתיות לצורך קבלת מידע שלם על סיכונים בפעילות, עשוי להביא לביקורת אפקטיבית התורמת לארגון.

עם החזרה לפעילות ביקורת מסורתית בשגרת קורונה, שבה פעלו ארגונים תחת עומס, אילוצי כ"א מצומצם ומגבלות על התקהלות ושמירת מרחק, מגובשים בימים אלה עקרונות לפעילות הביקורת הפנימית בתקופת הקורונה.

מטרת הביקורת היא להמשיך בפעילות הביקורת תחת המגבלות והקשיים הקיימים, תוך נקיטת זהירות מיוחדת הנוגעת לסיכוני בריאות והשבתת יחידות.

בהתאם לזאת, תהליך הביקורת והיקף הנושאים הנבדק התחדד ודויק, ושיטת הביקורת הותאמה למציאות שבה פגישות פיזיות נדירות.

**ההתאמות שאליהן נדרשנו, בתחילה כאילוץ, התגלו כהזדמנות להתייעלות וחידוד דוחות הביקורת ולשדרוג היכולות ושיטות העבודה.**

לסיכום, אנחנו המבקרים עוסקים בשינויים של אחרים באופן שוטף, אך האם נוכל לבחון ולהחיל את אותם עקרונות גם על עצמנו?

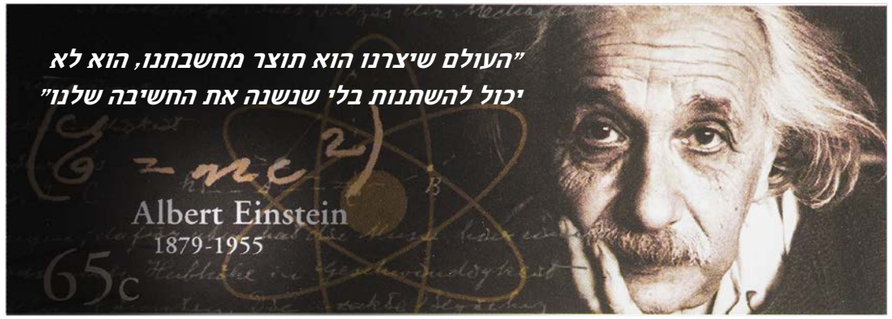
לאור ההתבוננות בשינויים שחווינו בתקופת הקורונה אל מול השינויים שביצענו בתקופות קודמות - הן מבחינת קצב והן מבחינת עוצמה - עולות מספר שאלות שמן הראוי לשאול את עצמנו. נזכיר שהביקורת עושה זאת באופן מובנה ופנימי כחלק מתהליך מתמשך ושוטף של שיפור איכות הביקורת, וכן באמצעות סקירה חיצונית אחת לתקופה.

# עדכון גירסה 20.20

## המבקר הפנימי על רקע שיבושים

**מאת:** רונית בירן | רו"ח, C.R.M.A, מבקרת פנימית ראשית לשעבר קבוצת שו"ב, חברת ועדת ביקורת בלשכת המבקרים הפנימיים IIA ישראל

בעז ענר | רו"ח, MA, CIA, מרצה, יועץ, מנהל סדנאות ביקורת, לשעבר משנה למנכ"ל - משרד מבקר המדינה




שיבוש מוגדר כ"קלקול, הפרעה, תקלה". לעיתים המונח מופיע כ"חדשנות משבשת" - המובילה ליצירת שוק חדש ובמקביל גורמת לשיבוש השוק הקיים (המסורתי) שלא נערך בהתאם.

לדוגמה: שיבוש הקורונה האיץ את הצורך בתקשורת מרחוק. למשל, טכנולוגיית ה-ZOOM מיושמת בכל עסק ובכל בית ואין ילד שהמילה הזאת אינה שגורה בפיו. השימוש הנרחב בכלי הזה, שלמעשה נכפה על הארגונים, תרם להמשכיות עסקית, לחיסכון ולהתייעלות. קיום ישיבות רבות משתתפים באמצעות ה-zoom מאפשר לצפות במצגות ובמקביל לנהל דיון פורה עם המשתתפים. הוא חוסך זמן ועלויות ניכרות של נסיעות בארץ ולחו"ל, ומאפשר למנהלים ולעובדים לנצל את הזמן הזה למשימות אחרות.

catwalker / Shutterstock.com





הקורונה החלה והעצימה שיבושים וסיכונים רפואיים-וירואליים, אך במהרה הפכה ל"סופה" של שיבושים. בין השאר היו שיבושים מדיניים, פוליטיים, טכנולוגיים, כלכליים, רגולטוריים, חברתיים, תעסוקתיים, תקשורתיים ועוד. במציאות של הכפר הגלובלי, "משק כנפי הפרפר" בסין אכן יצר טורנדו כלל עולמי.

המסקנה המערכתית: אנו בדור של שיבושים, לא חשוב מה שמם. יש להסתגל לכך ששיבושים ובהם שיבושים חיוביים (כמו פריצות דרך טכנולוגיות) הם מנת חלקנו השוטפת - היום, מחר, מחרתיים.

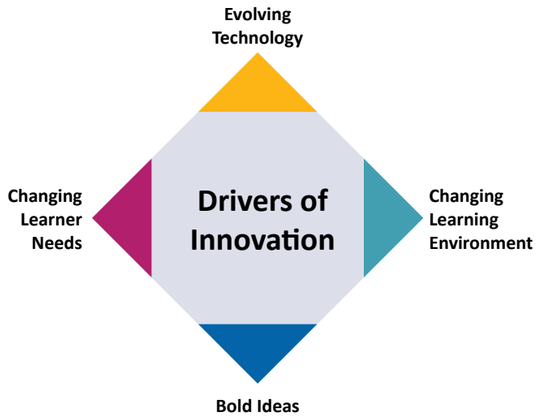
דוגמאות לשיבושים טכנולוגיים ולחדשנות בהווה ובעתיד הקרוב: מכוניות אוטונומיות, בינה מלאכותית, שימוש נרחב יותר בלוויינים וברחפנים, רפואה מרחוק, עבודה והוראה מרחוק, והגברת עוצמת הבינה המלאכותית, ומול כל זה עולים הסיכונים של אובדן פרטיות וכדומה.

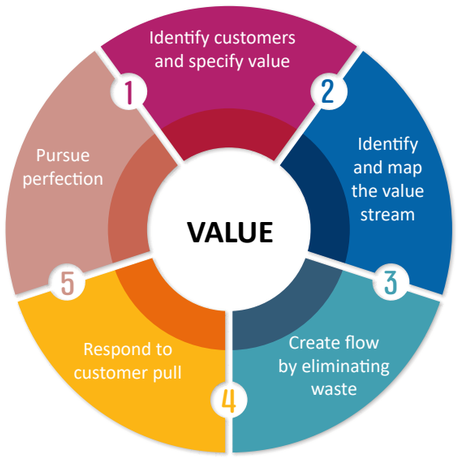
פועל יוצא - אופן ניהול העסקים שהכרנו לא ישמש אותנו לאורך זמן. הארגונים השונים צריכים להדביק את קצב השינויים (ולא רק העסקיים) על מנת להישאר רלוונטיים. ארגונים שאינם מתחדשים עתידים לקרוס (כפי שקרה לקודאק), כאשר יזמים חדשים או קיימים יבינו איך לשפר ולפתח טכנולוגיות או עסקים יעילים יותר, המשרתים טווח רחב יותר של לקוחות. לפי מחקר שפרסם בית הספר למינהל עסקים אולין Washington DC 40 חברות מרשימת ה-Fortune 500 ייעלמו בעשור הקרוב או יעברו טרנספורמציה משמעותית. במאמר זה נציג את השפעת ה"שיבושים" על המבקר הפנימי, שצריך להמשיך לעשות את הביקורת בהתאם להוראות החוק והתקנים, אולם בפורמט חדשני, מהיר, זריז וגמיש, ובצורה ההולמת את המציאות של שיבושים חוזרים ונשנים. במילים אחרות:

**לשלב בין מודלים חדשים לביצוע ביקורת ואופן הצגתה, לבין הטכנולוגיה, המשאבים והמתודולוגיות, כדי לייצר ערך ולהישאר רלוונטיים בעולם משתנה.**

> אנו בדור של שיבושים, לא חשוב מה שמם.
> יש להסתגל לכך שהם מנת חלקנו השוטפת – היום, מחר, מחרתיים.

## ההיבט ההתנהגותי – לשנות דפוסי חשיבה




שיבוש גורם לך להרגיש משותק, כאילו הקרקע מתחת לרגליך נשמטת, אתה מחפש פתרון מוכר מהארסנל שבתודעתך, אבל לא חושב באופן יצירתי איך להתמודד עם הסיטואציה שנוצרה בעקבות השיבוש. במצבים כאלו יש לנסות לאלתר, לצאת מהקיפאון ולהפוך את החיסרון ליתרון.

אורית וולף בהרצאתה "להמציא את עצמנו מחדש" הציגה סרטון על כנר שבאמצע הקונצרט התמודד עם "שיבוש": צלצול טלפון מהקהל. ה"שיבוש" גרם לכָּנר לצאת מריכוז לכמה שניות ואז הוא החל לנגן את הנעימה של צלצול הטלפון. הקהל פרץ בצחוק, וכך הפך את השיבוש הרגעי ליתרון.

