

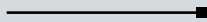
בינה מלאכותית
וביקורת פנימית
עמ' 6



מביטים אל העתיד:
על בינה (מלאכותית),
GPT וביקורת
עמ' 16



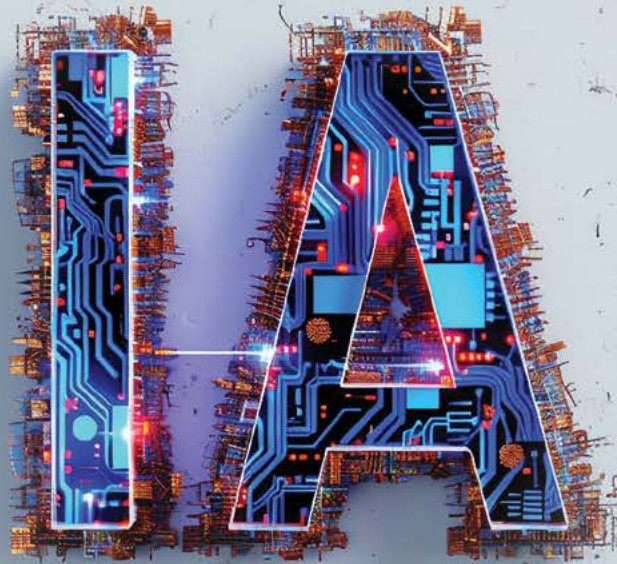
האם הטייטל שלנו
מגדיר אותנו?
עמ' 20



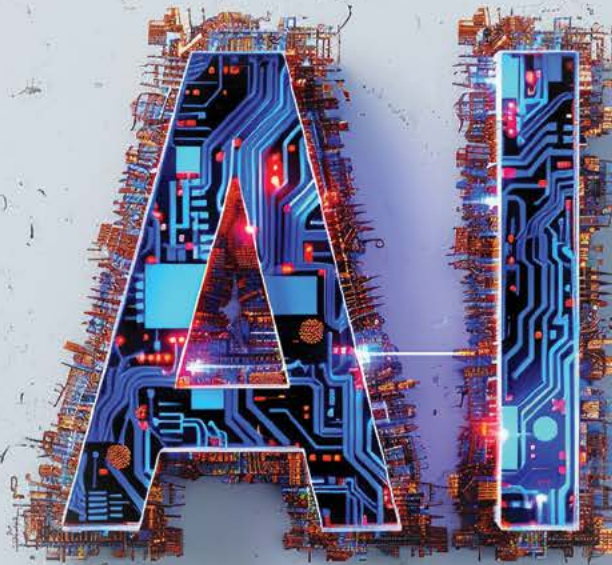
תמורות וחידושים
בתקנים מקצועיים
עמ' 32



ביקורת מעקב אחר
יישום המלצות
עמ' 44



WITH



תוכן עניינים

דבר הנשיא	4	דברים
דבר העורך	5	
בינה מלאכותית וביקורת פנימית	6-9	
בדיקות אנומליה כלי AI בשירות הביקורת הפנימית	10-14	
מביטים אל העתיד על בינה מלאכותית, GPT וביקורת	16-19	
האם הטייטל שלנו מגדיר אותנו?	20-24	
איום הולך וגובר	26-30	
תמורות וחידושים בתקנים המקצועיים הגלובליים	32-37	
צועדים אל העתיד	38-43	
ביקורת מעקב אחר יישום המלצות	44-47	
מתודולוגיה לביקורת פנימית בפרויקטים טכנולוגיים	48-52	
אבטחה נאותה וביקורת של מכשור רפואי במוסדות רפואיים	54-58	
Editor's note	60	דברים
President's note	61	

עורך כתב העת _____ **ליאור סגל** | עו"ד, רו"ח, MBA, CIA, CRMA, QAR, CISA, CISM, CRISC, CDPSE

חברי המערכת _____ **דרור בר משה** | רו"ח, CDPSE, AWS - CP, LLM, CIA, CISA, CFE, CISM, CSX-F, CRMA, CRISC

גרשון לוינסקי | רו"ח, MBA, CRMA

שלום כהן | רו"ח CIA

ד"ר נועם קוריאט | CISA

שרון ויטקובסקי טביב | רו"ח, CIA, CRMA

אורן שחר | רו"ח, MBA, CISA, CIA

דוד אגרנט | CIA, רו"ח

איל אורון | עו"ד

ננסי זכאכ אבו אלנסר | רו"ח, MA, QAR

נאוה חלמיש | רו"ח, MA

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

ערן שחף | עו"ד, MBA

אסף כרמון | CIA, CISA

לשכת המבקרים הפנימיים _____ אינה גולדרביטר ועדי חזוט

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 03-3742627 | 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, QAR, CRISC, CSX-F, CDPSE, CFE, MA, LLM
נשיא לשכת המבקרים הפנימיים IIA ישראל

ימים קשים עוברים על כולנו כאומה. אנו מקווים שאתם ומשפחותיכם בריאים, שומרים על אופטימיות וביחד נצח במערכה. אנו מבקשים להביע את תנחומינו למשפחות השכולות, מאחלים איחולי החלמה לפצועים, ומייחלים לשובם המהיר של החטופים ושל החיילים. אנו מביעים את תמיכתנו בכוחות הביטחון המתמודדים במערכה.

התקופה האחרונה, תקופת מלחמה, הינה תקופה קשה ומורכבת לכל עם ישראל. עם זאת, אנו רואים חשיבות רבה בהמשך פעילות סדירה של הלשכה, שמירה על מקצועיות ומתן מענה לכל המבקרות והמבקרים.

בנימה זאת אעדכן בקצרה על עיקרי הפעילות, שנעשתה:

הוועדה המקצועית פרסמה קווים מנחים - ביקורת פנימית בעת משבר (מלחמת "חרבות ברזל"), והמלצות לעבודה סינרגטית בוועדת הביקורת ככלי להמשכות עסקית בשעת חירום. **התקנים המקצועיים הגלובאליים** החדשים של ה- IIA יצאו לאור, והם תורגמו ע"י הוועדה המקצועית והופצו לחברים. במאמר פרי עטי בגיליון זה, סקרתי את התמורות והחידושים בתקנים המקצועיים הגלובאליים.

ועדת כנסים והשתלמויות הובילה פעילות ענפה במגוון קורסים, סדנאות, ערבי עיון וכנסים, וכן ייזום וריכוז אקדמי של לימודים אקדמיים במספר מוסדות.

הנושא המרכזי **בכנס השנתי** המוצלח שלנו היה AI. אורח הכבוד היה מבקר המדינה, רו"ח מתניהו אנגלמן, שתיאר את החדשנות בביקורת המדינה בשנת 2024. ר' התכנית הלאומית לבינה מלאכותית, ד"ר זיו קציר, סקר את פעילות יחידתו. המושבים המקצועיים כללו הרצאות בנושאים כגון כלי MRI, ChatGPT, שימוש ב- AI בעבודת הביקורת הפנימית, המפץ הדיגיטלי, ניהול סיכונים ועוד.

המשכנו לחזק את הקשרים עם **הרגולטורים** ועם **לשכות אחיות**. נפגשנו עם מנהלת היחידה לאסדרת **מקצוע** הביקורת הפנימית (משרד המשפטים) בעניין תיקוני חקיקה. פרסמנו נייר משותף ללשכה ולאגוד הדיקטורים בנושא ביקורת בעת מלחמה. המשכנו בפעילות של **ועדות ופורומים מקצועיים** שונים.

אני מברך את מערכת כתב העת בראשות **ליאור סגל** על הגיליון והמאמרים המקצועיים בנושא **AI**.

אסיים בבקשה, למי שטרם עשה זאת, **להצטרף ללשכה**, כדי שנוכל להמשיך ולהגביר את הפעילות הענפה לחיזוק המקצוע והעוסקים בו.

בריאות, חוסן, עשייה וצמיחה, ושנזכה במהרה לימים שקטים.
החלמה לפצועים, ושובם המהיר של החטופים ושל החיילים.
בברכת שנה טובה,

שלכם ובשבילכם,

דורון רונן

דבר העורך

ליאור סגל | עו"ד, רו"ח, CIA, CRMA QAR, CISA, CISM, CRISC, CDPSE

אני נרגש להציג את גיליון מספר 18 של לשכת המבקרים הפנימיים IIA ישראל, שעוסק בנושא "IA with AI".

זהו הגיליון הראשון שזכיתי לערוך, ואני מבקש להודות לשותפי לראשות המערכת, שלום כהן, גרשון לוינסקי ודרור בר משה. תודה גם לשרון ויטקובסקי-טביב, שערכה בנאמנות ובמסירות את כתב העת במשך 15 גיליונות.

לנושא הבינה המלאכותית יש חשיבות רבה מפני שהוא משנה את העולם המודרני ומזמן הזדמנויות ואתגרים רבים. בעידן שבו נתונים ואלגוריתמים הם חלק בלתי נפרד מתהליכי קבלת ההחלטות בארגונים, הביקורת הפנימית נדרשת להבין לעומק את השימוש ב-AI ואת הסיכונים הנלווים לו כנושא מבוקר. בנוסף, ה-AI הוא כלי חשוב ויעיל לביצוע ביקורת פנימית. יכולות האוטומציה, ניתוח נתונים וזיהוי הדפוסים יכולות להגביר את אפקטיביות הביקורת, ולכן היכולת לעבוד עם AI היא הכרחית למבקרים הפנימיים בעידן הדיגיטלי. הנושא גם זכה למקום משמעותי בכנסים שקיימו השנה לשכת המבקרים הפנימיים IIA ישראל ולשכת המבקרים הפנימיים העולמית.

בין המאמרים הכלולים בגיליון, אפנה את תשומת ליבכם למאמרים הבאים:

• במאמר "בינה מלאכותית וביקורת פנימית", מציין המחבר מספר אזורים שבהם ה-AI יכול לסייע לביקורת הפנימית.

• במאמר "כלי AI בשירות הביקורת הפנימית", הכותבים טוענים שה-AI יכול להציע יתרונות משמעותיים באמצעות אוטומציה של פעילויות הביקורת הפנימית, שיפור איכות וערך הביקורת, ומתן הבטחה וניטור מתמשכים.

• במאמר "מביטים אל העתיד – על בינה מלאכותית, GPT וביקורת", מנתח המחבר את השפעת ה-AI, ומציג את ההזדמנויות והאתגרים הרלוונטיים לביקורת הפנימית.

• במאמר "האם הטייטל שלנו מגדיר אותנו?", מתחבטים הכותבים בשאלה האם הטייטל הארגוני משפיע על תפיסת העולם של גורמים אחרים בארגון, ואפילו על תפיסת העולם שלנו, לגבי מהות התפקיד שלנו או מקומנו בארגון.

• במאמר "איום הולך וגובר", נטען כי ככל שארגונים משתמשים יותר ב-AI, כך הם נחשפים לסיכונים סייבר ופרטיות שיתקשו להתגבר עליהם.

בגיליון מספר מאמרים מעניינים ומועילים נוספים.

ברצוני להודות לוועדה המקצועית ולעומד בראשה דורון רונן על פרויקט תרגום התקנים המקצועיים הבינלאומיים לעברית. התקנים החדשים, שקדם לפרסומם הליך דיונים ארוך של ועדת התקנים הבינלאומיים, הם בעלי השפעה רבה על כל העוסקים בביקורת הפנימית, וככל הנראה נעסוק בהם בגיליונות עתידיים. להרחבה ראו מאמר בהמשך הגיליון העוסק בכך.

תודה לכל חברי מערכת כתב העת.

אני מצטרף לברכותיו של נשיא הלשכה, דורון רונן, ומייחל לשובם המהיר של החטופות והחטופים ושל התושבים המפונים לבתיהם.

ליאור סגל



בינה מלאכותית וביקורת פנימית



מאת:

דרור בר משה | ר"ח, מבקר פנימי ראשי סייבראק
LLM, CIA, CISA, CISM, CFE, CRISC, CRMA,
CSX-F, CDPSE, PMP, AWS-CP

הביקורת הפנימית מתמודדת עם אתגרים רבים בסביבה המורכבת והדינמית של ימינו, כגון משאבים מוגבלים, ציפיות גבוהות של מחזיקי עניין וסיכונים מתהווים. זה המקום שבו בינה מלאכותית יכולה להציע יתרונות משמעותיים על ידי אוטומציה של פעילויות הביקורת הפנימית, שיפור איכות וערך הביקורת, ומתן הבטחה וניטור מתמשכים.

מהי בינה מלאכותית וכיצד היא יכולה לעזור לביקורת פנימית?

בינה מלאכותית היא מונח רחב המקיף טכנולוגיות שונות שיכולות לבצע משימות הדורשות בדרך כלל אינטליגנציה אנושית, כמו חשיבה, למידה, קבלת החלטות ועיבוד שפה.

בינה מלאכותית יכולה לסייע לביקורת פנימית במספר דרכים, למשל:

ניתוח נתונים

בינה מלאכותית יכולה לעבד מערכי נתונים גדולים ומורכבים, לזהות דפוסים וחריגות ולייצר תובנות והמלצות. הדבר יכול לשפר את ההיקף, הדיוק והיעילות של בדיקות הביקורת, וכן לסייע בזיהוי ומניעה של הונאות וטעויות.

להלן דוגמאות לאופן שבו בינה מלאכותית יכולה לעזור לביקורת פנימית בניתוח נתונים:

עיבוד שפה | כדי לנתח נתונים מבוססי טקסט, כגון חוזים, מדיניות ונהלים, ולחלץ מהם מידע רלוונטי ותובנות רלוונטיות (לדוגמה, יישומים המאפשרים כרייה של תובנות ממסמכים עם מידע מובנה).

הבנת שפה | כדי לעבד ולפרש את המשמעות וההקשר של נתונים לא מובנים, כגון מיילים, הקלטות קוליות והודעות צ'אט, ולזהות ראיות ומידע רלוונטיים למטרות ביקורת (לדוגמה, יישומים המאפשרים כרייה של תובנות מתוך מיילים והקלטות).

למידת מכונה | כדי לזהות חריגים וסטיות בנתונים מספריים, כגון עסקאות, חשבוניות ותשלומים, ולזהות תרחישים וסיכונים פוטנציאליים (לדוגמה, זיהוי חריגים בתשלומים על סמך נתוני עבר).

זיהוי תווים אופטי | כדי לסרוק ולבצע דיגיטציה של מסמכים מבוססי נייר, כגון קבלות, חשבוניות ושוברים, ולהמיר אותם לנתונים אלקטרוניים שניתן לנתח ולבקר.

למידה עמוקה | כדי לנתח נתונים מורכבים, כגון תמונות, סרטונים וקובצי אודיו, ולזהות הונאות וחריגים, כגון חתימות מזויפות, מוצרים מזויפים ורשומות מזויפות.