והנמשל בהקשר של ביקורת:

**מבקרים פנימיים צריכים להתעשת במהירות ולמצוא את הדרך להביא ערך מוסף,**

לערוך השוואות (BENCMARKING); להעמיק ב-BEST PRACTICES, לשוחח עם מקבלי החלטות ועם דרגים אחרים, ובאמצעות מידע זה לבחון את ההערכות הארגונית לשיבושים;

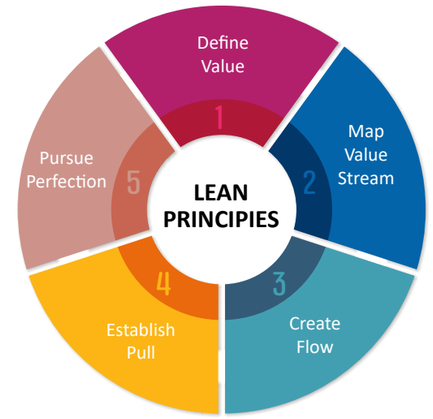
ו\או לנתח ולמפות באופן מזוקק סיכונים\שיבושים עתידיים ומהם לגזור מטלות לבדיקה; ו\או להיכנס לבדיקות בתחום התרבות הארגונית - תחום חדשני הכולל סיכונים שארגונים רבים טרם העריכו את עוצמתם;

ו\או לעזור ולתמוך ולספק תובנה לארגון כיצד הוא יכול לרתום את הכוח המשבש ליתרון ולהביא ערך מוסף.

האתגר: להביא ערך - זווית ראייה שונה, לתת את "הקונטרה" הדרושה בדיונים בדירקטוריון, להעביר תובנות להנהלה דרך ניתוח שונה או ניתוח המוסיף בדבר השלכות הסיכון והמשאבים - תהליכים הדרושים לצמצמו. המטרה - שמקבלי ההחלטות בארגון יוכלו לבחור\לשקול טוב יותר אסטרטגיות להמשך הפעילות העסקית בצורה מושכלת.

מטרת העל מבחינת המבקר הפנימי - להיות מבקר חדשני העוסק לא רק בביקורת מקובלת, אלא לובש דמות של מבקר הצופה פני עתיד ופועל כיוצא באמצעות דוחותיו והמלצותיו.

## כיצד עושים זאת: דרך המלך להגביר חדשנות בעבודת הביקורת




**בסביבת עסקים דינמית, סוגי הסיכונים, הסבירות להתרחשותם ומידת השפעתם, משתנים בתדירות גבוהה. כדי להוסיף ערך, על המבקר הפנימי לספק את תוצרי הביקורת במהירות, בדיוק ובחדות, תוך חדשנות רעיונית ותפעולית.**

## תובנות, הדגשים והמלצות לשינוי

- עידן הדבקות בתוכנית הביקורת השנתית הנוקשה - התערער. כעת הקו המוביל, תחת אישור של ועדת הביקורת, הוא זריזות ונכונות לשינויים מהירים בתוכנית ובביצועה.
- הביקורת המסורתית מפנה את מקומה לביקורת "רזה" (Lean Audit) או לביקורת זריזה-גמישה (AGILE). זהו תהליך עבודה המאתגר את המבקר שצריך כל העת לשאול את עצמו אם הוא מספק את צורכי הלקוח ונוגע בליבת הבעיות (TOP - 5), מתעלם מהטפל ומתמקד בעיקר, ונוקט את השיטה היעילה ביותר תוך חיסכון במשאבים. זהו עידן של התייעלות בלתי מתפשרת. כל עבודה שלא תומכת במדיניות זאת תתבטל מאליה.
- יש לקיים ישיבות, להפיץ שאלונים ולהתייעץ עם בעלי תפקידים האחראים על מעגל הבקרה הראשון (מנהלים ועובדי תפעול), ולאחר מכן עם בעלי התפקידים האחראים על המעגל השני (מנהל סיכונים, מנהל בקרה, מנהל ציות). יש לבצע סיעור מוחות עם כל הגורמים האלה בזמן קצר, דבר שיסייע לספק בהירות בהערכת הסיכונים ויתרום לאפקטיביות הבקרות הקיימות.
- כפועל יוצא, יש להתמקד בתחומים בעייתיים ובסיכונים מהותיים תוך צמצום הכניסה לביקורת באזורים שבהם קו ההגנה השני כבר מוליך לבקרה נאותה ולמציאות של סיכונים לא גבוהים לארגון.
- לבנות תוכנית ביקורת מוכוונת סיכונים ולא בקרות. באופן כזה ניתן לזהות סיכונים חדשים שטרם הוטמעו בגינם בקרות.
- לייעץ להפחתת הסיכונים באמצעות מתן המלצות אופרטיביות שהארגון יכול להכיל.
- להכין תוכנית ביקורת המבוססת על תחומים שבהם יש מקום להתייעלות וחיסכון.
- לדרג נושאים שעלו בסקר ובתוכנית הביקורת, להתמקד בעיקר (5-TOP) ולוותר על הטפל.
- לזהות ולנתח סיבות שורש לכל בעיה מהותית שעולה.

## לשפר את אופן הצגת ממצאים בעידן של שיבושים

תמצית מנהלים קצרה וממוקדת היא שם המשחק. מדיניות "Less is More" נכונה לאמור לעיל ונכונה גם לאופן הצגת דוחות הביקורת. הקשב בעידן הזה הוא קצר, ולכן יש למקד את עיקרי הממצאים, סיבת השורש ומתן פתרונות לבעיות בדרך הקצרה והיעילה ביותר להבנה.

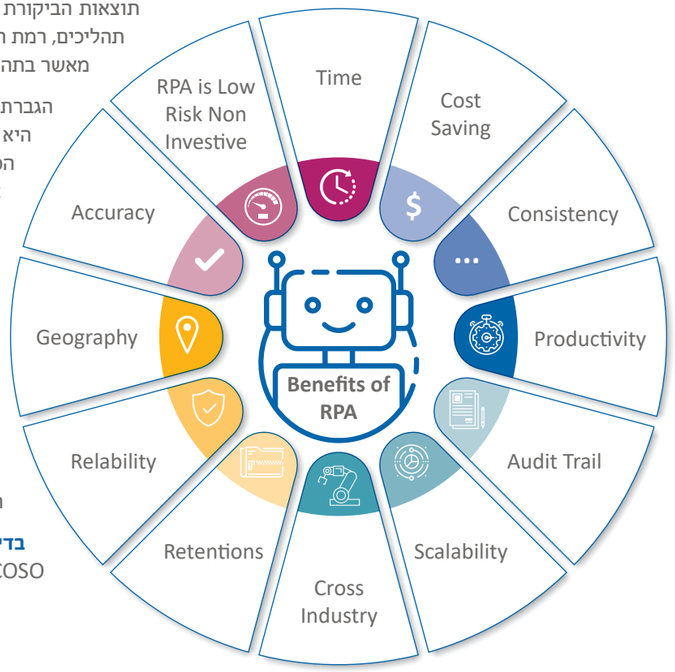
שימוש בכלים כמו תרשימי זרימה, גרפים, טבלאות, אלמנטים חזותיים, תמונות מהשטח (יעיל ביותר לכשלי בטיחות), הוא אפקטיבי מאוד להשגת המטרה.





## חדשנות בשיטות בדיקה

### רובוטיקה - Robotic Process Automation (RPA)




הגדלת היקף הביקורת, יעילות וחיסכון - שימוש ב-RPA לביצוע משימות ביקורת בקצב מואץ ומסביב לשעון יכול להביא לחיסכון משמעותי בעלויות, וכן לבדיקת אוכלוסייה מלאה במקום מדגם.

תוצאות הביקורת מדויקות יותר - עם סטנדרטיזציה מובנית של תהליכים, רמת הדיוק באיכות הנתונים הממוחשבים גבוהה יותר מאשר בתהליכים ידניים.

הגברת תדירות הביקורת - תוכנית הביקורת הנבנית היא מבוססת סיכונים. אם בעבר במקומות שבהם הסיכון נמוך נהגנו לערוך ביקורת בתדירות של אחת לכמה שנים, שימוש ב-RPA יאפשר ביצוע ביקורת בפרקי זמן קצרים יותר, ללא ניצול משאב של זמן או עובד, שבדרך כלל חסר בצוותי ביקורת.

כמובן, יש לתת את הדעת לכך שגם הסיכונים משתנים עם הטמעת RPA בתהליכי עבודה (כגון סיכונים טכנולוגיים, איבוד ידע, הפרדת תפקידים וכדומה).

**כניסה משמעותית לתחום הביקורת הרכה** **SOFT-AUDIT** ועימה כניסה לבדיקות בלב התרבות הארגונית.

**בדיקות לפי מודלים** (כמו מודל הבקרה - מודל COSO מודל הבשלות).

אנו חיים בעידן של שינוי. אין לחשוש מזה, אלא לראות בעבודה דיגיטלית כאמצעי עזר ולא איום.

RPA הוא קוד תוכנה המבצע אוטומציה של פעולות/משימות מובנות החוזרות על עצמן, ויודע להשתמש במערכות תוכנה קיימות כדי לנצל את הבקרות הקיימות בחברה.

שימוש מרכזי ב-RPA הוא איסוף ראיות ביקורת על ידי איסוף מידע מנתונים במערכות שונות שאינן משולבות. באמצעות מידע זה ניתן לנתח נתונים במהירות ובקנה מידה גדול כדי לשפר הערכות סיכון או לספק ראיות ביקורת. כמו כן, ניתן להשתמש בכלי זה לצורך ביצוע פעולות מובנות שלא מצריכות הפעלת שיקול דעת (כגון דרישות בסיסיות למתן אשראי ללקוח).

לשימוש ב-RPA לטובת הביקורת הפנימית יש יתרונות לא מעטים:

ניצול נכון יותר של משאבים - הפניית פעולות פשוטות ל- RPA (כמו בדיקת עמידה בנהלים טכניים) מאפשרת לאנשי הצוות להתמקד בפעילויות מורכבות יותר המצריכות ניתוח וחשיבה מעמיקה, כגון ניתוח סיבות שורש לחריגות שנמצאו, שיפור תהליכים ואינטראקציות בין אישיות.

## סיכום

אנו בפתחו של עידן שבו קצב הגורמים המשבשים רק יואץ. הדבר מחייב חדשנות, יצירתיות וחשיבה שונה בביקורת הפנימית. מַעבר לשימוש בטכנולוגיות מתקדמות כמו אנליטיקס ו-RPA, לצד מתודולוגיות חדשניות בתהליכי הביקורת, כמו ביקורת גמישה, זריזה ותמציתית - המנתחת טוב יותר גורמי סיבות השורש, נוגעת בעיקר ומגבשת המלצות פרגמטיות, קצרות וממוקדות ופתרון מעשי לבעיות - יביאו להעלאת הערך המוסף של המבקר לארגון. מבקר פנימי שיניע שינוי מהותי יחזק את מעמדו כמבקר-יועץ הפועל בזמן אמת ומייצר SECOND OPINION - זווית ראייה נוספת, שונה וחדשנית.

# GAME OVER?

## הביקורת הפנימית במשרדי הממשלה בעת חירום - מחוץ למשחק?

מאת: מירב שגיא יהודיין | המבקרת הפנימית, המשרד להגנת הסביבה, יו"ר פורום מבקרים במשרדי ממשלה לשכת המבקרים הפנימיים IIA ישראל

עו"ד יקיר שמעון | הביקורת הפנימית במשרד להגנת הסביבה

משבר הקורונה, שנכון לכתיבת שורות אלו טרם הסתיים, הוגדר כאירוע חירום בלתי צפוי בקנה מידה יוצא דופן, והשליך באופן ישיר גם על עבודת הביקורת הפנימית במשרדי הממשלה.

המשבר הציף שאלות וסוגיות באשר למקומה של הביקורת הפנימית בעת חירום, ובאשר למעמדו של המבקר הפנימי כשומר האינטרס הציבורי. כמו כן, המשבר אילץ את המבקרים הפנימיים והממונים עליהם לבחון מחדש את אופי פעילות הביקורת הפנימית בשגרה ובחירום.

מצד אחד, בתקופה זו נוצר איום להשבתת פעילות הביקורת הפנימית במקרי משבר. מצד שני, נוצרה הזדמנות לפעול לחיזוק הביקורת הפנימית ולעיגון פעילותה בעיתות שגרה וחירום.

בפברואר 2020 החל להתפשט נגיף הקורונה בישראל. ממשלת ישראל, באמצעות משרד הבריאות, העבירה הנחיות עיתיות להתמודדות עם הנגיף ולמניעת התפשטותו - כאשר בין היתר הוטלו מגבלות על פתיחת עסקים, על התקהלות אנשים ועוד.

ב-22.3.2020 הותקנו תקנות שעת חירום (הגבלת מספר העובדים במקום עבודה לשם צמצום התפשטות נגיף הקורונה החדש), תש"ף-2020, להגבלת מספר העובדים במקום עבודה, ולהנחיית אופן ההתנהלות במשרדים ממשלתיים ומעסיקים שאינם משרד ממשלתי העומדים בכללים למניעת התפשטות נגיף קורונה.

במרבית משרדי הממשלה ויחידות הסמך, רוב העובדים (לרבות המבקרים הפנימיים ועובדי הביקורת) הוגדרו "לא חיוניים" לתפקודם הרצוף של משרדי הממשלה והוצאו לחופשה כפויה/מרוכזת.

> "רק כ-50% מהמבקרים הפנימיים במשרדי הממשלה וביחידות הסמך הוגדרו כחיוניים והיתר הוצאו לחופשה"





## מסגרת חוקית

הביקורת הפנימית פועלת במשרדי הממשלה מכוח חוק הביקורת הפנימית התשנ"ב-1992, וכן על פי הנחיות נציב שירות המדינה שבהן הוגדר ייעודה כדלקמן: "...לביקורת הפנימית שני היבטים עיקריים: האחד - כלי ניהולי הנועד לסייע להנהלת הארגון בשיפור ובייעול עבודתו. השני - שמירת האינטרס הציבורי, והיותה חלק ממערך הגורמים הקיימים בארגון לבדיקת תקינות הגוף המבוקר".

אם כן, נראה כי שני ההיבטים המתוארים לעיל (היותה של הביקורת כלי ניהולי ושומרת האינטרס הציבורי), הנכונים בעת שגרה, מקבלים משנה תוקף בעת חירום. הסיבה לכך היא שבתקופת משבר הארגון עובר מהתנהלות לפי נהלים שבשגרה להתנהלות שונה שבה עלולים לנקוט "קיצורי דרך", והפוטנציאל לסיכונים שונים עולה בצורה משמעותית כשמתקבלות החלטות שעלולות להיות קריטיות לארגון. כמו כן, ישנה חשיבות לרציפות התפקודית של הארגון, שהביקורת מהווה חלק בלתי נפרד ממנו.

**על אף האמור, במשבר הקורונה מצאה עצמה הביקורת הפנימית בחלק ממשרדי הממשלה "מחוץ למשחק".**

## הביקורת הפנימית במשרדי הממשלה בעת הקורונה

### בנימה אישית

אציין כי ביום בהיר אחד, בתחילת תקופת הקורונה, מצאתי את עצמי, המבקרת הפנימית במשרד להגנת הסביבה, בחופשה בבית, כמו גם כל צוות האגף. וידוי קטן - ביומיים הראשונים חשבתי לעצמי שזו החלטה סבירה בהתחשב בנסיבות (רק 30% הוגדרו כחיוניים לתפקוד הרציף של המשרד) ושאולי מקומו של המבקר הפנימי בעת הזו הוא לא בחזית החירום. אל דאגה.... זה עבר לי... משיחות שקיימתי הבנתי שכמחצית מהקולגות שלי במשרדים האחרים (ולעיתים אף חלק מעובדיהם) המשיכו לעבוד. יצוין כי גם במהלך "החופשה" המשכתי לקחת חלק בישיבות ההנהלה המקוונות ולראות את עצמי כמחויבת למשימות שבאחריותי. בשלב זה הגעתי למסקנה כי זו שעת כושר לפעול לחיזוק מעמד הביקורת ולעיגון פעילותה בזמן חירום.

מבדיקה שנערכה עם נציבות שירות המדינה, עלה כי בתקופת הקורונה רק כ-50% מהמבקרים הפנימיים במשרדי הממשלה וביחידות הסמך הוגדרו כחיוניים והיתר הוצאו לחופשה. לעומת זאת, בשלטון המקומי יצאה הנחיה שקבעה בין היתר כי המבקר הפנימי נמנה על בעלי תפקידים סטטוטוריים חיוניים (ללא שיקול דעת בדבר אי העסקתם).

## דפוסי פעילות של הביקורת הפנימית בתקופת משבר הקורונה

בעת חירום, פעילות הביקורת הפנימית יכולה להתנהל במנעד רחב של סוגי פעילויות: החל מהמשך "עסקים כרגיל", דרך התמקדות בנושאי חירום, ועד עצירת פעילות מוחלטת. בשיחות עם מבקרים פנימיים בזמן המשבר ולאחר החזרה לשגרה, התברר כי הייתה שונות רבה באשר לאופי פעילותם. השונות הזאת באה לידי ביטוי בתרשים בעמוד הבא:

> "מסקר שנערך בחודש מאי 2020 בקרב מבקרים פנימיים ראשיים במשרדי ממשלה, נמצא כי ברוב משרדי הממשלה שנסקרו לא קיימים נהלים או הוראות לפעילות הביקורת הפנימית בעת חירום"

### ביקורת בשעת חרום

ביצוע ביקורות אד-הוק בנושאים הנובעים ממצב החירום, תוך קיצור לוחות הזמנים. הביקורת יכולה להתבצע הן כביקורת בדיעבד והן כביקורת בזמן אמת (תוך כדי תנועה).

### ביקורת מרחוק

ביצוע ביקורת מרחוק, בלי להגיע לאתרים המבוקרים ובהסתמך על המערכות הממוחשבות בארגון.

### ליווי וייעוץ

חבישת כובע ה"יועץ" וליווי מקבלי ההחלטות בזמן אמת.

### "כשהתותחים רועמים - הביקורת שותקת"

הפסקת פעילות הביקורת הפנימית בטענה כי כרגע הארגון צריך להתמקד במשימות החשובות ביותר ואין תרומה ממשית לפעילות הביקורת

### המבקר כמשקיף - תצפיות על ההתנהגות הארגונית בעת חירום

כולל התייחסות לנושא ניהול הסיכונים, הוצאות תקציביות, קיום בקרות, הפלטפורמה המחשובית והסייבר, התיעוד ועוד.

### טיפול בתלונות ציבור בלבד

המבקר הפנימי בשבתו גם כממונה על טיפול בתלונות הציבור, עוסק במתן מענה לתלונות הנובעות ממצב החירום.