ניתוח נתונים הוא אחת המשימות הגוזלות זמן רב ועתירות עבודה עבור מבקרים פנימיים. לעיתים קרובות הדבר כרוך בעבודה ידנית שחוזרת על עצמה, כגון דגימה, מיון וסינון נתונים. באמצעות AI מבקרים פנימיים יכולים להפוך משימות אלו לאוטומטיות ולהתמקד בהיבטים מורכבים ושיפוטיים יותר של ניתוח נתונים, כגון פרשנות ואימות התוצאות וניסוח והעברת הממצאים וההמלצות.

עיבוד שפה טבעית | NLP

Natural Language Processing

עוסקת בעיקר במתן יכולת למחשב לתמוך בשפה אנושית ולתפעל אותה. הדבר כרוך בעיבוד מערכי נתונים של שפה טבעית באמצעות גישות למידת מכונה מבוססות כללים או הסתברותיות. המטרה היא שמחשב יהיה מסוגל "להבין" תוכן של מסמכים, לרבות הניואנסים, ההקשרים של השפה בתוכם. לאחר מכן הטכנולוגיה יכולה לחלץ במדויק מידע ותובנות הכלולים במסמכים, וכן לסווג ולארגן את המסמכים עצמם.

הבנת שפה טבעית | NLU

Natural Language Understanding

היכולת של מחשב להבין את השפה האנושית. אפשר להשתמש בה עבור יישומים רבים, כגון צ'אטבוטים, עוזרים קוליים ושירותי תרגום אוטומטיים.

למידת מכונה | ML

Machine Learning

תחום העוסק בפיתוח וחקר של אלגוריתמים סטטיסטיים שיכולים להכליל ביעילות וכך לבצע משימות ללא הוראות מפורשות.

זיהוי תווים אופטי | OCR

Optical Character Recognition

טכנולוגיה להמרה של תמונה, טקסט מודפס או טקסט כתוב בכתב יד למסמך תמליל ממוחשב.

למידה עמוקה | Deep Learning

שיטה המלמדת מחשבים לעבד נתונים בהשראת המוח האנושי. מודלים של למידה עמוקה יכולים לזהות דפוסים מורכבים בתמונות, בטקסטים, בצלילים ובנתונים אחרים כדי לייצר תובנות ותחזיות מדויקות. ניתן להשתמש בשיטות למידה עמוקה כדי להפוך משימות שדורשות בדרך כלל אינטליגנציה אנושית למשימות אוטומטיות, כמו תיאור תמונות או תעתיק קובץ קול לטקסט.

מיליון מונחים

הערכת סיכונים

בינה מלאכותית יכולה לנטר ולנתח מקורות נתונים פנימיים וחיצוניים, כגון דוחות כספיים, מדיה חברתית וחדשות, ולספק התראות ועדכונים בזמן אמת על סיכונים מתהווים ומשתנים. זה יכול לעזור למבקרים פנימיים לתעדף ולהתמקד בתחומי הביקורת הרלוונטיים והמשמעותיים ביותר.

להלן דוגמאות לאופן שבו בינה מלאכותית יכולה לסייע לביקורת פנימית בהערכת סיכונים:

חילוץ מידע רשתי וכריית טקסט | כדי לאסוף ולנתח נתונים ממקורות מקוונים שונים, כגון אתרים, בלוגים, פורומים ופלטפורמות מדיה חברתית, ולזהות סיכונים ומגמות, כגון תלונות לקוחות, ביקורות שליליות ושינויים רגולטוריים.

עיבוד שפה ולמידת מכונה | כדי לנתח את הסנטימנט של הנתונים ("כרייה של דעות" או "בינה מלאכותית רגשית"), ולמדוד את המוניטין והאמינות של הארגון ומחזיקי העניין שלו, כגון לקוחות, ספקים ושותפים.

ניתוח אזהרות ורשתות עצביות מלאכותיות | כדי לדמות את התוצאות וההשפעות העתידיות של סיכונים ותרשימים שונים, ולספק הערכות הסתברותיות וכמותיות של חשיפת הסיכונים והתיאבון של הארגון.

הערכת סיכונים היא אחת המשימות הקריטיות והמאתגרות ביותר עבור מבקרים פנימיים, שכן היא מחייבת אותנו להתעדכן בסביבה המשתנה והלא ודאית ולצפות ולהגיב לצרכים ולציפיות המתפתחים של הארגון ומחזיקי העניין שלו. באמצעות AI מבקרים פנימיים יכולים לשפר את המודעות לסיכונים והמענה להם, ולספק הבטחה וייעוץ פרואקטיביים וצופי פני עתיד.

חילוץ מידע רשתי | Web Scraping

תהליך של שימוש בבוטים כדי לחלץ תוכן ונתונים מאתרי אינטרנט.

כריית טקסט | Text Mining

תהליך של חקירה וניתוח של כמויות גדולות של נתוני טקסט לא מובנים, בסיוע תוכנה שיכולה לזהות מושגים, דפוסים, נושאים, מילות מפתח ותכונות אחרות.

עיבוד שפה טבעית | NLP

Natural Language Processing

עוסקת בעיקר במתן יכולת למחשב לתמוך בשפה אנושית ולתפעל אותה. הדבר כרוך בעיבוד מערכי נתונים של שפה טבעית באמצעות גישות למידת מכונה מבוססות כללים או הסתברותיות. המטרה היא שמחשב יהיה מסוגל "להבין" תוכן של מסמכים, לרבות הניואנסים, ההקשרים של השפה בתוכם. לאחר מכן הטכנולוגיה יכולה לחלץ במדויק מידע ותובנות הכלולים במסמכים, וכן לסווג ולארגן את המסמכים עצמם.

ניתוח | Big Data

הוא תהליך של גילוי מגמות, דפוסים ומתאמים בכמויות גדולות של נתונים גולמיים כדי לסייע בקבלת החלטות מבוססות נתונים.

אוטומציה רובוטית של תהליכים | RPA

Robotic Process Automation

משתמשת בטכנולוגיות אוטומציה כדי לחקות משימות של עובדים אנושיים, כגון חילוץ נתונים, מילוי טפסים, העברת קבצים, וכדומה.

תכנון וביצוע ביקורת

AI יכולה לבצע אוטומציה ולייעל משימות ביקורת שונות, כגון איסוף נתונים, תיעוד, דגימה ודיווח, ולספק משוב למבקרים לאורך תהליך הביקורת. הדבר יכול להפחית עבודה ידנית וחוזרת על עצמה, להגביר את התפוקה והאיכות של עבודת הביקורת, ולפנות זמן למבקרים לבצע פעילויות אחרות כגון ייעוץ.

להלן דוגמאות לאופן שבו בינה מלאכותית יכולה לעזור לביקורת הפנימית בתכנון הביקורת וביצועה:

אוטומציה רובוטית של תהליכים | כדי לאסוף ולארגן נתונים ממקורות ומערכות שונות ולאחסן ולעדכן אותם בפורמט מרכזי וסטנדרטי.

שימוש בצ'אטבוטים ובעוזרים וירטואליים כדי ליצור אינטראקציה עם מבקרים ולספק להם מידע וסיוע, כגון מענה לשאלות, תזמון פגישות ושליחת תזכורות.

שימוש במערכות מבוססות כללים ובמערכות מומחים | כדי לספק למבקרים מתודולוגיות ביקורת ושיטות עבודה מומלצות, כגון תקני ביקורת, נהלים ותוכניות ביקורת, וכדי להעריך ולאמת את ראיות הביקורת והמסקנות.

שימוש בעיבוד שפה ולמידת מכונה | כדי להפיק דוחות ביקורת וסיכומים ולהתאים אותם למחזיקי עניין ולמטרות שונות, כגון ועדות ביקורת, הנהלה ורגולטורים.

תכנון הביקורת וביצועה הם מהמשימות החשובות והתובעניות ביותר עבור מבקרים פנימיים, שכן הם מחייבים לתכנן ולבצע את עבודת הביקורת בהתאם לתקני ויעדי הביקורת, וכן לתעד ולדווח על תוצאות הביקורת וחוות הדעת. על ידי שימוש בבינה מלאכותית, מבקרים פנימיים יכולים לשפר את היעילות והאפקטיביות של תהליך הביקורת ולספק תפוקות ותוצאות ביקורת רלוונטיות ומהימנות יותר.

מהם האתגרים וההזדמנויות של שימוש בבינה מלאכותית לביקורת פנימית?

בינה מלאכותית יכולה להציע יתרונות רבים לביקורת הפנימית, אך גם מציבה כמה אתגרים וסיכונים. לדוגמה:

איכות נתונים ואבטחה: בינה מלאכותית מסתמכת על הזמינות והאמינות של הנתונים. מבקרים פנימיים צריכים לוודא שהנתונים שהבינה המלאכותית משתמשת בהם אכן מדויקים, שלמים ועקביים, ושהם מוגנים מפני אובדן, גישה לא מורשית, או שינוי לא מורשה.

ממשל תאגידי ואתיקה של בינה מלאכותית: בינה מלאכותית כוללת אלגוריתמים ומודלים מורכבים שלא ניתנים להסבר בקלות. מבקרים פנימיים צריכים להבטיח שהבינה המלאכותית המשמשת את הביקורת הפנימית מותאמת ליעדי הארגון, לערכיו ולמדיניותו ושהיא הוגנת ושקופה.

מיומנויות וידע בבינה מלאכותית: בינה מלאכותית דורשת מיומנויות וידע חדשים ומיוחדים שאולי לא יהיו זמינים או נגישים. מבקרים פנימיים צריכים לפתח ולתחזק כישורים ומיומנויות בבינה מלאכותית או לשתף פעולה עם מומחים ושותפים חיצוניים כדי להשתמש בבינה מלאכותית ולפקח עליה ביעילות.

פרטיות וסודיות המידע: יש להעריך סיכוני פרטיות וסודיות המידע. חשוב לשים לב שקיימים יישומי בינה מלאכותית שאוספים את נתוני הקלט לצורכי שיפור היישום ושיתוף עם צדדים שלישיים.

למרות האתגרים הללו, הבינה המלאכותית גם מציגה הזדמנויות רבות לביקורת פנימית. לדוגמה:

שיפור הערך וההשפעה של הביקורת: בינה מלאכותית יכולה לעזור לביקורת הפנימית לספק תובנות והמלצות רלוונטיות וניתנות לפעולה, ולספק יותר ערך והשפעה לארגון ולמחזיקי העניין שלו.

חיזוק עצמאות ואובייקטיביות הביקורת: בינה מלאכותית יכולה לסייע לביקורת הפנימית להפחית את השפעת ההטיות והשיפוט האנושיים ולהגביר את העקביות והאמינות של תוצאות הביקורת וחוות הדעת.

מתן אפשרות לחדשנות וטרנספורמציה בביקורת: בינה מלאכותית יכולה לעזור לביקורת הפנימית למנף טכנולוגיות חדשות ומתפתחות, כגון מחשוב ענן, בלוקצ'יין ואינטרנט של הדברים, ולשנות את פונקציית הביקורת ואת תפקידה בארגון.

סיכום

בינה מלאכותית היא טכנולוגיה משמעותית שיכולה לשפר את הביקורת הפנימית במובנים רבים, ולצד זאת גם מציבה כמה אתגרים וסיכונים שיש לטפל בהם. מבקרים פנימיים צריכים לאמץ אותה ולפקח עליה כדי למקסם את יתרונותיה ולמזער את חסרונותיה. כך תוכל הביקורת הפנימית להפוך לזריזה, יעילה ואפקטיבית יותר, ולספק יותר ערך לארגון ולמחזיקי העניין שלו.

תפקידה של הביקורת הפנימית בתהליכי הפיתוח וההטמעה של כלי AI

הביקורת הפנימית נדרשת לכלול בתוכנית העבודה גם משימת ביקורת ייעודית לבחינת האופן שבו החברה נערכת להטמעתם של כלי AI. במסגרת זו, הביקורת צריכה לבחון האם כחלק מיישום אפקטיבי של תוכנית העבודה העסקית-תפעולית של החברה מתקיים תהליך מוסדר למיפוי הפעילויות שבהן קיים צורך להטמיע כלי AI, ואילו פעולות (ארגוניות, טכנולוגיות ואחרות) נוקטת החברה כדי לתת מענה לצרכים שמופּו.

אם מיושמים בחברה כלי AI, על הביקורת הפנימית (כחלק ממשימות הביקורת המבוצעות לגבי תהליכי עבודה מרכזיים) לבצע בדיקות לבחינת נאותות תהליכי הפיתוח וההטמעה של כלים אלו. הביקורת צריכה לבחון האם בוצעה הגדרה נכונה של השאלה העסקית שכלי ה-AI נועד לתת לה פתרון, האם במסגרת תהליך האפיון הראשוני בוצעה בדיקה נאותה לבחינת הכדאיות הכלכלית (ROI) של הטמעת הפיתוח, האם הפיתוח בוצע תוך שימוש בטכנולוגיה הרלוונטית, והאם הלכה למעשה הכלים שהוטמעו אכן משרתים באופן נאות את השאלה העסקית.

אם לא מיושמים בחברה כלי AI או שכלים מסוג זה מיושמים באופן לא מושכל או שיטתי, הביקורת יכולה להצביע על תחומי פעילות מסוימים שבהם יש מקום להטמיע כלי AI, ואף יכולה לפתח בעצמה, באמצעות כלי AI, מודלים רלוונטיים שיצביעו על הפוטנציאל הגלום בהטמעת כלים אלו בתחומי פעילות נבחרים. שימוש בכלי AI על ידי הביקורת הפנימית אף מאפשר לה לשפר את יכולותיה בביצוע משימות הביקורת הרגילות, ולבחון אם יש ליקויים ("אנומליות") בתהליכי העבודה גם במקומות שבהם קיים קושי לאתרם. אנומליה היא "אירוע שאינו תואם לדפוס הצפוי או ליתר התצפיות בבסיס הנתונים". כל חריגה מהוראת דין, מהוראות נוהל עבודה או מתוצאות חישוב נדרש, מהווה אנומליה, ולמעשה יכולה להופיע כליקוי במסגרת דוח ביקורת פנימית.

בכל משימת ביקורת אנו נדרשים להפעיל כלי ביקורת רלוונטי כדי להבין האם קיימות אנומליות בתהליך. הביקורת בודקת גם תהליכים שמבוצעות בהם פעולות רבות ובתדירות גבוהה (לרבות תהליכים הכוללים מאות אלפי פעולות בכל חודש), באופן שאינו מאפשר לביקורת להסתפק בבדיקה מדגמית אקראית לצורך מתן חוות דעת מושכלת בדבר נאותות התהליך הנבדק. במקרים מסוימים, הביקורת יכולה לבצע ניתוח נתונים של האוכלוסייה לצורך איתור חלקים שלגביהם קיים סיכוי גדול יותר לאיתור תקלות בתהליך, ובהמשך לכך תוכל הביקורת לבצע בדיקה מדגמית מוטה לאיתור אנומליות באוכלוסייה. במקרים כאלה, אם לא אותרו אנומליות או שהתקבלו הסברים מניחים את הדעת לגבי האנומליות שאותרו, הביקורת תוכל להתרשם שהתהליך הנבדק תקין. במקרים אחרים, לרבות במקרים של אי סדרים ומעילות והנאות, שבהם לא ניתן לאתר אנומליות תוך שימוש בכלי בדיקה שגרתיים, הביקורת תידרש להפעיל כלי AI ו-Machine Learning כדי לאתר ליקויים בתהליך.



כלי AI בשירות הביקורת הפנימית

הסביבה העסקית מתפתחת בקצב מואץ והופכת מורכבת יותר ויותר, ולפיכך מחייבת חברות להטמיע כלי AI לצורך שיפור הביצועים התפעוליים והעסקיים. הפעלת רובוטים והטמעת כלי חיזוי כבר אינן בגדר אירוע חריג, אלא חלק בלתי נפרד מהפעולות שבהן נוקטות חברות בתהליכי תפעול, שירות ומכירה.

בהמשך לכך, גם יחידות הביקורת הפנימית, המחויבות להישאר רלוונטיות ולהוות גורם משמעותי בשיפור התהליכים בארגון, מוכרחות לבצע את השינויים הנדרשים על מנת להתאים את עצמן למציאות המשתנה.

הביקורת הפנימית מתמודדת עם אתגרים רבים בסביבה המורכבת והדינמית של ימינו, כגון משאבים מוגבלים, ציפיות גבוהות של מחזיקי עניין וסיכונים מתהווים. זה המקום שבו בינה מלאכותית יכולה להציע יתרונות משמעותיים על ידי אוטומציה של פעילויות הביקורת הפנימית, שיפור איכות וערך הביקורת, ומתן הבטחה וניטור מתמשכים.

מאת:
דקל אלקלעי | רו"ח ו-Data Scientist, שותף
אנה רוזנברג | רו"ח ומפתחת תכנה, שותפה בכירה
UpSight, פירמה המתמחה בייעוץ אגב ביקורת

”
אנומליה היא "אירוע
שאינו תואם לדפוס
הצפוי או ליתר התצפיות
בבסיס הנתונים"
”

דוגמאות לשימוש בטכניקות שונות לאיתור
אנומליות במסגרת עבודת הביקורת הפנימית

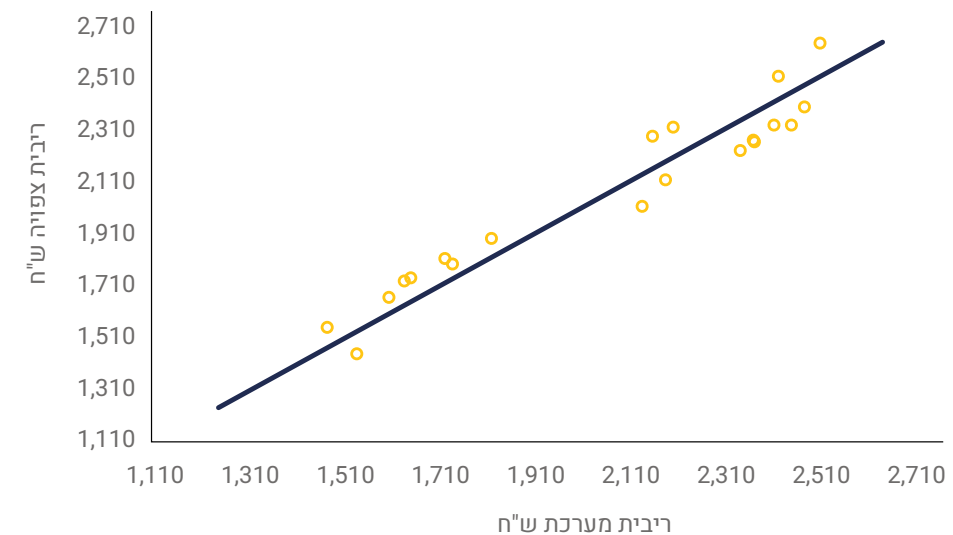


שיטות הבדיקה והדוגמאות המוצגות במאמר זה
באו לידי ביטוי במשימות ביקורת שבוצעו בפועל.

דוגמה 1 | בדיקת אנומליה מסוג Rule Based באמצעות כלי ביקורת AI

**בדיקה לאיתור חריגים בתהליך
הפקת דרישת תשלום בגין
הלוואות ללקוחות.**

אף שמדובר בדוגמה המתייחסת לסוג ביקורת שגרתית למדי, שכנראה מוכר לכל מי שעוסק
בביקורת פנימית, הרי שגם בדוגמה זו מבוצעת למעשה בדיקת אנומליה באמצעות כלי
ביקורת טכנולוגיים בסיסיים. במקרה של הפקת דרישת תשלום בגין הלוואה, מדובר
בחישוב המבוסס על חוקיות או פונקציה ידועה ומוגדרת מראש (Rule Based). אם יש
בידי הביקורת את המידע הגולמי בדבר סכום הלוואה, סוג הלוואה, מספר התשלומים
והריבית השנתית, הביקורת יכולה לבצע חישוב של תשלום הקרן והריבית של הלוואה
בכל נקודת זמן עבור כל אחת מההלוואות (בדיקת כל האוכלוסייה), ואת תוצאות החישוב
הבלתי תלוי של הביקורת, עבור כל אחת מההלוואות, ניתן להשוות לחישוב המערכת וכך
לאתר מקרים חריגים. אם אותרו מקרים חריגים, הביקורת תבצע בדיקה מדגמית מושכלת
כדי לבחון מול הגורמים הרלוונטיים בחברה (הגורמים העסקיים ו/או בעלי תפקיד ביחידה
הטכנולוגית) האם אכן מדובר בליקוי בתהליך החישוב או שקיים הסבר מניח את הדעת
לקיומם של החריגים.



*הנקודות הכחולות ("הקו הישר")
משקף את תוצאות החישוב התקין,
ואילו הנקודות שמחוץ לקו משקפות
את המקרים החריגים.

דוגמה 2 | בדיקת אנומליה מסוג Supervised Learning באמצעות כלי AI

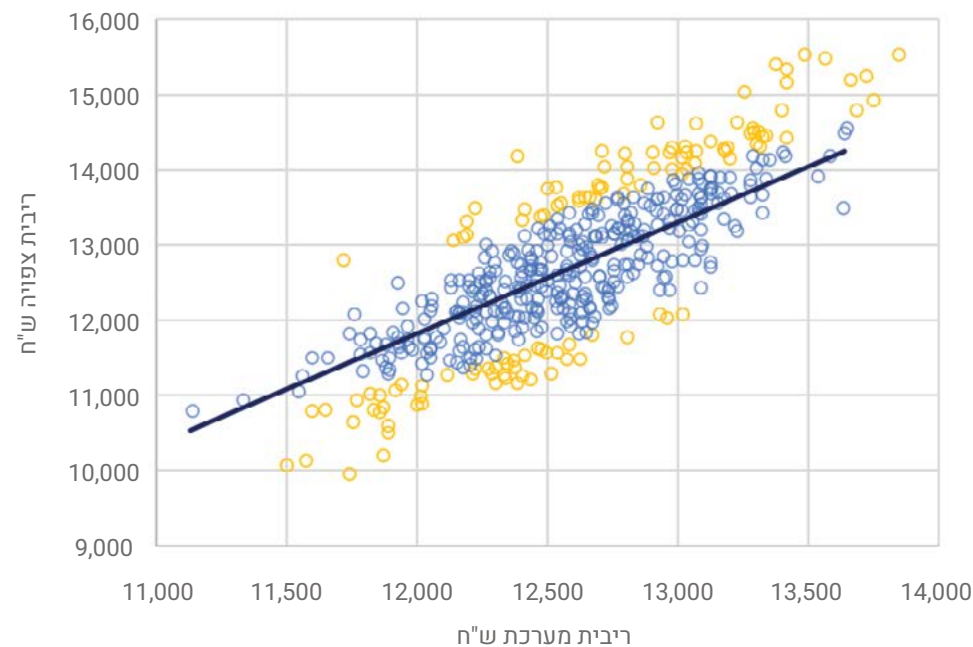
**בדיקה לאיתור חריגים בתהליך
החיתום בעת קבלת לקוח חדש**

יצוין כי טרם התקשרות בעסקה עם לקוח חדש, מבוצעת הערכת סיכון של הלקוח על פי מספר רב
של פרמטרים לצורך קביעה האם תבוצע התקשרות עם הלקוח (אישור העסקה או דחייתה), ואם
תבוצע עסקה – קביעת המחיר שישלם הלקוח (שיעור ריבית על הלוואה, או סכום פרמיה בגין
כיסוי ביטוחי, וכדומה). הערכת הסיכון מבוצעת על ידי החתם, תוך הפעלת שיקול דעת מקצועי
המבוסס על מידע ידוע בדבר מאפייני הלקוח ומאפייני פעילותו. לדוגמה: סוג העסק, גודל פיזי,
מחזור פעילות, מיקום, כמות עובדים וכו'.

ביקורת על תהליך מסוג זה היא משימה מורכבת מאוד, שכן בדרך כלל ניתן לחתם שיקול דעת
רחב לקביעת המחיר הסופי. כך שבפועל לא קיימת חוקיות או פונקציה ידועה ומוגדרת מראש
שלפיה מתקבלת החלטה על בסיס המידע הקיים לגבי לקוח ספציפי, ובמיוחד כאשר הפעילות
מבוצעת על ידי מספר רב של חתמים, שכל אחד מהם מפעיל שיקול דעת מקצועי עצמאי כדי
להשיג את המטרה המשותפת: התקשרות בעסקה שגלומה בה רווחיות לחברה. קושי מרכזי נוסף
העומד בפני הביקורת כרוך בכך שבדיקה לבחינת נאותות תהליך החיתום במקרים ספציפיים
מצריכה מומחיות מקצועית שפעמים רבות אינה מצויה בידי הביקורת.

לצורך איתור חריגים אפשריים בתהליך מורכב מסוג זה, הביקורת נדרשת להסתייע בכלי AI. בדוגמה
זו, הביקורת תפתח מודל בתהליך של למידת מכונה (Machine Learning) על בסיס הנתונים
הגולמיים שיש בידי החברה לגבי המאפיינים של הלקוחות ומאפייני פעילותם, לצד תוצאות
ההחלטות שקיבלו החתמים בעבר (Supervised Learning) בדבר שיעור הריבית או סכום הפרמיה
שנגבה מכל לקוח. את תוצאות המודל שפיתחה הביקורת לחיזוי החלטות החתמים עבור כל אחת
מההתקשרויות שבוצעו, ניתן להשוות להחלטות שהתקבלו בפועל על ידי החתמים, ובדרך זו לאתר
מקרים חריגים. לגבי מקרים שבהם קיימים פערים משמעותיים בין תוצאות המודל לבין ההחלטה
שהתקבלה בפועל, הביקורת תבצע בדיקה מול גורם מקצועי (כזה שלא קיבל את ההחלטה בפועל)
כדי להבין האם אכן מדובר במקרה חריג.

יצוין כי ממצאי ביקורת מסוג זה יכולים להצביע בפני הנהלת החברה וועדת הביקורת על פוטנציאל
השימוש של הגורמים העסקיים עצמם במודל סטטיסטי מתקדם לחיזוי קבלת ההחלטה של
חתם: למשל, איתור שוטף של מקרים שבהם הפרמיה שנקבעה על ידי החתם נמוכה משמעותית
מזו שנחזתה על ידי המודל (על בסיס מקרים בעלי מאפיינים דומים), זאת לצורך ביצוע בדיקות
משלימות של מנהל יחידת החיתום על תפקוד החתמים.



* הנקודות הכחולות ("הפיזור הקרוב
לקו הרגרסיה") משקף את תוצאות
החישוב הסביר, ואילו הנקודות
הכתומות הרחוקות מקו הרגרסיה
משקפות את המקרים החריגים.



IIA INTERNATIONAL
CONFERENCE
14-16 JULY 2025

TORONTO
save the date!

יצוין כי במקרים רבים קיים מספר גדול של מוצרים שמשווקים על ידי החברה, לכל מוצר מיוחס שיעור עמלת מכירה שונה, וייתכן אף שקיימת שונות בשיעור העמלה שניתן לאנשי מכירות שונים בגין מכירת מוצר מסוים (בשל שיקול דעת מקצועי שמופעל על ידי סמנכ"ל המכירות מול כל סוכן מכירות).

בנסיבות שבהן קיימת שונות רבה בשיעורי העמלה, ובמיוחד במקרים שבהם הקלדת הנתונים למערכת מבוצעת על ידי גורם יחיד וללא בדיקה של גורם נוסף בתהליך, קיים סיכון מוגבר להקלדה מוטעית של נתונים ואפילו סיכון לפעולה מכוונת של אי סדרים בתהליך.

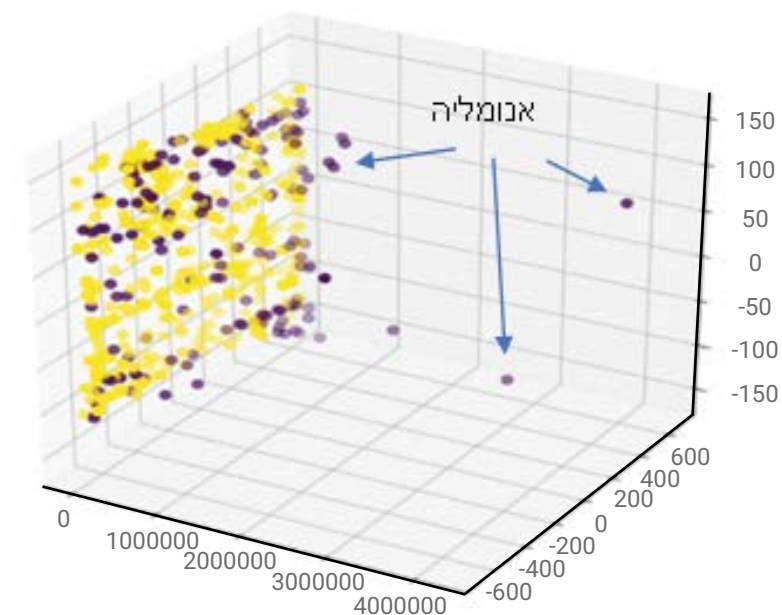
ביקורת על תהליך מסוג זה היא משימה מורכבת מאוד, מכיוון שלא רק שאין חוקיות או פונקציה ידועה ומוגדרת מראש שלפיה נקבע שיעור העמלה לאיש מכירות ספציפי, אלא גם לא קיימת תוצאה מסוימת שניתן להשוות אליה שיעור עמלה של סוכן אחד לעומת אחר.