### "עסקים כרגיל" אך בעצימות נמוכה

המשך פעילות שוטפת, תוך התחשבות במצב החירום (דחיית פגישות למשל) ומיקוד בשלבי עבודה שאינם מחייבים אינטראקציות עם המבוקרים (כתיבת טיוטות, הכנת תוכנית, ניתוח נתונים ועוד).

### "להיכנס תחת האלונקה" יחד עם הארגון

יציאה מתחומי פעילות הביקורת הפנימית ולקיחת חלק בתפקידים ביצועיים בשעת החירום.

## תובנות

בעת חירום, נדרשים ארגונים (לרבות משרדי הממשלה) לשנות את אופי פעילותם. בדרך כלל שינויים אלו יאופיינו בחריגה מנהלים שבשגרה, "קיצורי דרך" וקבלת החלטות שעלולות להיות בעלות השלכות משמעותיות לארגון לאורך זמן. התנהלות מעין זו טומנת בתוכה פוטנציאל מהותי להתממשות סיכונים ולחריגה מכללי מינהל תקין. על כן, דווקא בעת הזו ישנה חשיבות מיוחדת לכך שהביקורת הפנימית תמשיך בפעילותה, ובין היתר תלווה את הליכי קבלת ההחלטות.

לכל אחד מאופני הפעולה שצוינו למעלה יש יתרונות וחסרונות. ניתן לנתח את פעולת הביקורת הפנימית במשרדי הממשלה בתקופת החירום באמצעות מודל ה-SWOT:





## דוגמה לניתוח פעילות הביקורת באמצעות מודל SWOT

**W**

- תפיסה רווחת היא שהמבקרים הפנימיים אינם מובילים בחזית החירום ולכן אינם חיוניים לתפקודם הרציף של המשרדים.
- אתגר בלימוד מעמיק של נושא החירום בסד זמנים קצר ותוך כדי תנועה.

**S**

- גמישות בביצוע הביקורת והיכולת להתאים את תוכניות העבודה בזמן קצר.
- היכרות הביקורת עם הארגון וראייה מערכתית מאפשרות למבקר לשמש כיועץ ולהשיא ערך לארגון.
- לביקורת סמכות לקבל כל מסמך, להיכנס לכל אתר ולצפות בכל מערכות המידע בגוף המבוקר. סמכויות אלו מקנות לה ראייה מערכתית חיונית בעת חירום.

**T**

- היעדר יכולת לקבל החלטה עצמאית לעניין עבודה בעת חירום בשל הכפיפות למנכ"ל המשרד ולהנחיות נציבות שירות המדינה.
- חשש מחריגה מהוראות חוק הביקורת הפנימית בהתייחס ללקיחת חלק בתפקיד ביצועי במשרד

**O**

- פעילות הביקורת הפנימית בממשלה ובכלל מעוגנת בחוק הביקורת הפנימית התשנ"ב – 1992, בנוהל הנציב ובהנחיות מקצועיות. עובדה זו יש בה כדי לסייע בהמשך עבודת המבקרים בעת חירום כמתחייב על פי החוק.
- לשכת המבקרים פועלת להגן על העצמאות המקצועית, המעמד והזכויות של המבקרים הפנימיים באשר הם.
- בעקבות המעבר של חלק מעבודת המשרדים לעבודת מרחוק, המבקרים יכולים להרחיב את ארגז הכלים ולהסתייע בכלים דיגיטליים בעבודתם השוטפת.

לגישתי, אל לביקורת הפנימית לשבת בחיבוק ידיים, אלא עליה לפעול במהירות לאיתור המוקדים שבהם תוכל להשפיע במסגרת תפקידי הביקורת והייעוץ. בהתאם, על הביקורת לפנות באופן אקטיבי לממונה ולהציע מיוזמתה לעדכן את תוכנית העבודה כך שתבצע ביקורות שישיאו ערך לארגון בנושא החירום. עם זאת, מומלץ שהביקורת תימנע מיציאה מגדרי תפקידה ולא תיכנס לנעליים של בעלי תפקידים ביצועיים, גם אם מבחינת הארגון הדבר נראה נדרש באותו הרגע.

## פנינו לאן?

מתוך הכרה בחשיבות המשך פעילות הביקורת הפנימית בשעת חירום, וכחלק ממגמה כללית של חיזוק הביקורת בשירות המדינה, הוחלט לפנות לגורמים הרלוונטיים כדי לעגן את פעילות הביקורת במשרדי הממשלה בזמן חירום. ואכן, נשלחה פנייה מטעם מרבית מבקרי משרדי הממשלה ויחידות הסמך כי תצא הנחיה הקובעת כי המבקרים הפנימיים בממשלה יוגדרו כחיוניים בעת חירום.

נוסף על כך, מסקר מצומצם שנערך בתחילת חודש מאי 2020 בקרב מבקרים פנימיים ראשיים במשרדי ממשלה, נמצא כי ברוב משרדי הממשלה שנסקרו לא קיימים נהלים או הוראות לפעילות הביקורת הפנימית בעת חירום. על כן, מוצע גם שכל מבקר פנימי במשרדו, בשיתוף עם המנכ"ל, ידאג להכנת "תוכנית עבודה לביקורת הפנימית בעת חירום" שתתווה את עיקרי הפעילויות ואת שיטות העבודה בחירום. כפי שצוין בסעיף ד', ישנו מנעד רחב לאפשרויות פעילות המבקר הפנימי, בהתאם לנסיבות מצב החירום (ביטחוני, רפואי, אסון טבע וכו') ולאופיו של הארגון, כגון המשך "עסקים כרגיל", טיפול בתלונות ציבור, ביקורת בשעת חירום, ביקורת מרחוק, ליווי וייעוץ, ותצפית על התנהלות הארגון. כמו כן, בסיום תקופת החירום, מומלץ לבצע (בשיתוף המנכ"ל) חשיבה מחודשת באשר לתוכנית העבודה המקורית ולהתמקד בנושאי "פוסט קורונה" שעל הפרק.

תקופת חירום, שבה ייקח המבקר הפנימי חלק פעיל כמבקר וכיועץ, תמחיש להנהלת הארגון את היתרונות הגלומים בהסתייעות בביקורות בעיתות חירום ושגרה, תמצב את המבקר כגורם חיוני ורלוונטי, ותתרום באופן ישיר לחיזוק מעמדה של הביקורת הפנימית בארגון.

**ובנימה זו תמיד יש לזכור כי "אם לתקן הכול אין הזמן מספיק, אך כל תיקון ממעט את החיסרון" ("המלביש", ש"י עגנון)**

# "כבר תרמתי במשרד"

## השפעת משבר הקורונה על המגזר השלישי ושינויים הנדרשים ממבקר פנימי

מאת: אולגה פרלמן | MPA, מנהלת ביקורת פנים, JDC International - The Joint
דוד אגרנט | רו"ח, CIA, ראש צוות ביקורת פנים, JDC International - The Joint
מריה אלכסנדרוב | MPA, ראש צוות ביקורת פנים, JDC International - The Joint

"המגזר השלישי", הידוע גם בשם "מגזר ההתנדבות", הוא כינוי לארגונים הפועלים ללא כוונה ליצירת רווח לבעלי המניות ואינם חלק ממוסדות המדינה או השלטון המקומי. מטרת העל הייחודית של מבקרי פנים ב"מגזר השלישי" היא לוודא כי הסיוע לנזקקים/השירות לציבור אכן יגיעו אל אוכלוסיית היעד. **הצלחתה של הביקורת הפנימית בארגונים המעניקים סיוע לנזקקים לא מתבטאת בשורת הרווח ואינה נמדדת בהגדלת המכירות, אלא בהיותה חוליה חזקה ואיכותית בשרשרת שבקצה שלה עומד אדם הזקוק לעזרה - ניצול שואה מרותק למיטה, ילד בסיכון או משפחה רעבה. כלומר, בעבודתנו המקצועית מעורבים היבטים כגון רגש אנושי, מוסר ואתיקה.**

הפעם האחרונה שכולנו חווינו השפעה של משבר גלובלי הייתה בשנים 2008-2009, כאשר משבר כלכלי חמור הכה בעולם. אולם מבחינת השפעתו על ארגונים במגזר השלישי, משבר הקורונה הנוכחי שונה מאוד מהמשבר הקודם מפני שהוא משנה לגמרי את תהליכי העבודה שאנחנו כמבקרים פנימיים הכרנו היטב עד חודש פברואר 2020. לנוסחה המוכרת "משבר = גידול במספר הנזקקים + קיטון בהיקף התרומות" נוספו פקטורים חדשים: כל העולם השתנה, סביבת העבודה של כולנו השתנתה, אוכלוסיית מקבלי הסיוע שינתה את דפוסי פעילותה; ותחשבו איזה שינוי קיצוני עבר על תחום הזקנה... השפעות משבר הקורונה לטווח הארוך לוטות בערפל.

במאמר הזה נציג דוגמאות לשינויים בתהליכי העבודה בארגונים בטווח הקצר, נסקור את השפעת השינויים על עבודת הביקורת הפנימית, וכן ניתן המלצות מניסיוננו.