לצורך איתור חריגים אפשריים בתהליך מורכב מסוג זה, אין דרך לבצע ביקורת ללא שימוש בכלי AI. בדוגמה זו, הביקורת תפתח מודל בתהליך של למידת מכונה (Machine Learning) על בסיס הנתונים שיש בידי החברה לגבי שיעורי העמלה השונים במוצרים השונים ואצל הסוכנים השונים, באופן עצמאי לא מונחה (Unsupervised Learning). באמצעות המודל שפותח ניתן יהיה לאתר הסכמים בעלי שיעורי עמלות חריגים אל מול שאר ההסכמים. לגבי המקרים שעל פי המודל נמצאו כחריגים ביותר, הביקורת תבצע בדיקה של שיעור העמלה המופיע במערכת מול שיעור העמלה המופיע בהסכם הפיזי, כדי להבין אם מדובר בהקלדה מוטעית. כמו כן, אם לא מדובר בטעות הקלדה, ניתן להציג את אותם הסכמים בפני סמנכ"ל המכירות כדי להבין אם שיעורי העמלה שנקבעו בהסכם אכן משקפים את תפיסתו ושיקול דעתו המקצועי. יצוין בהקשר זה כי ייתכן שסמנכ"ל המכירות כלל לא היה ער לכך שמדובר בהסכם התקשרות חריג. יכול להיות שלאורך השנים בוצעו מספר שינויים בהסכם ההתקשרות עם איש מכירות מסוים (כל פעם בוצע שינוי אחר ברכיב אחד המתייחס למוצר מסוים) באופן שכל שינוי בפני עצמו בנפרד אינו מהווה חריג אך בהסתכלות כוללת על כל השינויים מדובר בהסכם חריג.

בסוגי המקרים או התהליכים שבהם איתור אנומליות יכול להתבצע רק באמצעות פיתוח מודל לא מונחה של למידת מכונה, נדרשת גם בחינה ספציפית משלימה של מומחה בתחום הפעילות כדי שיאשר כי חריג שאותר על ידי המודל הוא אכן חריג בפועל, מכיוון שהמודל רק מצביע על קיומו של חריג ואינו מספק את ההסבר לכך. מודל מסוג זה רלוונטי במיוחד לאיתור מקרים של מעילות והונאות, מכיוון שמקרים כאלה משקפים חריגים באוכלוסייה שאין להם הסבר מניח את הדעת.

דוגמה 3 | בדיקת אנומליה
מסוג Unsupervised
Learning באמצעות כלי
AI

**בדיקה לאיתור חריגים בהקלדה
למערכת של מידע בדבר שיעורי
עמלות הכלולים בהסכמי התקשרות
עם סוכני מכירות (אנשי מכירות
עצמאיים כדוגמת סוכני ביטוח).**



מביטים אל העתיד: על בינה (מלאכותית), GPT וביקורת

מאת:

ד"ר נועם קוריאט | CISA, מנהל מחלקת ביקורת מערכות מידע בחטיבת הביקורת הפנימית בבנק דיסקונט.

לקראת סוף שנת 2022 הושק (GPT ChatGPT) של חברת OpenAI, שהביא למימוש הציפיות מהמהפכה התעשייתית החמישית – מהפכת הבינה המלאכותית.

בהמשך הוצגו מוצרים מתחרים דוגמת Bard של Google, Bing Chat (CoPilot) של Microsoft, וכן אלפי מודלים נוספים ייעודיים לתחומים ולנושאים ספציפיים, כגון משפטים, מחקר ומוזיקה, וכן מודלים יוצרים בתחומי התמונה, הווידאו, הצליל ועוד. באופן חסר תקדים הונגשה להמונים היכולת לנהל שיח טבעי בשפה אנושית עם המחשב לשם הפקת תוצרים איכותיים ומשמעותיים.

המהפכה התעשייתית החמישית, שאת מלוא היקף השפעתה טרם ניתן לאמוד, מצטרפת כתוספת משמעותית למהפכה התעשייתית הרביעית, מהפכת הטרנספורמציה הדיגיטלית, ומעצימה את קצב השינויים המהיר ואת קצב יצירת המוצרים, השירותים והצעות הערך שלא היו קיימים קודם. המציאות החדשה מאלצת את כלל הגורמים בארגון לבצע התאמות שיאפשרו להם להישאר רלוונטיים, ובהם גם הביקורת הפנימית¹.

במאמר הנוכחי נסקור את המושג בינה מלאכותית יוצרת (Generative Artificial Intelligence GenAI), תוך חשיפת ההזדמנויות והאתגרים הרלוונטיים עבור הביקורת הפנימית.



מה זה בינה מלאכותית יוצרת (Generative Artificial Intelligence)?

בינה (Intelligence) היא היכולת לחשוב באופן מופשט, להבין ולנתח מידע שאינו מובנה ורעיונות מורכבים, וללמוד מתוך ניסיון. כאשר יכולות אלה מבוצעות על ידי מחשב או רובוט לשם ביצוע משימה או חלק ממשימה, הדבר נקרא בינה מלאכותית (Artificial Intelligence)?

בדרך כלל, מודלים של בינה מלאכותית משתמשים במידע קיים שעליו הם מאומנים באופן מפורק (Supervised) או לא מפורק (Unsupervised), ויודעים לבצע משימות של חשיבה אינטליגנטית שתוצאותיהן הן במסגרת המידע הקיים, בלי ליצור מידע חדש.

בינה מלאכותית יוצרת (Generative AI) היא למעשה מודלים המאפשרים ליצור מידע חדש על בסיס המידע שעליו אומנו המכונות. המידע החדש יכול להתבטא בטקסט, בתמונות, בצלילים, בווידיאו ועוד. לדוגמה, ChatGPT שכותב שיר או Dall-e שמייצר תמונה.



ככל שה-prompt מדויק יותר, וככל שמרחב ה-data שזמין למודל איכותי יותר, כך המודל יכול לספק תשובה מדויקת יותר

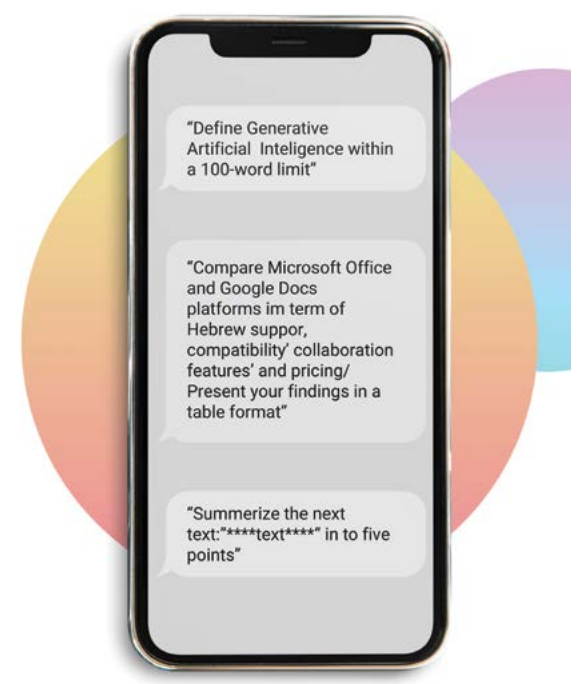


איך זה עובד?

מודלים של GenAI מאומנים על data מסוגים שונים: מובנה (structured) כגון טבלאות, ולא מובנה (unstructured) כגון מסמכים, מצגות, תמלולי אודיו/וידאו וכדומה.

המשתמש פונה אל המודל באמצעות prompt – טקסט של משפט אחד או יותר המבטא את בקשתו.

תרשים 1 | דוגמאות ל-prompt



לדוגמה, במודל מסוג text-to-text generator כגון ChatGPT, מתבצע תהליך סטטיסטי על בסיס ה-data שעליו אומן המודל לבחירת מילים ביחס ל-prompt. התשובה מיוצרת מילה אחר מילה.

זהו איננו תהליך של "הבנה" על ידי המודל, אלא של יצירת תוכן חדש המיוצר בתהליך סטטיסטי. במודל מסוג text-to-image generator יתבצע תהליך דומה המייצר פיקסלים במקום מילים.

ככל שה-prompt מדויק יותר, וככל שמרחב ה-data שזמין למודל איכותי יותר, כך המודל יכול לייצר באופן טוב יותר את המילה הבאה בתשובה, ולספק תשובה מדויקת, תקפה ומהימנה שקרובה יותר לציפייה של המשתמש.

בסיום התהליך יכול המשתמש לספק היזון חוזר למודל – האם התשובה שקיבל רלוונטית או לא, ובכך לאפשר למודל לכייל את המודל הסטטיסטי הפועל מאחורי הקלעים.

¹Koriat, N. (2023). Internal audit as a Driver for Innovation. ISACA Journal, 4 (The Evolution of The Global Information Environment), 21-25.
²Kok, J. N., Boers, E. J., Kosters, W. A., Van der Putten, P., & Poel, M. (2009). Artificial intelligence: definition, trends, techniques, and cases. Artificial intelligence, 1, 270-299.

Inexplicability

המודל אינו "מבין" את ה-prompt. התוצר (תשובת המודל) הוא פועל יוצא של תהליך סטטיסטי. לכן המודלים בדרך כלל אינם יודעים להסביר כיצד הגיעו לתשובה, או להציג באופן מדויק את מקורות המידע שעליהם התשובה שנוצרה מתבססת. מצב זה מקשה על היכולת של המשתמש לוודא כי התשובה תקפה ומהימנה.

Hallucination

אם מרחב ה-data שעליו מאומן המודל אינו רחב ואיכותי מספיק, ומהצד השני ה-prompt אינו מצמצם את מרחב הניתוח הרלוונטי באופן מספק, התהליך הסטטיסטי עשוי להתקל בקושי לאתר תוצאות רלוונטיות לשם ייצור תשובה.

במודל טקסט לדוגמה, הדבר יכול להתבטא בבחירת מילים ליצירת תשובה שאינן תואמות את בקשת המשתמש, והמודל אף עשוי "להמציא" תוכן חדש.

מאפיין זה בשילוב עם Inexplicability, מגביר את הסיכוי לתשובות שאינן תקפות ומהימנות תוך הגדלת הקושי לבצע ולידציה. הדבר יכול לגרום להתממשות סיכונים כמו Overreliance, תוך שימוש במידע מטעה ולא מבוסס שעשוי להוביל להחלטות שגויות ולביצוע פעולות שאינן תקינות.

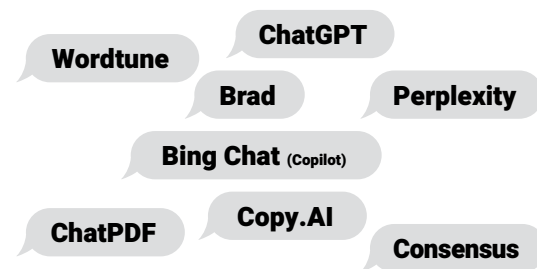
הטיות, אתיקה ומוסר

ככל שמרחב ה-data כולל יותר תוכן שמוטה באופן מסוים, לדוגמה בהיבטים של מגדר, דת, גזע וכדומה, כך קיים סיכוי גבוה יותר שהתשובות שיתקבלו יהיו מוטות, תוך סיכון מוגבר לתשובות שאינן אתיות או מוסריות.

שילוב של בינה מלאכותית מבוססת מחשב, דוגמת GenAI, עם היכולות האנושיות, מאפשר לייצר בינה משופרת או מורחבת – Augmented Intelligence^{3,4}, ובכך להעצים את המיומנויות והכישורים האנושיים. לדוגמה, באמצעות האפשרות להשתמש ב-GenAI text-to-text generator למשימות שונות. למשל:

- למידה, סיכום וניתוח תוכן. לדוגמה, סיכום מסמך ב-250 מילים או זיקוק חמש התובנות העיקריות ממסמך כלשהו.
- השוואה בין סטנדרטים, מוצרים, ארגונים, מסמכים וכדומה. לדוגמה, השוואה בין מוצר למתחרים על בסיסי קריטריונים שהוגדרו מראש, או האם נוהל בארגון נותן מענה להנחיה רגולטורית.
- איתור נושא ספציפי בתוכן רחב היקף. לדוגמה, איתור הנחיה ספציפית הנוגעת לנושא מסוים בהוראה רגולטורית או חוק.
- חשיבה מתבדרת וסיעור מוחות. לדוגמה, כתיבת מפרט ביקורת בנושא מסוים.
- תרגום ועריכה לשונית. לדוגמה, תרגום מעברית לאנגלית, ניסוח מחדש של משפטים, קיצור טקסט, מילים/נוסח חלופיים וכדומה.

תרשים 2 | דוגמאות ל-Text-to-Text Generators



במסגרת זאת יש פוטנציאל להתייעלות הביקורת, תוך קיצור זמנים וגישה למרחבי תוכן גדולים משמעותית מאלו שהביקורת יכולה לגשת אליהם באופן ידני אנושי במסגרת לוחות זמנים מוגבלים.

את היכולות ניתן לממש בכלי "מדף", כגון אלה המופיעים בתרשים 2, וכן באמצעות מימוש פלטפורמת GenAI ארגונית "פרטית" המבוססת על גבי פלטפורמות דוגמת Azure OpenAI Service או Google Vertex AI. מימוש עצמאי מאפשר, בין השאר, העלאת תכנים שאינם ציבוריים, בקרה על גישה לתכנים רגישים ומוגנים, ושליטה טובה יותר ב-data שעליו מאומן המודל, תוך צמצום סיכונים הנובעים מ-Hallucination, הטיות, מוסר ואתיקה.

³Sadiku, M. N., Musa, S. M., Sadiku, M. N., & Musa, S. M. (2021). Augmented intelligence. A Primer on Multiple Intelligences, 191-199.
⁴Noy, S., & Zhang, W. (2023). Experimental Evidence on the Productivity Effects of Generative Artificial Intelligence.

בנוסף, השימוש ב-GenAI עשוי לשנות את סביבת הסיכון שהביקורת הפנימית נדרשת להתייחס אליה בתהליך ניהול הסיכונים ואת אופן בחינת הבקורות בארגון. לדוגמה:

מתחרים | קצב השינויים הגבוה ואימוץ טכנולוגיות (ובפרט GenAI) ובעקבותיהן טרנספורמציה דיגיטלית בארגונים, כל אלה עשויים לשנות באופן משמעותי את המוצרים, השירותים והצעת הערך של ארגונים מתחרים, ואף להכניס לסביבת התחרות ארגונים או מוצרים חדשים. האם נערך מיפוי וקיימת תוכנית תגובה לתהליכים עסקיים, מוצרים ושירותים שצפויים להשתנות בעקבות אימוץ GenAI?

לקוחות | ובפרט Digital Natives (דורות Y, Z, ובהמשך Alpha), שהם בעלי העדפה לשימוש בטכנולוגיות חדשות, צפויים לדרוש כי השירותים והצעת הערך של הארגון יותאמו ליכולות המקובלות בשוק. לדוגמה, שיח טבעי מותאם אישית עם האפליקציה במקום תפריטים אחידים. האם הארגון רגיש (Hyper-Awareness) מספיק לשינויים בדרישות הלקוחות? האם התשתית הטכנולוגית מספקת יכולת תגובה וביצוע מהירות⁵ (Fast Execution)?

מהצד השני, לקוחות צפויים להשתמש בטכנולוגיה החדשה על מנת לשפר את מצבם. האם נערכת חשיבה צופה פני עתיד באשר להצעת הערך במוצרים בהתאם למצב החדש?

ספקים | בדומה ללקוחות, צפויים להשתמש ב-GenAI. לדוגמה, זיהוי נקודות חולשה במסמכי התקשרות. האם הארגון עושה שימוש בתהליכים מקבילים על מנת לאתר נקודות חולשה במסמכי ההתקשרות ובבדיקת הצעות המחיר של הספקים?

עובדים | כיום ארגונים שמים את העובד במרכז ופועלים ליצירת "חוויות עובד" איכותיות. לכן השימוש ב-GenAI מגביר את החשיפה לסיכונים דומים לאלו שפורטו לגבי לקוחות וספקים. לדוגמה, סיכונים הנובעים מדרישת העובדים לשירותים המממשים את היכולות החדשות או לתהליכי העסקה (חוזה העסקה, תגמול, הערכה וכו').

האם הארגון נערך לשימוש בכלי GenAI כפלטפורמה לשירותים ומתן מענה לדרישות עדכניות מצד העובדים? האם הארגון נערך לניתוח, ניטור ויצירת מענה מותאם אישית לעובדים בהתאמה למאפייניהם המיוחדים? האם מתבצעת הערכות לשימוש בטכנולוגיה למימוש פרקטיקות של משאבי אנוש, דוגמת בחינת חוזי העסקה?

איומים פנימיים וחיצוניים | ניתן להשתמש ב-GenAI על מנת לאתר חולשות, לכתוב קוד המנצל את החולשות, ולהבנות תהליכים להנדסה חברתית, לרבות כתיבה ודיבור בשפת האם של הלקוח. כל אלה מגדילים את יכולת התוקפים לנצל את משטחי התקיפה באופן יעיל (מהירות ומשאבים) ואפקטיבי יותר מבעבר.

בנוסף, תוכן ארגוני רגיש עסקית או פרטים אישיים עשויים להיות מוזנים במסגרת prompt לכלי מדף ציבורי, ולהישמר במאגר המידע שעליו המודל מאומן, תוך סיכון לחשיפת המידע באופן שאינו מבוקר.

האם מערכי הגנת הסייבר והגנת הפרטיות בארגון מעדכנים את מפת הסיכונים בהתאם למצב החדש ונערכים בהתאם? האם נעשה שימוש בכלים מבוססי GenAI על מנת להגדיל את אפקטיביות הפעילות, לדוגמה בהיבטי ניטור?

סיכום

המהפכה התעשייתית החמישית, ובפרט טכנולוגיית ה-GenAI, מספקות הזדמנות טכנולוגיות ייחודיות המאפשרות לארגונים שכבה נוספת של טרנספורמציה דיגיטלית, מעבר לטכנולוגיות המהפכה התעשייתית הרביעית (SMAC – Social, Mobile, Analytics, Cloud).

ניצול ההזדמנות מזמן פוטנציאל למינוף ההון האנושי מצד אחד, וליצירת מוצרים, שירותים והצעות ערך חדשים המשנים את הסביבה התחרותית מהצד השני.

איכות ה-GenAI היא כאיכות ה-data. מידע חסר, שגוי או מוטה יכולים להשפיע על תוצרי המודל והאפשרות להשתמש בו בצורה אפקטיבית. היערכות ארגונית בהיבטי ניהול הנתונים, המידע והידע הארגוניים הם קריטיים לניצול אפקטיבי של הטכנולוגיה.

בכובע אחד, הביקורת הפנימית נדרשת לחתור לניצול ההזדמנות למינוף ההון האנושי תוך התייחסות לסיכונים הגלומים. בכובע השני, הביקורת נדרשת לחתור להבנה מעמיקה של השינוי והשלכותיו על הארגון בכלל ההיבטים, לרבות מתחרים, לקוחות, ספקים, עובדים ואיומים פנימיים וחיצוניים, תוך יישומה בתהליך ניהול הסיכונים ובחינת הבקורות בביקורות המתבצעות בארגון.

⁵ Wade, M., A. Tarling (2016). The Digital Business Agility Imperative: How Companies Can Fight Digital Disruption, International Institute for Management Development, Switzerland

⁶OWASP (2023). OWASP Top 10 for LLM Applications, https://llmtop10.com

האם הטייטל שלנו מגדיר אותנו?

מאת:

חן הרייתי | רו"ח, MA-BE, CISA, CISO, CDPSE, CSA, מבקר פנימי ראשי בחברת מרכז סליקה בנקאי (מסב)

יובל דיין | MA-BE, מנהלת שיווק ותפעול בחברת Quantum Hub

האם הטייטל "מבקר" או "מבקר" משפיע על תפיסת העולם של גורמים אחרים בארגון, ואפילו על תפיסת העולם שלנו, לגבי מהות התפקיד שלנו או מקומנו בארגון? התשובה הקצרה היא כן! מחקרים מראים שלטייטלים יש השפעה מהותית על עיצוב התפיסה העצמית של עובדים (ובכך על המציאות), וגם על היכולת של ארגונים להשתמש בהם ככלים להעצמת עובדים. למונח הלוועזי Job Title אין מקבילה מדויקת בעברית, אך נדמה שגם בתרבות הישראלית יש ל"טייטל" מקום משמעותי למדי. הנושא הזה רלוונטי כמעט לכל התחומים, אך כפי שתראו יש לו השפעה קריטית על הביקורת הפנימית.



הקשר בין שפה למציאות

פסיכולוגיוויסטיקה היא תחום מחקר העוסק בחקר התהליכים הפסיכולוגיים המעורבים ברכישה, שימוש ועיבוד השפה. תחום זה מתמקד בקשר שבין השפה והמוח האנושי, ובמחקרים מסוימים גם בהשפעת השפה על תפיסת המציאות של אנשים. אחת ההשערות המובילות בתחום היא השערת ספיר-וורף, הגורסת כי המבנה הסמנטי של שפה משפיע על תפיסת העולם של הדוברים, ולמעשה אפילו מעצב אותה.

איך שפה מתקשרת לטייטל שלנו?

בהקשר הארגוני, פסיכולוגיוויסטיקה-ארגונית מנתחת תהליכי תקשורת ארגוניים כדי לשפר את מצבם הנפשי של העובדים ואת רווחתם ולערבם בפעילות הארגונית. לכל ארגון יש שפה משלו, שיכולה לספר לנו על התרבות הארגונית ועל ערכי ארגון דרך עבודתו וכיצד הארגון מציג את עצמו. אחד המאפיינים העיקריים של השפה הארגונית הם טייטלים ("Job Titles").

למה אנחנו צריכים טייטלים?

בשנים האחרונות הטייטל שלנו הפך להיות חשוב ביותר. לעיתים קרובות זה המידע הראשוני שאנו חולקים על עצמנו עם עמיתים חדשים, לקוחות ואחרים. יתרה מכך, בארגונים מודרניים טייטלים הם אבן יסוד ומשמשים כ"תג זהות", כלומר הם דרך מהירה לתאר את הידע, המיומנויות, היכולות ומאפיינים נוספים שיש לעובדים, ואת האחריות של העובד או העובדת בארגון.

טייטלים כאינדיקטור לכישורים ולידע של עובדים

מחקרים מראים כי טייטלים שונים לאותו תפקיד עשויים להשפיע על האופן שבו אחרים מעריכים את הכישורים והידע של עמיתיהם, ואפילו על האופן שבו העובדים תופסים את עצמם. לדוגמה, כאשר אתם פוגשים אדם חדש שנכנס לארגון, לרוב השאלה הראשונה תהיה "לאיזה תפקיד?". לתשובה לשאלה זו יש השפעה על תפיסת היכולת או הידע של אותו עובד או עובדת בעיניכם. התשובה גם לא תהיה זהה במקרה שהוא נכנס לתפקיד של סמנכ"ל פיתוח, סמנכ"ל כספים או סמנכ"ל שיווק. בנוסף, ברור לכולם כי קיים הבדל בין סמנכ"לית כספים לחשבת לדוגמה, אומנם שני התפקידים עוסקים באותו התחום אבל הטייטל עצמו מצביע על הבדל בניסיון ובסמכות. יתרה מזאת, הטייטל שלנו לא נשאר רק בארגון, הוא יכול להוות מקור גאווה וזהות עבורנו גם ברמה האישית. בעולם שמחוץ לעבודה, כשאנחנו פוגשים אנשים חדשים אנחנו שואלים אותם במה הם עוסקים כדי להכיר אותם טוב יותר. גם פה המוח שלנו משתמש בתארים האלה כקיצור דרך להבנת הידע, היכולות, המעמד והערכים שלהם. בדרך כלל אנו גם מצפים שאחרים ישאלו אותנו על התפקיד שלנו כדי להציג את עצמנו בפניהם.

ארגונים רבים משתמשים בטייטלים לצורך העצמת עובדים, שיפור המוטיבציה והתפיסה העצמית. לדוגמה, אנו רואים הרבה טייטלים חדשים עבור תפקידים שקיימים בארגון עשרות שנים, או הוספת טייטל שכולל את המילה "מנהל/ת" לתפקיד שבו לא מנהלים אף אחד. ההתייחסות לעובד כמנהל מאפשרת לתת לו תחושת אחריות גדולה יותר, משפרת את המיתוג העצמי ומעלה את המוטיבציה.

לטייטלים עצמם יש גם השפעה על תפיסת המקצועיות של הגורם שעומד לפנינו. מחקר שבוצע בארה"ב בחן את האופן שבו טייטל של סוכני AI (צ'אטבוטים) יכול להשפיע על תפיסת הלקוחות את מקצועיות הסוכנים הללו, להשפיע על שביעות רצון הלקוחות ועל היחס למוטג, ולתרום להחלטה האם להסתמך בפועל על המלצת AI. המחקר הראה כי הצרכנים תופסים את "מנהל הבינה המלאכותית" (AI Manager) באופן חיובי מובהק יותר מאשר "נציג הבינה המלאכותית" (AI Representative), והרושם החיובי נשמר גם בין "מנהלי הבינה המלאכותית" לבין "נציגים אנושיים". המחקר הראה את היכולת לשפר באופן מלאכותי את האמון שניתן לסוכני AI על ידי שינוי הטייטל שלהם בלבד, גם כאשר שאר הפרמטרים זהים.



אז איך זה קשור אלינו?

עכשיו, כשיש לנו את הכלים להבין את ההשפעה של הטייטל על תפיסת העולם שלנו ושל גורמים אחרים בארגון, בואו ננתח את ההשפעה על המקצוע שלנו – "ביקורת פנימית". בשפה היומיומית למילה "ביקורת" יש קונוטציה שלילית, ולעיתים מתייחסים למונח "ביקורת" כמילה נרדפת ל"ביקורת שלילית".

עוד נקודה מעניינת לחשוב עליה היא ההבדל בין תפיסת הטייטל בעברית ובאנגלית. אם ננתח את הטייטל "מבקר פנימי", התרגום האינטואיטיבי של המילה "מבקר" ייטה לכיוון של Criticism השלילי יותר ולא דווקא ל-Auditing. **האם המשמעות היא שאנחנו למעשה מסתובבים בארגון עם שם שמצביע יותר על "Internal Critic" מאשר על "Internal Auditor"?**

מחקר מעניין שבוצע בישראל טוען כי תיאור סיטואציה על ידי שימוש ב"פועל" יוצר תגובה עזה יותר (חיובית או שלילית) לעומת השימוש ב"שם פעולה". לדוגמה, המילה "הפסיד" מעוררת רגשות עזים יותר מאשר המילה "הפסד". מחקר זה יכול להצביע על הקשר בין השימוש בטייטל "מבקר" או "מבקרית" לבין טייטל שנושא בתוכו את המילה "ביקורת", כמו "מנהל ביקורת" למשל.

אז מה בעצם הבעיה?

ראינו את הקשר בין השפה והיכולת שלה להשפיע על תפיסת המציאות של אנשים, ואת הקשר בין הטייטל שלנו לתפיסת המציאות ומקומנו בארגון. כאשר הטייטל אינו משקף את ציפיות העובדים או אינו תואם את התפקיד בפועל, הדבר עלול להשפיע לרעה על תפיסתם העצמית של העובדים או על האופן שבו הסביבה מעריכה אותם ולהשפיע על המוטיבציה והביצועים שלהם!

אז מה הפתרון?

מחקרים מראים את הפוטנציאל לשימוש בטייטל ככלי להעצמת עובדים, שכן קיים קשר הדוק בין הטייטל לבין הזהות שלנו. טייטל חיובי ומעצים יכול לסייע למניע האנושי הבסיסי לתקשר את זהותנו וערכנו לאחרים. כך לדוגמה, מחקר שבוצע בארה"ב הראה כי בארגון שבו העובדים בחרו לעצמם "FUN טייטלים", הטייטל עצמו סייע להפחית תשישות רגשית ולהעצים עובדים, ואפשר להם למלא תפקיד פרואקטיבי יותר. עוד הראה המחקר כי עובדים הרגישו מאושרים ובטוחים פסיכולוגית כאשר הם ביטאו את זהותם, וכל זאת באמצעות שינוי הטייטל בלבד!

אז מה אפשר לעשות בנוגע לביקורת?

ההמלצה הראשונה שלנו היא לחשוב על הטייטל עצמו! האם ביקורת פנימית היא התואר הנכון לנו בשנת 2024? הרי אנחנו מדברים על מיצוב הביקורת כגורם המסייע לארגון לעמוד ביעדיו, הפיכה לגורם מוביל ומשפיע בארגון וכו'. האם הטייטל "מבקרית" או "מבקר" משקף זאת? לדעתנו, ייתכן מאוד שלא..!

אבל עד שנצליח למתג מחדש את שם המקצוע, קיימות פרקטיקות פשוטות יותר ליישום שיכולות להפחית או למנוע את ההשפעות של ההטיות המצוינות מעלה. לצורך כך, אנו נבחן את אפקטיביות השימוש בכלים מתחום הכלכלה התנהגותית הנוגעים לעולמות ה-Debiasing. המונח Debiasing מתייחס למגוון רחב של טכניקות, שיטות והתערבויות שנועדו לצמצם או לבטל הטיות בתהליך קבלת ההחלטות. בהקשר הזה יש לנו שתי המלצות: הראשונה תשפיע באופן ישיר על עובדי הארגון ועלינו, והשנייה תשפיע על סביבת העבודה ובאופן עקיף על עובדי הארגון ועלינו.

ההמלצה הראשונה שלנו היא לחשוב על הטייטל עצמו! האם ביקורת פנימית היא התואר הנכון לנו בשנת 2024?

FORUM AI

חברות וחברים יקרים,

אנו מזמינים אתכם להשתתף ולקחת חלק
פעיל בפורום חדש של הלשכה, פורום ה-AI.