בנוסף נתייחס לפעילות של יחידת הביקורת הפנימית של הג'וינט במדינות ברית המועצות לשעבר. פעילות הג'וינט באזורים אלו נעשית על ידי יחידה ארגונית מיוחדת שהמטה שלה נמצא בירושלים. לפעילות במדינות ברית המועצות לשעבר מוקצים כ-40% מהתקציב השנתי של הארגון - כ-155 מיליון דולר; היקף הביקורת - מעל 100 ביקורות בשנה





## סקר שבוצע במגזר השלישי בעקבות משבר הקורונה

במהלך אפריל 2020 ערך ארגון הגג של המגזר השלישי, "מנהיגות אזרחית", סקר בקרב יותר מ-300 אלכ"רים. מהסקר עלה כי הפגיעה בארגונים כה אנושה,

עד כי **39%** מתוכם מעריכים בסבירות בינונית עד גבוהה כי **לא ישרדו את המשבר.**

בחודש מאי כבר התברר כי **85%** מן **הארגונים הגדולים** ו-**86%** מן **הארגונים הקטנים** נפגעו.

יותר משני שלישים מן הארגונים דיווחו כי היכולת לספק שירותים נפגעה משמעותית או שהופסקה לחלוטין. בקרב הארגונים קטנים הפגיעה חמורה עוד יותר, **ועבודתם של 38% מהם הופסקה לחלוטין.**

**89%** מן הארגונים מדווחים על **צמצום הכנסות מהמדינה והכנסות עצמיות,** **61%** מדווחים על **צמצום הכנסות מתרומות,**

ובקרב כ-**70%** מהארגונים **הצטמצם היקף העבודה בשכר** ו-**55%** **מהעובדים (בממוצע) הוצאו לחל"ת או פוטרו.**

## שינוי במתכונת הפעילות

שוחחנו עם מספר מבקרים פנימיים במגזר השלישי, והתובנות שלהם ממשבר הקורונה סייעו בגיבוש המאמר. לדברי מר דורון רוזביץ' (רו"ח), מבקר ראשי של החברה למתנ"סים, משבר הקורונה שינה ללא היכר את מתכונת פעילות החברה והמרכזים הקהילתיים.

**עם חידוש הפעילות בחודש יוני 2020, התחדשה גם פעילות הביקורת תוך מתן התייחסות לבחינת תהליכי העבודה תוך כדי המשבר וביציאה ממנו, לצד חשיבה על מיקוד הביקורת בתהליכי העבודה החדשים (בשגרה ובחירום).**

בטווח הקצר, משבר הקורונה גרם למגבלות משמעותיות למבקרים פנימיים במגזר השלישי בביצוע עבודתם. הסיבות המרכזיות לכך הן:

- המבוקרים עסוקים בעניינים דחופים, ולכן "קצרי רוח" ואינם זמינים לביקורת.
- המנהלים חושבים שהביקורת הפנימית לא אפקטיבית מספיק ומהווה מטרד בלתי סביר, בוודאי בתקופת המשבר.
- נוצרו מגבלות במקורות מידע: עקב משבר הקורונה הוגבלה גישה פיזית לאתר המבוקר לשם ביצוע תצפית, הוגבלה גישה למסמכים פיזיים, הוגבלה האפשרות לפגוש פיזית את מקבלי הסיוע/השירות וכו'.
- קוצצו המשאבים ליחידת הביקורת הפנימית.

כמו כן, אירעו שינויים מהותיים בסיכונים, בבקרות, בנוהלי העבודה ובתהליכי העבודה בארגונים. לצורך המחשת עומק השינויים בתהליכי הביקורת, נציג דוגמה בולטת מארגון הג'וינט. אחת מגולות הכותרת של פעילות הג'וינט במדינות ברית המועצות לשעבר היא תוכנית "HOMECARE". במסגרת תוכנית זו הג'וינט מעניק סיוע בעבודות הבית לקשישים, לנכים ולניצולי שואה. התוכנית מופעלת באלפי ערים ויישובים ברחבי העולם ומקיפה עשרות אלפי נזקקים (כ-40% מהם ניצולי שואה) באמצעות אלפי עובדים סוציאליים ועובדי תפעול אחרים.

ייחודיות עבודת השטח של יחידת הביקורת בתוכנית זו התבטאה בהליך ביקורת המחייב "ביקורי בית" (מאות ביקורים בשנה שביצעו צוות המבקרים הפנימיים המקומיים שלנו, לעיתים קרובות בשילוב צוות ביקורת ישראלי). "ביקורי בית" אפשרו לצוות הביקורת לפגוש פנים אל פנים את הקשישים מקבלי הסיוע, לבחון את הצרכים שלהם, לערוך תצפית על מצב שטח המגורים, "לראות בעיניים" את קבלתו של הסיוע במלואו, ולאמת את האינפורמציה אל מול נתונים המופיעים במערכות מידע. לעיתים קרובות ביקורי הבית הניבו מידע רב ואיכותי שהיווה "קצה חוט" להמשך הבדיקה או להרחבתה. אך עקב משבר הקורונה הוקפאו כל ביקורי הבית.

## על קצה המזלג - המגזר השלישי וארגון הג'וינט

המגזר השלישי מעסיק כ-15% מכוח העבודה בישראל ואחראי על כ-6% מהתל"ג. המגזר כולל ארגונים, עמותות, אגודות שיתופיות, חברות לתועלת הציבור (חל"צ), הקדשות, ארגוני צדקה וארגונים בינלאומיים. לפי רשם העמותות, נכון לשנת 2018 היו רשומות בישראל כ-40,000 עמותות (כמחציתן פעילות) וכ-1,300 חברות לתועלת הציבור.

הג'וינט העולמי (American Jewish Joint Distribution Committee), ארגון אמריקאי שבסיסו בניו יורק, הוא הארגון היהודי ההומניטרי הגדול בעולם. הארגון נוסד בשנת 1914 כדי לסייע ליהודים בארץ ישראל ובמזרח אירופה בזמן מלחמת העולם הראשונה, ולאחר מכן המשיך לפעול למען הקהילות היהודיות ברחבי העולם. כיום הארגון פועל ביותר מ-70 מדינות, ופעילותו הענפה משפרת את חייהם של מיליוני אנשים. בשנים האחרונות התקציב השנתי של הארגון העולמי נע סביב 370 מיליון דולר. בשנת 2019 הועסקו בג'וינט העולמי מעל 1,000 עובדים, והארגון מימן אלפי עובדים נוספים כעובדים במיקור חוץ.



catwalker / Shutterstock.com

## שינויים בסדרי עבודת הביקורת הפנימית

### תוכניות ביקורת ממוקדות מעילות והונאות

בתקופת משבר הקורונה נחלשו קווי ההגנה, מערכי הבקרה והפיקוח בארגוני המגזר השלישי. כתוצאה מכך גבר הסיכון להתרחשות מעילות והונאות. מומלץ לגבש וליישם תוכנית ביקורת ממוקדת מעילות והונאות, תוך התייחסות לנושאים הבאים:

- **הפעלת בקרה על תוכניות ואספקת סיוע (או שירות) ללקוחות הקצה** - כדי לוודא כי לקוחות הקצה קיבלו את הסיוע במלוא היקפו בהתאם למדווח במערכות מידע.
- **בנקים** - בחינת העברות בלתי מוסברות של כספים בין החשבונות השונים, שינויים בזכויות חתימה, שימוש חריג בכרטיסי אשראי והמחאות בנקאיות.
- **רכש** - בחינת קיום צורך אמיתי של כמויות ומהות ביצוע הרכש, בחינת רכש ציוד מגן במחירים מופקעים, בחינת חשש לקיום ספקים פיקטיביים, בחינת סדרי אישור ספקים חדשים, רכישות מוצרים/שירותים שלא תואמים את תחום עיסוקם הרגיל של הספקים.
- **שכר ומשאבי אנוש** - בחינת אפשרות של רישום עובדים פיקטיביים שנקלטו בתקופת המשבר, כמו גם תשלומים בלתי מבוססים של שכר וגמול לקבלני המשנה.
- **ניהול קופות מזומנים** - שימושים חורגים במזומנים, גידול בלתי מוסבר במחזור הקופות.
- **רישומי הנהלת החשבונות** - לוודא שמירה על נכסי הארגון מבחינה רישומית ופיזית, בחינת סדרי השמדות נכסים ומלאי, אופן רישום החזרים כספיים.
- **ממשל תאגידי** - בחינת קבלת החלטות וביצוע פעולות "במחטף" - לעניין זה מומלץ לסקור מידע בפרוטוקולים של אורגנים.

## תובנות ודעות

### הרחבת השימוש בסקרים ובשאלונים בקרב לקוחות קצה

מן הראוי להרחיב ככל הניתן את היקפי סקרי שביעות רצון בקרב לקוחות הקצה (בטלפון או באמצעים טכנולוגיים אחרים), כדי לאמת קבלת סיוע או שירות. כתוצר לוואי מתקבל אימות פרטי קשר המופיעים במערכות מידע. פועל יוצא נוסף הוא הפגת בדידותם של הקשישים ומתן תחושה שיש מי שדואג להם ומתעניין בשלומם. לעיתים שיחת טלפון כזאת חשובה לא פחות מהסיוע שהם מקבלים מהארגון.