כל המעוניין/ת להצטרף ולקחת חלק פעיל
בפורום, מוזמן/ת לפנות ליו"ר הכורום

חן הרייתי

CHEN.HARYATI@GMAIL.COM

מטרות הפורום,

לשמש כמסגרת ארגונית מקצועית
לחדשנות בביקורת, בעולמות ה-AI עבור
מבקרים פנימיים

לפעול להגברת מודעות חברי לשכת
המבקרים הפנימיים לעולם ה-AI ובדגש
על פיתוח יכולות לשימוש בכלי AI
במסגרת תהליכי הביקורת הפנימית.

לפעול לשיפור הידע וההכשרה של
מבקרים פנימיים, באמצעות הכלים
הבאים

פרסום מעט לעת של מאמרים
ופרסומים מקצועיים הנוגעים
לעולמות ה-AI ושלובם בעולמות
הביקורת הפנימית

יצירת מאגר ידע ומחקר בתחום ה-AI-
לשימוש חברי הפורום

קיום הכשרות מקצועיות באמצעות
ערבי עיון, הכשרות וסדנאות

הקמת קבוצת ווטסאפ, אשר תסייע
לחברי הפורום לחלוק בידע ובניסיון
בשימוש בכלי AI בתחום הביקורת
הפנימית

סיכום ומסקנות

מתוך הבנה כי תפקיד הביקורת הפנימית הופך למשמעותי יותר והרצון שלנו הוא להביא ערך ולקדם תהליכים בארגון, חשוב שנשים לב לאתגר שמציב בפנינו הטייטל שלנו. "מבקר" או "מבקר" עדיין נתפסים אינטואיטיבית כשליילים, וחשוב שנבין את הסיכון הכרוך בכך הן בתפיסה העצמית שלנו והן בתפיסת גורמים אחרים בארגון אותו. אנו מאמינים כי באמצעות יישום כלים מעולמות הפסיכולוגיה והכלכלה ההתנהגותית שהצענו, אפשר למתן את ההשפעה האינטואיטיבית של הטייטלים שלנו ולהעצים את ההון האנושי בביקורת הפנימית ואת תפיסת הארגון אותו, מה שיוביל בשלב הבא לביקורת אפקטיבית יותר המסוגלת להביא ערך אמיתי לארגון. תזכרו! טייטל יוצר מציאות! **ו-ביקורת | בונה | הצלחה!**

תודתנו לד"ר אורלי אידן על ההשראה לכתיבת המאמר, כחלק מקורס "פסיכולוגיה וביקורת: שפה חלון לנפשנו", במסגרת התוכנית לתואר שני בכלכלה התנהגותית באוניברסיטת רייכמן

1 לימוד (Education)

אחת הטכניקות החזקות ביותר להפחתת עוגנים והטיות היא לימוד הנושא (טכניקה זו פועלת באופן ישיר על מושא ההטיה). בהקשר הזה ניתן לקיים שיח פתוח בתוך צוות הביקורת ומול מנהלים בארגון לגבי מטרות העל של הביקורת הפנימית, תפקידה בארגון, דוגמאות לתרומה שהביאו ביקורות קודמות לארגון וכדומה.

טיפ אישי שאני משתמש בו כמבקר ראשי הוא לשוחח על הנושא בגובה העיניים ואפילו להעלות את נושא הטייטלים לדיון. לדוגמה, במסגרת תפקידי אני משתתף באופן קבוע בימי אוריינטציה בארגון ובמפגשי היכרות עם מחלקות שונות, ולא פעם אני מעלה את השאלה: "איך אתם תופסים את הטייטל של מבקר פנימי?" או "מה לדעתכם התפקיד שלי כמבקר הארגון?" ספויילר: זה כמעט אף פעם לא תשובה שנעיס לשמוע... עם זאת, בדרך כלל אחרי שיח כזה התפיסה בנוגע למבקר או לביקורת משתנה לגמרי. כתוצאה מהדיונים האלו נשאלתי לא פעם: "אם הטייטל לא משקף את העבודה שאתם עושים, למה אתם לא משנים אותו?".

2 תזכורות (Reminder)

הטכניקה החזקה ביותר להפחתת עוגנים והטיות היא תזכורות שוטפות (טכניקה זו פועלת על סביבת מושא ההטיה). באמצעות תזכורות שוטפות אפשר לחזק באופן שיטתי את תפיסת המבקרות והמבקרים בצוות בנוגע לעצמם ("גאוות יחידה"). מול מנהלים אחרים בארגון, לדוגמה בישיבת פתיחת הביקורת או לפני דיונים על דוחות הביקורת, אפשר לציין באופן תמציתי את מטרות העל של הביקורת ולהתייחס לנושאי השוטפות, הדיאלוג והשיח. דוגמה מצוינת לשימוש נכון בכלי התזכורות אני יכול להביא מהתקופה שבה עבדתי בצוות הביקורת באל-על. בכל מסמך של הביקורת (פנימי או חיצוני, כגון דוח הביקורת, מכתב פתיחה וכדומה) היינו כותבים את המשפט הבא בתחתית העמוד "**ביקורת | בונה | הצלחה**" והמשפט הזה היה כתוב בצבע כחול בולט ובפונט מודגש. לתזכורת הזו יש אפקט חזק כי מעבר לעובדה שהיא ניכרת לעין, היא גם משלבת בתוכה משחק מילים שמסקרן את הקוראים וגורם להם להתעמק במשפט. למעשה אני משתמש במשפט הזה עד היום ואין פעם שאני לא מקבל עליו פידבק חיובי. שילוב משפט כזה באופן שוטף משמש כתזכורת שוטפות ל"אני מאמין" ולמטרת העל של הביקורת הפנימית, ומסייע הן בשיפור התפיסה העצמית שלנו כמבקרים פנימיים והן במיצוב מול גורמים אחרים בארגון.

איום הולך וגובר

מאת:

ניל הודג' | עיתונאי עצמאי מנוטינגהאם, אנגליה

מאמר מתורגם מגיליון אוגוסט 2023,
כתב העת Internal Auditor

ככל שארגונים משתמשים יותר ב-AI, כך הם חושפים את עצמם לסיכונים סייבר ופרטיות שהם יתקשו להתגבר עליהם

כבר נכתב רבות על ההשפעות המזיקות שיכולות להיות לבינה מלאכותית (AI) ולמידת מכונה על אנשים וארגונים לאור העובדה שהן מייצרות תוצאות מוטות המבוססות על נתונים סלקטיביים, חלקיים או לא טובים. הסכנה כה חמורה עד שרוב הפונקציות בביקורת הפנימית מדרגות את הבינה המלאכותית היוצרת בראש טבלת הסיכונים שלהן. עם זאת, ארגונים רבים עשויים להתעלם מסיכון גדול עוד יותר הקשור לשימוש בבינה מלאכותית – אבטחת סייבר ופרטיות.

מכונות מבוססות AI הן עתירות עוצמה, ויכולות ללמוד דפוסי התנהגות, לזהות ולחזות מגמות ולחקות מילים, פעולות, צלילים ותמונות מהר יותר מאי פעם – והכול בדיוקנות רבה. הן גם יכולות להתמודד עם כמויות הרבה יותר גדולות של נתונים. יכולות אלו מגבירות בצורה משמעותית את הסיכונים להונאות, לתוכנות כופר ולאובדן/ גניבה של נתונים, ומעלות את הפוטנציאל להשפעות הרסניות של הסיכונים הללו.

למספר חברות כבר נגרם נזק כבד. בשנת 2019, פושעי סייבר השתמשו בשיחה קולית מזויפת המופעלת על ידי AI כדי לרמות מנכ"ל של חברת אנרגיה באנגליה ושכנעו אותו להעביר 220,000 אירו לגורם שהמנכ"ל האמין שהוא ספק ידוע בהונגריה. בדומה לכך, בשנת 2020 עובד בחברה בהונג קונג נפל קורבן לנוכלים שהשתמשו בטכנולוגיית שיבוט כדי לזייף שיחה מהמנכ"ל שמאשר העברות מזומנים. פשעים אלה התרחשו לפני הופעת הבכורה של בינה מלאכותית יוצרת.

מלבד הונאות אלה, שבהן הבינה המלאכותית מזייפת דמות אמינה בעיני הקורבן, מומחים מזהירים כי הסיכונים המרכזיים שבהם ארגונים צריכים לטפל בהם במהירות הם דליפת נתונים, וכן התקפות סייבר המכוונות למודלים של למידת מכונה, במטרה לייצר במכוון תחזיות או החלטות שגויות. מאחר שאלגוריתמים של AI דורשים בדרך כלל גישה למערכות נתונים גדולות, הפוטנציאל לאובדן נתונים ולפריצות גדל באופן ניכר. כמו כן, מניפולציות של נתונים על ידי האקרים עלולות לגרום נזק רב, למשל במקרים שבהם האקרים משנים בכוונה מידע רפואי או פיננסי של אנשים.

"מערכות בינה מלאכותית מסתמכות על כמויות גדולות של נתונים כדי לאמן מודלים ולבצע תחזיות מדויקות", אומר מוחמד עבדור רזאקה, פרופסור-עמית למחקר במרכז לחדשנות דיגיטלית באוניברסיטת טסייד שבאנגליה. "עם זאת, התלות הרבה בנתונים מעלה חששות לגבי פרצות נתונים, לגבי פרטיות ולגבי הגנה. ייתכן שלארגונים רבים אין מספיק ידע ומומחיות כדי להבין את סיכוני האבטחה הייחודיים הקשורים ל-AI, והם עלולים להמעיט בחשיבות של בדיקה יסודית ותיקוף מודלים ומערכות מבוססי AI".

אם בעבר מתקפות סייבר הסתכמו בהודעות פישנינג גנריות, כיום המתקפות מתוחכמות יותר, אומר וויל ריצ'מנד-קוגן, שותף בסניף אוקספורד של משרד עורכי הדין הבריטי פריט'ס (Freeths) ומומחה לסכסוכים בנושאים של טכנולוגיות מתפתחות, נתונים ופרטיות. המתקפות היום יכולות לכלול שימוש בהודעות דוא"ל שנוצרו על ידי בינה מלאכותית ונכתבו בסגנון של המנכ"ל או סמנכ"ל הכספים, כולל הוראות משכנעות להעביר כספים, או שימוש בהודעות דוא"ל המנסות לשכנע את הנמענים ללחוץ על לינקים שיפעילו נזקות. נגמרו הימים שבהם אנשים יכלו להבחין בהודעות פישנינג בקלות, הוא מזהיר.

"ההתפתחות המהירה של טכנולוגיית הדיפ-פייק פירושה שמתקפת פישנינג עשויה לכלול שיחת אודיו או אפילו שיחת וידאו משכנעת לכאורה מקולגה או מממונה בעסק", אומר ריצ'מנד-קוגן. "ככל שמחשוב קוונטי מתחיל להיות זמין בצורה מסחרית, כך חברות תצטרכנה לבחון מחדש חלק גדול מהסדרי האבטחה הקיימים שלהן, ובמיוחד את ההיבטים התלויים באבטחת סיסמאות והצפנה".

בעיה נוספת שמבקרים צריכים להיות מודעים לה היא הצורך להעלות את הגנת הפרטיות ואבטחת המידע לראש סדר העדיפויות עקב היכולת של הבינה המלאכותית "לחבר בין נקודות". "גם כאשר מבצעים התממת נתונים, אלגוריתם AI עשוי להיות מסוגל לבטל את ההתממה ולהיות מחדש אדם על ידי התאמת הנתונים למקורות מידע זמניים אחרים", אומרת ורה צ'רפאנובה, מנכ"לית ושותפה מייסדת בחברת ייעוץ בנושא ציות, סטודיו אתיקה, בעיר בורמיו שבאיטליה. יכולת זו תפר בהכרח את חוקי הפרטיות ברחבי העולם.

באופן דומה, היא מוסיפה, לאלגוריתמים ספציפיים של בינה מלאכותית יש פוטנציאל לבצע ניחושים ולהוציא תחזיות לא אתיות. בשנת 2012 פרסם ה'ניו יורק טיימס' כתבה על כך שהקמעונאית האמריקאית 'טרנט' זיהתה שלקוחות נמצאות בהיריון לפי קנייה של 25 פריטים שנקנו ביחד, ולאחר מכן השתמשה במידע הזה כדי לשלוח לנשים – ולפעמים גם לילדות – קופונים עבור מוצרי תינוקות. "היום, הכוח והנגישות של AI הרבה יותר גדולים ממה שהיו אז", מזהירה צ'רפאנובה.

ארגונים יכולים לנקוט מספר צעדים מעשיים כדי לצמצם סיכונים אלה. צעד אחד שהוא מובן מאליו, אומרים מומחים, הוא ליישם ולאכוף אמצעי אבטחת נתונים חזקים באמצעות הצפנת נתונים, הגברת אבטחת האחסון והגבלת הגישה למערכי נתונים.

אמצעים אלה צריכים להיות מלווים בהערכה ובעדכון שוטפים של פרוטוקולים ומדיניות אבטחת נתונים כדי ליישר קו עם הסטנדרטים בתעשייה ולהתמודד עם האיומים המתפתחים. עוד חובה היא ביצוע ביקורות והערכות סיכונים יזומות ושוטפות של מודלים של AI ושל נקודות התורפה שלהם.

עם זאת, דארון סאן, ראש מחלקת ה-IT באגודת הדיור של הונג קונג, אומר כי אחת הטעויות הנפוצות ביותר במאמצים לצמצם סיכוני AI היא חוסר ההבנה לגבי הסיכונים הקשורים לטכנולוגיות AI מלכתחילה. "ארגונים עשויים שלא להיות מודעים לסיכוני אבטחת הסייבר והפרטיות הספציפיים הקשורים ל-AI, או אולי הם לא מבינים איך פועלות מערכות AI ואיך הן יכולות להיות פגיעות להתקפות", מסביר סאן. "חוסר ההבנה הזה עלול להוביל להערכות סיכונים לקויות ולאסטרטגיות צמצום סיכונים לא אפקטיביות".

בנוסף, ארגונים עלולים שלא לקחת בחשבון את כל מחזור החיים של פיתוח AI בעת זיהוי וצמצום סיכוני אבטחת סייבר, שכן כל שלב בפיתוח מעלה סיכוני אבטחת סייבר ופרטיות ייחודיים הדורשים מענה, אומר סאן. לדוגמה: יש לבצע תסקיר השפעה על הפרטיות והערכות סיכוני אבטחה בשלב התכנון, בעוד ניטור ובדיקות שוטפות צריכים להתבצע במהלך שלבי הפריסה והתחזוקה.



ארגונים עשויים שלא להיות מודעים לסיכוני אבטחת הסייבר והפרטיות הספציפיים הקשורים ל-AI, או אולי הם לא מבינים איך פועלות מערכות AI ואיך הן יכולות להיות פגיעות להתקפות



מה קורה עם הנתונים

נושא נוסף שארגונים עלולים לפספס הוא קביעת מדיניות ונהלים ברורים עבור האיסוף, השימוש והשיתוף של נתונים, אומר סאן. "ארגונים צריכים להיות שקופים לגבי מערכות ה-AI שלהם, לרבות הצורה שבה הן פועלות, אילו נתונים הן אוספות, ואיך הארגון משתמש בנתונים שהמערכות הללו מייצרות", הוא מסביר. "מנהלי הארגון צריכים לקבוע נוהלי אחריות כדי לוודא שהם משתמשים במערכות AI באופן אתי והוגן, ועליהם להיות שקופים לגבי תקריות ופריצות אם הן מתרחשות".

מבקרים פנימיים צריכים להבין כיצד טכנולוגיות AI משתמשות בנתונים, "ולא רק לחשוב אילו נתונים נכנסים ואילו נתונים יוצאים", אומר ג'יימס גרבר, מנכ"ל חברת אבטחת הסייבר 'סימספייס' הממוקמת בבוסטון. "חוסר היכולת לבצע מעקב בכל הקשור ל-AI הוא כנראה הסוגיה הבעייתית ביותר עבור חברות, במיוחד אם מידע אישי הניתן לזיהוי מעורב בתהליך".

לדוגמה: מבקרים פנימיים צריכים לשאול באיזה אופן נעשה שימוש בנתונים ולאן הם הולכים. האם הם נשארים אצל המפתחים? האם המפתחים משתמשים בנתונים כדי ליצור מערכות אחרות? האם הם חולקים את הנתונים עם מתחרים או עם ספקים אחרים? האם הנתונים נמחקים בכלל?

"חברות צריכות להבין שיש להן אחריות לכל שימוש לרעה שנעשה בנתונים אגב השימוש שלהן בטכנולוגיה, בדיוק כמו חברות הטכנולוגיה שמפתחות את המערכות", אומר גרבר. "הן גם צריכות להיות מודעות לכך במקרים רבים חברות טכנולוגיה אינן נדרשות על פי דין להכניס את המוצרים שלהן ל'ארגז חול' (אזור חסין שבו מפתחים בודקים את המוצרים שלהם בפני רגולטורים כדי לוודא שהם עומדים בדרישות עוד לפני השקתם), ולכך שמפתחים רבים עדיין לא מוודאים שמוצרים נבנים עם הגנת פרטיות כברירת המחדל מלכתחילה".

על ארגונים להבטיח שפרטיות ואבטחה נלקחות בחשבון לכל אורך מחזור החיים של פיתוח AI, אומר סאן. הדבר צריך לכלול ביצוע תסקיר השפעה על הפרטיות והערכות סיכוני אבטחה, כמו גם יישום עקרונות של אבטחה ופרטיות בעיצוב.

"צמצום הסיכונים הקשורים לטכנולוגיות AI דורש גישה פרואקטיבית והוליסטית לאבטחת סייבר ופרטיות המשלבת אמצעים טכניים, ארגוניים וממוקדים באדם", אומר סאן. "אם ארגונים ינקטו בצעדים המעשיים האלה, הם יוכלו לצמצם את הסיכון לאירועי אבטחת סייבר ופרטיות, להגן על השלמות והאמינות של מערכות ותהליכי ה-AI שלהם, ולהבטיח שימוש אתי והוגן בטכנולוגיות של בינה מלאכותית".

מודעות לסיכונים

אחת הטעויות הנפוצות, אומר סאן, היא הסתמכות יתר על פתרונות טכניים כמו הצפנה ובקורות גישה כדי לצמצם סיכונים באבטחת הסייבר של AI במקום לטפל בגורם הבעיה העיקרי – היעדר הכשרת עובדים או מודעות לסיכוני AI. "ארגונים צריכים ליישם אמצעים מגוונים, כגון תוכניות הכשרה ומודעות לעובדים, כדי לוודא שכולם מודעים לסיכונים הקשורים לטכנולוגיות AI ויודעים כיצד להגיב לאיומים פוטנציאליים", הוא אומר.

ארגונים רבים אימצו את השימוש ב'אטבובטים מבוססי בינה מלאכותית כמו ChatGPT, וממשיכים לאפשר את השימוש בהם על אף שסיכונים משמעותיים הקשורים לטכנולוגיה הזאת ידועים היטב. 'אטבובטים יכולים לאפשר התקפות פישנינג, ליצור

מטרת הסדנה

ללמוד את נבכי התקנים המקצועיים המקובלים – תקני ה- IIA, במהדורה המעודכנת, וכן בסיס להשלמת הפערים המתקנים הישנים לחדשים.

בסיס הסדנה

יצאו המשתתפים עם ידע עדכני בנוגע לתקנים המקצועיים המקובלים העדכניים הדרושים לעבודת הביקורת הפנימית.

מתכונת 4x4

4 מפגשים
4 שעות אקדמיות כל מפגש

סה"כ 16 שעות CPE.

שעות

16:45 - 20:25

מועדים

16.12.24 יום ב'

18.12.24 יום ד'

23.12.24 יום ב'

6.1.25 יום ב'

כרטיס והרשמה

באתר הלשכה או בטלפון: 03-3742627

סדנת התקנים החדשים

התקנים המקצועיים הגלובאליים של ה- IIA משמשים בעבודתם כ- 245 אלף מבקרים פנימיים חברי ה- IIA, בכ- 180 מדינות. תקנים אלה אומצו גם ע"י הגופים בהם מדינת ישראל חברה/ נספחת: האו"ם, OECD, IFAC, EU, INTOSAI (איגוד מבקרי המדינה בעולם), הבנק העולמי, רשות משרדי רו"ח ועוד. חוק הביקורת הפנימית וחוקים ורגולציות שונים מאמצים את התקנים ומחילים אותם על עבודת המבקרים הפנימיים בישראל.

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

התקנים חלים על מבקרים פנימיים יחידים ועל פונקציית הביקורת הפנימית. על כל המבקרים הפנימיים חלה האחריות לפעול בהתאם לתקנים המקצועיים הקשורים ליושרה, אובייקטיביות, יכולת מקצועית, זהירות מקצועית, וסודיות וכן בהתאם לתקנים הרלוונטיים לתחומי האחריות שבתפקידם (ממשל, ניהול, וביצוע הביקורת הפנימית). מבקרים פנימיים ראשיים אחראים, בנוסף, על כי פעילות הביקורת הפנימית בכללותה תתבצע בהתאם לתקנים, ולשם השגת תכלית הביקורת הפנימית.

ב- 9/1/2024 עודכנו התקנים המקצועיים הגלובאליים (IIA) במקצוע הביקורת הפנימית.

מרכז אקדמי ומרצה

רו"ח דורון רונן

CIA, CRMA, QAR, CRISC, CSX-F, CDPSE, CFE, MA, LLM

נשיא ויו"ר הוועדה המקצועית – לשכת המבקרים הפנימיים IIA ישראל

חבר ועדת התקנים הבינלאומית IIASB

גיזום הנתונים

מבקרים פנימיים עשויים לרצות לייעץ להנהלה לחשוב מחדש על המדיניות שלה לשמירת נתונים כדי לשפר את אבטחת הסייבר. צריך לבדוק ביסודיות כל כלי AI שיש לו גישה לכל מאגרי הנתונים של הארגון. המטרה היא להיות אפקטיבי, לצד ודאות לגבי אופן השימוש בנתונים ולגבי זהויות הגורמים שאיתם הארגון משתף את הנתונים, אומר ריצ'מונד-קוגן. "כבר ראינו כמה חברות טכנולוגיה שנפלו עקב העלאת מידע מסחרי רגיש לבדיקות צ'אטבוט ציבוריות של AI, מה שהוביל לכך שהמידע הזה הפך לזמין לצדדים שלישיים, לרבות מתחרים של החברה", הוא אומר.

התנהלות נכונה היא חיונית, מבהיר ריצ'מונד-קוגן. "אספו רק את המידע שאתם באמת צריכים, שמרו רק את מה ששימושי, ושמרו אותו רק כל עוד שהוא נחוץ", הוא מייעץ. "כמו כן, תהיו קפדניים לגבי אכיפת מחיקה בתום תקופות השמירה".

דיוויד הלברג, מנהל ביקורת פנימית ואתיקה תאגידית בחברת קמקו, חברה לכריית אורניום בססקטון, אלברטה, קנדה, אומר שארגונים חייבים לבחון מחדש את נוהלי שמירת ואבטחת הנתונים שלהם ככל שמתגבר השימוש בבינה מלאכותית. "הבינה המלאכותית היוצרת דורשת יותר ויותר נתונים כדי לשפר את התפוקות שלה, דבר שמנוגד לחקיקות מרכזיות, כגון הרגולציה הכללית להגנת נתונים (ה-GDPR) וחוק פרטיות הצרכן של מדינת קליפורניה, הקוראים למזעור נתונים", הוא מסביר.

ככל שלארגונים יש יותר נתונים, כך הם נמצאים בסיכון גבוה יותר אם שחקנים רעים יקבלו גישה אליהם. "חברות חייבות להבדיל בין נתונים שהן חייבות להחזיק לבין נתונים שהן רוצות, מכיוון שאובדן כמויות משמעותיות של נתונים ארגוניים ואישיים כתוצאה ממתקפה מבוססת AI עלול להיות קטסטרופלי", אומר הלברג.

טיפול בסיכוני סייבר

אין ספק כי AI הוא כלי רב ערך, אך מבקרים פנימיים צריכים לדעת שהארגונים שלהם אחראים לזיהוי וניהול הסיכונים הגלומים בטכנולוגיה. פריצת סייבר מוצלחת שכוללת כמויות אדירות של נתונים המוזנים למערכות AI תגרום לא רק לקנסות כבדים, אלא גם לעלויות ציות משמעותיות – כמו גם לפגיעה חמורה באמינות.

חשבונות מזויפים נטולי שגיאות בפלטפורמות של מדיה חברתית, ואפילו יכולים לכתב וירוסים כדי לתקוף שפות תכנות אחרות.

בינתיים, ChatGPT מאחסן את כל מה שמוקלד לתוכו, כולל שאלות ופרטי משתמשים. "אם כל המידע הזה ייפול לידיים הלא נכונות, התוצאות עלולות להיות קטסטרופליות בקנה מידה עולמי", אומר סטיוארט פול-רוב, מנכ"ל חברת KCSGE, חברת ייעוץ למודיעין אסטרטגי וניהול סיכונים שנמצאת בלונדון.

ברגע שעובדים משתמשים בכלי AI במקום העבודה, קשה להגביל את הגישה אליהם, אומר ליאון טיל, בודק חדירות בכיר בספקית אבטחת הסייבר IT Governance בלית'ם סנט אנס שבאנגליה. "למשל, איך מונעים מפרנק במכירות גישה לפרטי מקבלי תשלומים עבור קולגות שלו?", הוא שואל. "כדי למנוע גישה, החברה תצטרך להגדיר בדיקנות כל רכיב בנתוני העבודה הזמין ל-ChatGPT ולבנות רשימות של 'מי מורשה גישה למה' – וזה עניין נזיל מאוד".

פתרון אפשרי אחד הוא להיות מאוד סלקטיבי לגבי הסוגים של כלי AI שבהם הארגון משתמש. חברות גדולות כמו אמזון, אפל, סטייגרופ, סמסונג ווריון, אסרו על עובדים להשתמש ב-ChatGPT. רזאקה ממליץ לארגונים לבחור במודלים של AI שעמידים בפני התקפות וליישם טכניקות שונות, כגון אימון עם יריב זיהוי אנומליות, כדי לשפר את החוסן של מודלים מבוססי AI. ארגונים גם צריכים לבצע בדיקות ספקים מפורטות בעת הוצאת שירותים הקשורים ל-AI במיקור חוץ, הוא אומר.

מארק ג'יימס, יועץ בחברה המתמחה בפרטיות נתונים, DQM GRC, בהיי וויקומב שבאנגליה, מסכים כי מבקרים פנימיים "צריכים לוודא שלאפליקציית הצ'אטבוט שבה הם משתמשים יש אינטראקציות מוצפנות כדי למנוע גישה לא מורשית על ידי צדדים שלישיים". הוא ממליץ לארגונים להשתמש בצ'אטבוטים רק ממקורות אמינים ולהימנע משיתוף מידע רגיש כמו סיסמאות או מידע פיננסי בשיחות צ'אטבוט. "זה אמור להבטיח שירות פרטי ומאובטח", הוא אומר.

תמורות וחידושים בתקנים המקצועיים הגלובאליים

מאת:

רו"ח דורון רונן, MA, LLM, CIA, CRMA, QAR, CRISC, CSX-F, CDPSE, CFE
נשיא ויו"ר הוועדה המקצועית לשכת המבקרים הפנימיים IIA ישראל
חבר IIASB - ועדת התקנים הבינלאומית של ה-IIA
שותף מנהל - דורון רונן, רו"ח - ייעוץ בקרה וניהול סיכונים

התקנים המקצועיים שמנחים אותנו בעבודתנו כמבקרים פנימיים אינם קופאים על השמרים, ומתעדכנים בהתאם להתפתחות המקצוע.

בתקנים נעשה שימוש על ידי למעלה מ-245 אלף מבקרים פנימיים בכ-180 מדינות. התקנים אומצו על ידי הגופים הבינלאומיים שבהם מדינת ישראל חברה (או נספחת): האו"ם, ה-OECD, הפדרציה הבינלאומית של רו"ח - IFAC, השוק האירופי המשותף EU, איגוד מבקרי המדינה בעולם INTOSAI, הבנק העולמי, רשתות משרדי רו"ח ועוד. ככל שהפעילות הכלכלית הגלובאלית מתרחבת, כך גדל מספר המשתמשים בתקנים. למעשה, התקנים מאפשרים אחידות מושגית ומקצועית התורמת רבות לשחקנים בשווקים הבינלאומיים בהערכת האפקטיביות של הביקורת הפנימית בישראל מתייחס ל"תקנים מקצועיים מקובלים", והרגולטורים השונים אימצו את תקני לשכת המבקרים הפנימיים העולמית (ה-IIA) כתקנים מחייבים בארץ.

התקנים שלפיהם אנו פועלים משמשים אותנו משנת 2017. לפני הכניסה לפרויקט עדכון התקנים, פרסם ה-IIA סקר מקיף בקרב

מבקרים פנימיים ומחזיקי עניין אחרים, והגיבו לו מעל ל-3,600 אנשים מכל העולם. השאלה המרכזית בסקר הייתה: מה הציפייה שלכם מהתקנים ומה ניתן לשפר בתקנים הקיימים? רוב התשובות התמקדו בפן הפרקטי של התקנים הן מבחינת התוכן והן מבחינת המבנה. מבקרים פנימיים רואים בתקנים לא רק כללים מנחים ומסגרת של עקרונות, אלא גם כלי שישמש אותם בפרקטיקה של הביקורת הפנימית. במקום לחפש ולתור בשדות זרים, ברחבי האינטרנט וברשתות החברתיות אחר תוכניות ביקורת ופרקטיקות מובילות לעבודה במקצוע, המבקרים מעדיפים One-Stop-Shop - כלומר את התקנים המקצועיים של ה-IIA. תפיסה זאת היא אחד מהשינויים המרכזיים לקראת עדכון התקנים.