### ביצוע הערכות סיכונים בטווח הקצר והקפאת ביצוע סקרי סיכונים חדשים

**ייתכן שסקרי הסיכונים שבוצעו לפני משבר הקורונה כבר אינם רלוונטיים ואינם משקפים סיכונים בתהליכים עתידיים בצורה נאותה. לכן רצוי לבצע הערכה תכופה של הסיכונים העיקריים ולפעול בהתאם.**

### גמישות בביצוע תוכנית העבודה השנתית

לאור המציאות המשתנה וצמצום משאבי הביקורת, רצוי לפעול בגמישות ובהתאמה מתמדת של תוכנית העבודה השנתית. כמו כן, יש להתחשב במצב המבוקרים ולפעול ביתר שאת לתיאום עם כל הגורמים הרלוונטיים לגבי אפשרות קיום הביקורות ולגבי הפורמט המתאים ביותר לעריכתה.

### התאמת איסוף ראיות ביקורת למצב החדש

לאור ביצוע ביקורת מרחוק אל מול מבוקרים שעובדים מהבית, יש לחשב מסלול מחדש לגבי אופן איסוף ראיות ביקורת, תוך שימוש באמצעים אלטרנטיביים (צילומי מסך ותיעוד אלקטרוני של תהליכים כגון ביצוע תשלומים ואישורם).

### הבטחת גישה מרחוק לנתונים

כדאי לנצל תקופות "הקלה" שמאפשרות פעילות שוטפת, לשם השגת גישה מרחוק לנתונים אלקטרוניים שישמשו את הביקורת בהמשך.

בנוסף חשוב להגביר את התקשורת בין חברי יחידת הביקורת פנימית

## לסיכום,

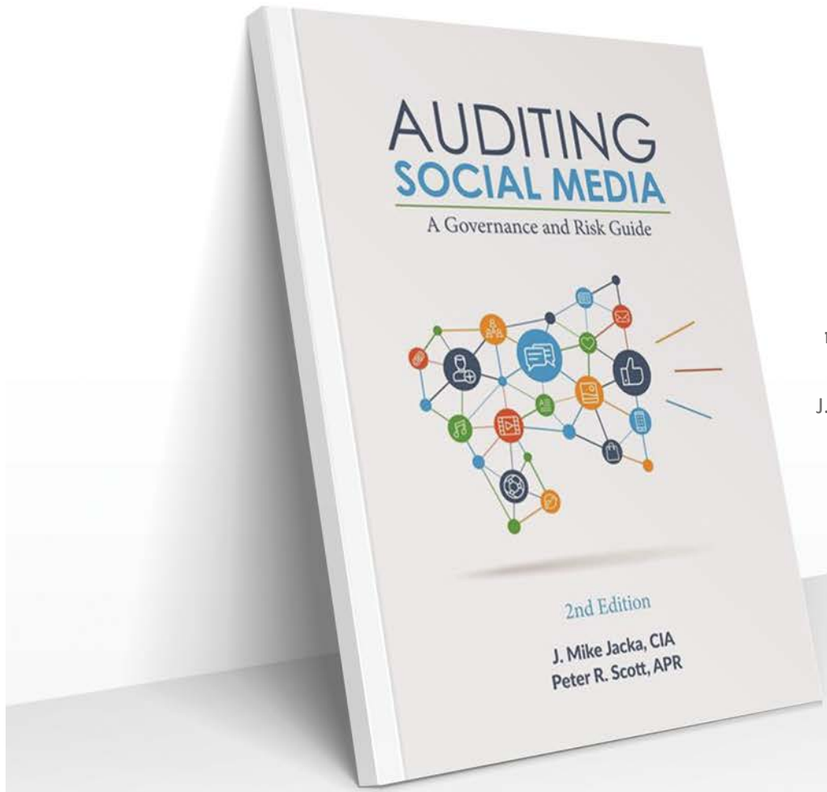
קיים חוסר ודאות לגבי אופן הפעילות העתידי של ארגוני המגזר השלישי, ובהתאם לגבי אופן פעילותם של מבקרים פנימיים בארגונים אלה.

**על יחידות הביקורת במגזר השלישי להתאים את עצמן למצב החדש על מנת להישאר רלוונטיות,**

תוך שאיפה להביא ערך מוסף לארגונים המבוקרים בהווה ובעתיד.

# "שדה הקרב" של העסקים עובר למדיה החברתית – גם המבקר הפנימי מתייצב

מאת: ד"ר יוסי נטוביץ | רו"ח מנכ"ל טיוב יועצי מערכות בע"מ




**המאמר מבוסס על הספר - ביקורת המדיה החברתית - מדריך ממשל וסיכונים (מהדורה II)**

מאת | J. Mike Jacka and Peter R. Scott

בהוצאת: IIA Foundation 2019





## עידן של שיבושים במדיה החברתית

**המדיה החברתית הדיגיטלית פורחת במיוחד בעידן הקורונה, הבידוד והריחוק הפיזי. אנשים מוצאים בה תחליף לפעילות החברתית שנמנעת מהם, וארגונים שכבר גילו את הפוטנציאל העסקי של מדיה זו מגבירים בה את פעילותם.**

אך התמונה לא תמיד ורודה - ביוני 2020, פורסם כי "טבע" הגישה תביעה נגד "אבוט", יבואנית תחליף החלב לתינוקות סימילאק, בטענה ש"פעלה בשיטה פסולה, נפסדת ונכלולית", שבמסגרתה הופעלו פרופילים פיקטיביים של אימהות לצד מגיבות בתשלום ברשתות החברתיות, וזאת כדי להשמיץ את המותג נוטרילון של טבע ולזרוע בהלה וחשש בקרב הורים לתינוקות, תוך הפצת מידע מטעה. לטענת טבע, השיח השלילי שנוצר במדיה החברתית הביא לנפילת פלח השוק של נוטרילון מ-21% ל-17% והסב לה נזק של כ-40 מיליון ש"ח.

תביעה זו ממחישה כיצד המדיה החברתית הפכה כיום לשדה מערכה חדש ואפקטיבי בעסקים מצד אחד, ומצד שני מצביעה על הסיכונים הטמונים בפעילות זו, בייחוד כשהיא נערכת כסוג של פשיטת קומנדו המבוצעת באופן מבוזר על ידי קבוצות ובודדים, "שכירי חרב" חיצוניים, כאשר יכולות הבקרה והפיקוח הניהולי מוגבלים ונזקי השגיאות והטעויות בשיקול הדעת עלולים להיות קולוסאליים.

> "המדיה החברתית עצמה עשויה להוות כלי ביקורת רב עוצמה ובעל ערך למבקר הפנימי"

## רק בת עשר

עידן המדיה החברתית בעסקים החל לפני מעט למעלה מעשור עם נסיקתן של האפליקציות פייסבוק, טוויטר ודומיהן. כתחום חדש יחסית המתרחב במהירות (רק בפייסבוק למשל, נכון להיום פועלים למעלה מ-2.6 מיליארד משתמשים בחודש), ואף שעסקים פועלים במדיה מאז היווסדה, עדיין מורגשת חסרונה של תורה סדורה של ניהול סיכונים, בקרות וביקורת. לכן שמחתי שלאחרונה יצא ספרם העדכני של Scott-וJacka "ביקורת המדיה החברתית - מדריך ממשל וסיכונים" שעוסק בנושא. הבשורה שעולה ממנו - ביקורת המדיה החברתית מביאה ערך רב לארגון, אבל יותר מכך - המדיה החברתית עצמה עשויה להוות כלי ביקורת רב עוצמה ובעל ערך למבקר הפנימי.

## תועלות וסיכונים

למרות שמו, הספר לא נועד למבקרים פנימיים בלבד, גם מנהלים ימצאו בו ספר לימוד שיטתי שמציע תובנות עסקיות על המדיה החברתית. המדיה החברתית היא לא רק כלי אפקטיבי לשיווק ולפיתוח מותגים ולמכירות, אלא טומנת בחובה תועלות עסקיות. ארגונים משתמשים במדיה חברתית למטרות שונות, ובהן גיוס "טאלנטים" ורתימת לקוחות ועובדים כממליצים לארגון. כמו כן,

**ערנות ומעורבות בשיח ברשתות החברתיות יכולות לסייע לארגון לחשוף ולתקן חולשות ואף לטפל במשברים.**

במקביל, המחברים מנתחים ביסודיות את הסיכונים ואופן ההתמודדות עימם. הסיכון הברור הוא נזק לתדמיתו של הארגון כתוצאה משיח שלילי. אולם קיימים גם סיכונים נוספים ובכללם אבטחת מידע, כולל דליפת מידע ונכסים אינטלקטואליים; פשעי מחשב רלוונטיים כגון דיוג, וירוסים, רוגלה וכופרה; הסחת דעת של עובדים במהלך העבודה; סיכוני ציות לחוק ולרגולציה, כולל חשיפה לתביעות כתוצאה משימוש במידע שאיננו נכון ("Fake News"). סיכונים עלולים לנבוע גם מאסטרטגיה לא אפקטיבית, או גרוע מכך - היעדר אסטרטגיה והתעלמות מהמדיה החברתית.

מעניין לגלות כי בדרך כלל המקור לסיכונים איננו במדיה עצמה. היא בסך הכול משקפת בעיות אמיתיות בתפעול הארגון עצמו. למשל, אם הארגון לא פועל נכון בנושא מסוים, קרוב לוודאי שהתלונות על כך מצד לקוחות ובעלי עניין יהדהדו במדיה החברתית ויגרמו ל"כאב ראש" לארגון. זוהי תובנה חשובה במיוחד למבקר ועוד נחזור אליה בהמשך, אבל חשוב להבין שהתמודדות נבונה עם תלונות אלה, ולא התעלמות או התכחשות, יכולה לתקן את הנזק במידה רבה.

## מדיה חברתית אינה חינם

בניגוד לטעות נפוצה, הפעילות במדיה החברתית איננה חינמית, היא דורשת השקעת משאבים רבים. אולם כאשר מבצעים אותה נכון החזר ההשקעה גבוה. יצירת קשרים חברתיים טובים ובריאים עם לקוחות משתלמת מאוד. מאידך, ניהול חובבני ולא מושכל של המדיה החברתית עלול לעלות ביוקר.

ואכן, 14 פרקי הספר מציגים לעומק את הצורך בניהול שיטתי ומפוקח של הפעילות הארגונית ברשת החברתית, ובכלל זה הגדרת גופי ממשל ופיקוח, קביעת אסטרטגיה, הכנת תוכניות טקטיות, בניית מדדים, ניטור השיח החברתי, פיתוח וניהול מותג ומוניטין, קביעת מדיניות, ציות לרגולציה, הדרכות וניהול ספקים. כל אחד מן הפרקים מסביר מהו ה-Best Practice של הנושא תוך הבאת אנקדוטות להמחשה מעולם העסקים.

## בקבוק קטשופ להמחשה

לדוגמה, אחד הנושאים החשובים בניהול ובקרה (על אף שבמבט ראשון הוא עלול להראות אזוטרי) הוא עריכת אינוונטר של החשבונות שהארגון ועובדיו פתחו ברשתות החברתיות השונות. עם השנים הארגון עובר לפלטפורמות חברתיות מתקדמות יותר, יוזמות חדשות נפתחות והקודמות נזנחות, ובנוסף עובדים מתחלפים. כך מצטברים במדיה עשרות חשבונות ארגוניים ויותר.

**היעדר תיעוד ופיקוח על אינוונטר החשבונות יכול לסכן את הארגון בקיום חשבונות ישנים עם פעילות בלתי מנוטרת שתוכנם לא תואם למדיניות הארגון.**

בשנת 2015 ערכה חברת המזון Heinz מבצע שבמסגרתו הוטבע על כל בקבוק קטשופ קוד QR לסריקה שהפנה את הלקוחות לכתובת של אתר אינטרנט מיוחד. בתום המבצע החברה זנחה את כתובת ה- URL הזאת והיא נרכשה על ידי חברת אתרי רשת מפוקפקים, וכך יצא שמשפחה שרצתה לצפות באיחור בתוכן המקודם על ידי הבקבוק של חברת Heinz מצאה את עצמה מופנית לאתר פורנו... למזלה של החברה לא הרבה לקוחות המשיכו להתעניין בקוד ה-QR לפני שהדבר התגלה, אבל הלקח ברור: יש צורך לטפל בהוצאה מסודרת משימוש של חשבונות ישנים, ואם המבקר הפנימי מסייע בהקמה ובעדכון מצב אינוונטר החשבונות, הרי שכבר בזאת השיא ערך נכבד לחברה.

## תוכנית ביקורת "מסורתית"

המבקר הפנימי ימצא בספר לא רק ניתוח עיוני של תחום ביקורת חדש ומרתק זה אלא גם מדריך מקצועי שימושי. בפרק החותם את הספר מוצעת תוכנית ביקורת מפורטת הכוללת היבטים ניהוליים רבים, ובכל אחד מהם מוצגת הגדרת הסיכונים והמטרות, נקודות לבדיקה, שיטות וטכניקות. תוכנית זו יכולה לשמש את הביקורת הפנימית בכל ארגון כבסיס לפיתוח תוכנית ביקורת מותאמת.

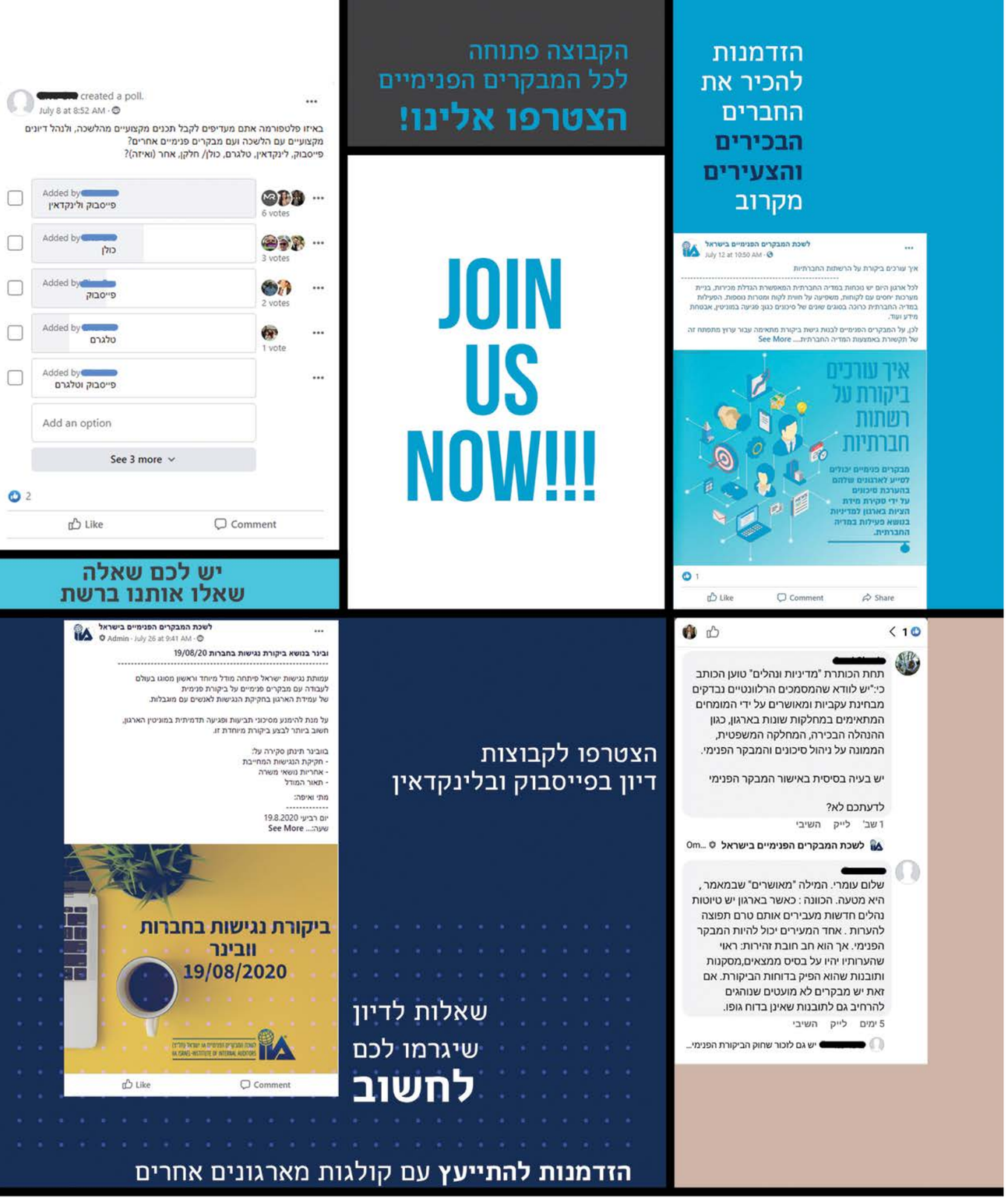
עם זאת, מאכזב לגלות שלמרות החדשנות והטכנולוגיות המאפיינת רשתות חברתיות, השיטות וטכניקות הביקורת המוצעות בספר נותרו מסורתיות. תוכנית ביקורת השטח של הספר מבוססת בעיקר על סקירת מסמכים וראיונות או דיונים עם בעלי תפקידים, ואין בה הצעות לשילוב טכניקות וכלים ממוחשבים כלשהם. אומנם הספר מציג בנספח נפרד רשימה אלפביתית ממצה של כלים ומקורות באינטרנט, אך היא נטולת הסבר והקשר ספציפי, וחבל. סוגים שונים של כלים ממוחשבים עשויים להעלות את האפקטיביות של הביקורת ואף זמינים באינטרנט בעלות חודשית נמוכה יחסית, לדוגמה:

- ניטור השיח - זיהוי והעברה באופן מיידי של כל מסר שנכתב על הארגון ברשתות השונות.
- "ניתוח סנטימנט" - ניתוח אגרגטיבי של מסרים לזיהוי הלך הרוח הכללי ברשתות החברתיות, חיובי או שלילי, ביחס לארגון ולמותגים שלו.
- הפצה ומעקב תכנים - כלים שמסייעים לארגון להפיץ תכנים בערוצים החברתיים השונים ולזהות את היקף ההתייחסות והתגובות ועוצמתן.

> "מבקר פנימי שיתחבר לרשת החברתית יוכל לזהות בעיות בארגון שאף אחד לא מספר לו עליהן."

## בין השורות: המדיה החברתית - גם כלי אפקטיבי לביקורת

הערה אחרונה לסיכום: המדיה החברתית מוצגת בספר כמושא לביקורת פנימית, אולם בין השורות מחלחלת תובנה נוספת - הרשת החברתית עצמה עשויה להוות כלי עבודה אפקטיבי בשירות הביקורת הפנימית. מבקר פנימי שיתחבר לרשת החברתית יוכל לזהות בעיות בארגון המציקות ללקוחות ואולי אף לעובדים ולשותפים עסקיים, שאף אחד לא מספר לו עליהן. אומנם בעבר לקוחות התבקשו לפנות בתלונות והערות לתיבת התלונות של הארגון, אך היום חלקם הגדול לא ימצא בכך טעם ויעדיף לשתף את תחושותיו עם חבריו לרשת. באמצעות המדיה המבקר הפנימי יכול לחשוף בעיות אמיתיות בארגון הדורשות טיפול: תהליכים לא יעילים ומסורבלים, מדיניות לקויה, והיעדר בקרות נדרשות. מידע זה יסייע לו לזהות חולשות ולמקד בהן את משאבי הביקורת המוגבלים שברשותו ולספק בכך יותר ערך מבורך להנהלה. אבל זה כבר אולי נושא לספר אחר.



# Editor's Note

**Sharon Witkowski Tabib,** CPA, CIA, CRMA
Vice President of IIA Israel - Institute of Internal Auditors

We published the last edition in March 2020, at the peak of the coronavirus crisis. It appears that, within the global crisis caused by the pandemic, organizations are managing sub-crises and the system needs to act quickly, under pressure and under enormous uncertainty – very bad conditions for decision-making.

It is now clear to everyone that this is not a transient crisis, but rather a new reality that will accompany us for many months, or even years – the New Normal.

The new reality that was forced on us constitutes a clear manifestation of a crisis that embodies threats and risks, but also opportunities, in both the personal sphere (such as 'rediscovering our families') and the professional sphere (streamlining work processes without compromising quality).

To assess the impact of the coronavirus crisis on internal auditing, the IIA disseminated a survey in North America in April 2020. In July, we disseminated a similar survey in Israel, with the objective of analyzing the changes that occurred in Israel as a result of the crisis compared to the IIA survey. The highlights of these surveysare presented in this edition. The survey found that internal auditing in Israel is swift, flexible and rapidly responds to changes. The survey also found that significant changes have occurred in internal auditing work: in the volume of manpower, annual work plans and auditing assignments themselves.

The theme of this edition is "Era of Disruptions" and we divided the articles into several categories:

**Disruptions and innovations:** risk assessment in a post-pandemic world, innovation during crisis – the pandemic's challenges as opportunities, how to implement and manage remote working.

**Tools and work practices:** internal auditing during an era of crises – the material and existential risk that are now part of corporate risk management, the challenge of "getting out in the field" and the advantages of "alertness testing", managing cyber events and more.

**Insights and opinions:** auditors share their experiences: the push for changes in internal audit in coronavirus times; the changes internal auditors had to make in response to the disruptions; the standing of the internal audit function in government ministries during times of emergency; the impact of the coronavirus crisis on the third sector etc.

We must make significant changes in processes and even in our perceptions, and this period is testing internal auditors: Are we ourselves implementing the ideas? Are we ourselves capable of changing and adjusting to the new and emerging reality? Are we preoccupied by all these adjustments or are we taking the lead in reactivating processes that became stuck during the crisis? Are we waiting to be called upon or are we taking initiative? Are we serving as personal and organizational role models?

As we approach the new year, I hope that we will succeed in being leaders who points out the ray of light in every situation and grow from it.

I want to close by quoting one of the customary biblical blessings prior to Rosh Hashanah: "May we be the head and not the tail."

**I wish you enjoyable and inspiring reading,**
**Happy New Year and robust good health**

**Sharon Witkowski Tabib**



# President's Note

**Doron Ronen,** CPA, CIA, CRMA
President of IIA Israel – Institute of Internal Auditors

The coronavirus pandemic is challenging the world. Countries, organizations and individuals are contending with unprecedented health, economic and operating difficulties and persisting uncertainty with no end in sight.

The pandemic has also jolted the IA profession, prompting questions such as: How essential is IA? How can IAs help organizations contend with this situation? Should the current paradigms be revamped? Etc. This edition's topic is **"Era of Disruptions"** and it elaborates on this issues.

A few months ago, I was elected as IIA Israel's president and I thank for the confidence in my ability to lead the institute during this challenging period. We will maintain the professionalism of our institute and work for the benefit of our members and of our profession. We will continue to provide our members with knowledge and tools: conferences and courses, academic studies, a professional journal, standards and professional guidelines, responses to professional questions, legal and professional umbrella for our members and cooperative efforts with organizations in Israel and abroad.

I wish to thank CPA **Doron Cohen**, who concluded his office as IIA Israel's first president, after having been appointed as a major company's CEO. Doron initially held office as IIA Israel's president and, after leading the professional organizations' merger, on behalf of IIA Israel, he held office as the unified IIA Israel's president.

When Israel and the entire world are contending with an economic crisis and with technological developments, it becomes even more essential for IAs to provide real and meaningful added value and to strengthen their organizations as key gatekeepers. We also contribute to improving the intraorganizational controls and processes.

The pandemic has presented IIA Israel with complex challenges. Despite the difficulties, we defined committees' charters, offered numerous distance learning webinars and courses, drafted position papers (including on the above topics), approved professional guidelines that are unique to Israel (such as the IA's role as an ombudsman), launched for the first time an LLM program specializing in IA, added considerable professional material to our website and we are getting our getting ready for the annual professional conference to be held on 21.1.21.

We also launched a strategy committee that will focus on the IA's role in the future. Concurrently, we are holding a competition to scout for innovative young auditors who will be recognized during the annual conference.

**I appeal to IAs who have not yet done so, to join IIA Israel**. Many important matters are on our agenda: IA's status , the IA Law, and more. A large and strong IIA Israel can promote topics effectively and contribute to IAs entire community.

In addition to the committees, we also assembled a variety of forums: sectoral (financial, governmental companies, government ministries, local authorities); **professional specializations** (risk management, fraud and embezzlement, innovation and analytics, data security and cybersecurity), a forum for chief **auditors and a young auditors forum**.

**Any member wanting to promote a topic in IIA Israel is invited to do so; we will succeed in advancing our profession and members only by working together!**

**Best wishes for a happy, healthy and resilient new year**
**and a speedy return to normalcy,**
**Yours faithfully,**
**Doron Ronen**

Editor — **Sharon Witkowski Tabib,** CPA, CIA, CRMA

Vice Editor — **Oren Shachar,** CPA, CIA, CISA, MBA

Editorial Team — **David Agranat,** CPA (Isr.), CIA

**Boaz Aner,** CPA, CIA, MA

**Dror Bar Moshe,** CPA, LLM, CIA, CISA, CRMA, CRISC

**Shlomit Eitan,** Adv, CIA

**Yosi Elias**, CPA

**Nava Halamish,** CPA, MA

**Chen Katz,** CPA, EMBA, CIA

**Dr. Joseph Natovich,** CPA

**Eyal Oron,** Adv

**Doron Ronen,** CPA, CIA, CRMA, QAR, CRISC, CFE, MA, LLM, CSX-F, CDPSE

**Dr. Gabi Sayag,** D.E.A

**Lior Segal,** Adv. CPA, MBA

**Margalit Sperber,** CPA, MBA, CIA

**Nancy Zakak Abu Elnaser,** CPA, MA, QAR

President's Office Manager — **Inna Golderbiter**

Graphical Design — **Studio Daga**

Linguistic Editing — **Udi Levinger**

Publisher — **IIA Israel Institute of Internal Auditors**

IIA Israel Institute of Internal Auditors
Address in Israel: **PO box 29281, Tel Aviv, 6129201**
Tel: **03-5116617** | Fax: **03-5116647** | For comments and remarks: **office@theiia.org.il**

The views expressed in the articles are the Authors' opinions. IIA Israel. carries no responsibility regarding them. All rights reserve to IIA israel Institute of Internal Auditors

**July 27, 2020**

**אנו נפרדים מנשיא ומנכ"ל ה IIA העולמי מר ריצ'רד צ'יימברס**
**לאחר הודעת הפרישה שלו, להלן מכתב שנשלח אליו:**

**Dear Richard,**

We witnessed your notice to IIA Global Board of your desire to step down as President and CEO of the IIA as of March 31st 2021 to pursue other career and family objectives. While this is sad news for the IIA, we are sure you recognize, as we do, your outstanding contribution to the IIA, to IIA affiliates, volunteers and the business community for over 12 years.

You were appointed as President and CEO 12 years ago (during the Great Recession) bringing with you decades of experience in Internal Audit. You have led the IIA to record membership levels, certifications and financial performance, with outstanding revenues and members in nearly 200 countries and territories.

You are undoubtedly the best advocate and global voice of Internal Audit, your passion and enthusiasm for internal audit, and your global advocating voice of the profession has elevated the IIA to new heights.

IIA Israel Board is extremely grateful for your long-time support to our institute, we cherish good memories from yours and Kim's visits to Israel which helped us and enabled an even stronger institute after the unification of the two Israeli entities.

We take this opportunity to thank you personally for your wisdom, leadership, attentive ear, friendship, integrity and courage. Your experience as an internal auditor, your knowledge and expertise on matters relating to the IIA particularly and Internal Audit in general is second to none. You will be missed as President and CEO and we and others will appreciate if you will continue to play a role as consultant in some capacity with the IIA into the future.

While you will be greatly missed, we are certain you will leave the IIA strong and healthy for a great future and a smooth transition for your successor. We wish you well with new endeavors.

You will always have friends here in Israel.

**Doron Ronen**, CIA, CRMA
President
IIA Israel

**Doron Rozenblum**, CIA, CRMA
VP & International Institutes Liaison
IIA Israel

THE INTERNAL AUDITOR JOURNAL