התקנים הישנים כוללים את משימת והגדרת הביקורת הפנימית, עקרונות ליבה, התקנים, וקוד האתיקה. התקנים החדשים, שפורסמו ב-9/1/2024 וייכנסו לתוקף עד 9/1/2025, כוללים גם את הנחיות היישום (Implementation Guidance). לפני פרסומם כסופיים, פורסמה טיוטת התקנים לציבור המבקרים הפנימיים ומחזיקי העניין, והתקבלו אלפי התייחסות ולמעלה מ-14 אלף הערות פרטניות, שאליהן התייחסה ועדת התקנים הבינלאומית IIASB בכובד ראש. הוועדה המקצועית של לשכת המבקרים הפנימיים IIA ישראל תרגמה את התקנים לעברית.

ריכוז השינויים העיקריים בתקנים

מבנה ותוכן חדשים.

הגדרת תכלית הביקורת הפנימית.

שיקולים ליישום התקנים.

תנאים הכרחיים לממשל תאגידי.

עקרון העמידה בתקנים או מתן הסבר לאי-עמידה בהם.

אסטרטגיה של הביקורת הפנימית.

בניית יחסים מקצועיים

מסקנה: מסקנה כוללת של הביקורת ברמת מטלת הביקורת, מסקנה ברמת נושאים מרכזיים (תמות) ממספר מטלות ביקורת, ומסקנות ברמת היחידה העסקית/ארגונית או הארגון בכללותו.

דגש על פיקוח מצד מועצת המנהלים.

רמת הביצוע כחלק מאיכות הביקורת.

ביטול ההפרדה בהתייחסות התקנים בין ביקורת (הבטחה) לבין יעץ (ייעוץ).

פרק המתייחס למגזר הציבורי.

נושא א'

תכלית הביקורת הפנימית

נושא זה מאחד חלקים ממשימת והגדרת הביקורת הפנימית (כפי שמפורט בתקנים הישנים). הגדרת תכלית הביקורת הפנימית היא: ביקורת פנימית משפרת את יכולת הארגון ליצור, להגן ולשמר ערך, בכך שהיא מספקת למועצת המנהלים ולהנהלה שירותי הבטחה, ייעוץ, תובנות ותחזיות בלתי-תלויים ומבוססי סיכונים. לאחר מכן מפורטות התועלות מתכלית זו, לצד פירוט התנאים ההכרחיים לקיום ביקורת פנימית אפקטיבית.

נושא ב'

אתיקה ומקצועיות

ישרה מקצועית (כולל שימוש מפורש במילים "אומץ מקצועי"), אובייקטיביות, הפגנת יכולת, זהירות מקצועית ראויה (שכוללת עמידה בתקנים, וספקנות מקצועית), ושמירה על סודיות.

נושא ג'

"ממשל ופיקוח על פונקציית הביקורת הפנימית"

נושא מיוחד, משום שמצד אחד הוא חל על פונקציית הביקורת הפנימית ובראשה המבקר הפנימי הראשי, ומצד שני הוא מהווה הנחיות בסיסיות למועצת המנהלים (או ועדת הביקורת). לדוגמה, חבר ועדת ביקורת מוזמן לקרוא את נושא ג' ולהבין מה מצופה ממנו (מבלי להידרש לקרוא את כל יתר הנושאים והתקנים). הסדרי ממשל תאגידי נאותים חיוניים על מנת לאפשר לפונקציית הביקורת הפנימית להיות אפקטיבית. לכן נושא ג' מתווה את הדרישות לעבודה צמודה של מבקרים פנימיים ראשיים יחד עם מועצת המנהלים לצורך ביסוס פונקציית הביקורת הפנימית, להבטיח את מעמדה הבלתי-תלוי, ולפקח על ביצועיה. נושא זה מתווה גם את תחומי האחריות של ההנהלה הבכירה, התומכים בתחומי האחריות של מועצת המנהלים ומקדמים ממשל ופיקוח חזקים על פונקציית הביקורת הפנימית. ברור לכולנו, כי למרות שהמבקר הפנימי הראשי נושא באחריות לדרישות בנושא זה, פעולות מועצת המנהלים וההנהלה הבכירה חיוניות ליכולתה של פונקציית הביקורת הפנימית לממש את תכלית הביקורת הפנימית.

פעולות אלה מוגדרות כ"תנאים חיוניים" בכל תקן, ומסודרות יסודות נחוצים לדיאלוג אפקטיבי בין מועצת המנהלים, ההנהלה



התקנים הגלובאליים החדשים

כוללים חמישה נושאים, 15 עקרונות ו-52 תקנים.

כל **תקן** מחולק לשלושה חלקים: דרישות, שיקולים ליישום התקנים (שמפרטים פרקטיקות מקובלות ומועדפות), ודוגמאות לראייה לעמידה בדרישות התקנים. מילון המונחים מחדד את ההבדלים בין דרישות שהן חובה לבין פרקטיקות מועדפות שראויות ליישום (אך אינן חובה) במסגרת השיקולים, ולבין "רשאי/יכול" לגבי שיקולים ליישום שהם אופציונליים.

דרישות נושאות מהוות חלק ממסגרת הכללים המקצועיים (IPPF), וגם הן מחולקות לשלושה חלקים כאמור. דוגמאות לדרישות נושאות: אבטחת סייבר, ESG, ניהול סיכונים הונאות, המגזר הציבורי ועוד. ה-IIA עומל על הדרישות הנושאות, וחלקן פורסמו כבר כטייטה להתייחסות ציבור המבקרים הפנימיים ומחזיקי העניין.

מבנה התקנים החדשים

בפרק **המבוא** לתקנים מפורטים: עקרונות הבסיס של התקנים הגלובאליים של הביקורת הפנימית, וכן מילון מונחים. מטרתם היא ליצוק שפה אחידה והבנה לגבי אופן השימוש בתקנים. פרק זה מתייחס למשמעות הביקורת כעניין לציבור, חשיבות העמידה בתקנים, וסוגיות מיוחדות לגבי פונקציית ביקורת קטנות ולגבי המגזר הציבורי (לגבי הוקדש גם פרק נפרד בסוף התקנים).

מילון המונחים מחדד את ההבדלים בין רמת הדרישות והשיקולים (חייב, ראוי, רשאי/יכול). המילון מגדיר צ'רטר ומנדט לצד מדריך לביקורת הפנימית ומתודולוגיות של הביקורת הפנימית. לראשונה, ניתן לראות הגדרות של מרכיבי דוח הביקורת: תבחין (נורמה), מצב קיים, ממצא (פער), השלכה, סיבת שורש, המלצות ו/או תוכניות פעולה, וכן מסקנה כוללת. המילון גם מברר לנו את המושג משמעותי או משמעותיות, וגם את המושגים השונים בעולם הסיכונים ואת הפונקציות ובעלי התפקידים בארגון שאליהם התקנים מתייחסים.



כל תקן מחולק לשלושה חלקים: דרישות, שיקולים ליישום התקנים, ודוגמאות לראייה לעמידה בדרישות התקנים. מילון המונחים מחדד את ההבדלים בין דרישות שהן חובה לבין פרקטיקות מועדפות שראויות ליישום



הבכירה והמבקר הפנימי הראשי, אשר בסופו של דבר מאפשר פונקציית ביקורת פנימית אפקטיבית. העקרונות והתקנים בנושא זה כוללים:

- הסמכה מטעם מועצת המנהלים: מנדט וצ'רטר הביקורת הפנימית, ותמיכת מועצת המנהלים והנהלה הבכירה
- מעמד בלתי תלוי: אי-תלות ארגונית, וכישוריו המקצועיים של המבקר הפנימי הראשי
- פיקוח מועצת המנהלים: קשר עם מועצת המנהלים, משאבים, איכות (הערכות איכות חיצונית ופנימיות), הערכת איכות חיצונית

נושא ד'

שנפלה בחלקי הזכות להוביל את כתיבתו במסגרת ה-IASB, מפרט את אחריות המבקר הפנימי הראשי לניהול פונקציית הביקורת הפנימית, בהתאם לכתב האמנה (צ'רטר) של הביקורת הפנימית ולתקנים הגלובאליים של הביקורת הפנימית. אחריות זו כוללת תכנון אסטרטגי, השגת משאבים ושימוש בהם, בניית יחסים מקצועיים, תקשורת עם מחזיקי עניין, והבטחת ושיפור ביצועי הפונקציה. המבקר הפנימי הראשי רשאי להאציל תחומי אחריות מתאימים לאנשי מקצוע מוסמכים אחרים בפונקציית הביקורת הפנימית, אך האחראיות (accountability) היסודית שלו נשמרת. להלן פירוט העקרונות והתקנים בנושא זה:

- תכנון אסטרטגי דורש מהמבקר הפנימי הראשי להבין את המנדט של הביקורת הפנימית ואת תהליכי ה-GRC של הארגון. פונקציית ביקורת פנימית בעלת משאבים ומעמד (מיצוב) נאותים מפתחת ומיישמת אסטרטגיה התומכת בהצלחת הארגון. המבקר הפנימי הראשי ממסד ומיישם מתודולוגיות כדי להנחות את פונקציית הביקורת הפנימית ועל-מנת לפתח את תוכנית עבודת הביקורת פנימית. המתודולוגיות כוללות: מדיניות, תהליכים ונהלים שנקבעו על ידי המבקר הפנימי הראשי, על מנת להנחות את פונקציית הביקורת הפנימית ולשפר את האפקטיביות שלה. התקנים בנושא זה מפרטים את: ההבנה של תהליכי ה-GRC, אסטרטגיית הביקורת הפנימית (שחייבת לכלול חזון, יעדים אסטרטגיים ויזמות תומכות עבור פונקציית הביקורת הפנימית), מתודולוגיות, תוכנית עבודת הביקורת הפנימית, ותיאום עם נותני שירותי הבטחה פנימיים וחיצוניים והסתמכות על עבודתם.
- ניהול משאבי פונקציית הביקורת הפנימית: משאבים פיננסיים, משאבי אנוש, ומשאבים טכנולוגיים.
- תקשור ודיווח באופן אפקטיבי: בניית מערכות יחסים ותקשורת עם מחזיקי עניין, תקשורת אפקטיבית, תקשור

תוצרי הביקורת (לרבות התייחסות לנושא המסקנות הכוללות, כאמור), שגיאות והשמטות, ותקשור ביחס לקבלת סיכונים.

- הגבר האיכות: איכות היא מדד משולב של עמידה בדרישות התקנים הגלובאליים של הביקורת הפנימית ושל מימוש יעדי הביצוע של פונקציית הביקורת הפנימית. לפיכך, תוכנית להבטחה ולשיפור האיכות נועדה להעריך ולקדם את עמידת פונקציית הביקורת הפנימית בדרישות התקנים, להשיג את יעדי הביצוע, ולחתור לשיפור מתמיד. התוכנית כוללת הערכות פנימיות וחיזויות. המבקר הפנימי הראשי אחראי להבטיח שפונקציית הביקורת הפנימית חותרת לשיפור באופן מתמיד. צורך זה דורש פיתוח של **מדדים להערכת הביצועים** של מטלות ביקורת פנימית, של מבקרים פנימיים ושל פונקציית הביקורת הפנימית. מדדים אלה מהווים את הבסיס להערכת ההתקדמות לקראת יעדי הביצוע, לרבות שיפור מתמיד. בעיקרון זה משולבים מספר תקנים: הערכת איכות פנימית (ניטור שוטף והערכות עצמיות תקופתיות), מדידת ביצועים, ופיקוח ושיפור ביצוע מטלת ביקורת תקן 12.2 **מדידת ביצועים** הוא אחד מהחידושים האהובים עליי; כל מנהל בכיר בארגון נמדד לגבי הביצועים של היחידה שבראשה הוא עומד, והמבקר הפנימי לא אמור להיות שונה בעניין זה. מיסוד מדדי ביצוע הוא קריטי, כדי לקבוע האם פונקציית הביקורת הפנימית מממשת את המנדט בהתאם לדרישות התקנים, ומשיגה שיפור בהתאם לאסטרטגיה שלה. לאחר שהמבקר הפנימי יזהה את מדדי הביצוע, ראוי שהוא יקבע מטרות, הן כמותיות והן איכותיות, למעקב אחר ההתקדמות לקראת עמידה ביעדי הביצוע. ראוי שלמבקר הפנימי הראשי תהיה מתודולוגיה לאימות תקופתי של דיוק המדדים המדווחים ולהעלאת ציפיות הביצוע. התקן מפרט 11 דוגמאות לקטגוריות ביצועים שיש לשקול במיסוד יעדים ומדדי ביצוע.

נושא ה'

נוגע לעבודת השטח, כלומר **ביצוע שירותי הביקורת הפנימית**:

תכנון – תכנן באפקטיביות את מטלות הביקורת: תקשור מטלת הביקורת, סקר סיכונים (המינוח הקודם היה "סקר מוקדם") במטלת הביקורת, יעדי מטלת הביקורת והיקפה, תבחינים (נורמות) להערכה, משאבי מטלת הביקורת, ותוכנית מטלת הביקורת (תוכנית ביקורת).

ביצוע – בצע את מטלת הביקורת: איסוף מידע לניתוח והערכה, ניתוחים וממצאים פוטנציאליים של מטלת ביקורת, הערכת הממצאים, המלצות ותוכניות פעולה ליישום, מסקנות מטלת הביקורת, ותיעוד מטלת הביקורת.

דיווח – דווח את תוצרי מטלת הביקורת ונטר אחר יישום תוכניות

הפעולה: דוח סופי של מטלת הביקורת (כולל מרכיבי חובה בדוח), וידוא יישום המלצות או תוכניות פעולה ("בדיקות יישום").

פרק אחרון ומיוחד למגזר הציבורי

"יישום התקנים הגלובאליים
של הביקורת הפנימית במגזר הציבורי"

המקצוע מכיר בייחודיות המגזר הציבורי, והתקנים מתארים מצבים שבהם יישום התקנים עשוי להיות שונה עבור מבקרים פנימיים במגזר הציבורי בשל סוגיות שונות:

- **חוקים ו/או תקנות** אשר משפיעים על יכולת פונקציית הביקורת הפנימית לעמוד באופן מלא בכל הוראות התקנים.
- **ממשל תאגידי ומבנה ארגוני**: פונקציות ביקורת פנימית במגזר הציבורי כפופות למגוון מבנים. ארגונים מסוימים במגזר הציבורי יכולים להיות כפופים למספר רמות ממשל, הן בתוך הארגון והן מחוצה לו; דבר אשר עלול לסבך את יחסי הכפיפות והדיווח של המבקר הפנימי הראשי וכמו כן את הפיקוח על הפונקציה ותקצובה.
- **תקצוב**: תהליכי התקצוב של פונקציות ביקורת פנימית מגוונים מאוד במגזר הציבורי. מבני ממשל ומבנים ארגוניים מסוימים אינם מעניקים למועצת המנהלים ולהנהלה הבכירה סמכות ניהולית על התקציב. מצבים אלה מונעים מהמבקר הפנימי הראשי את היכולת לבקש אישור תקציבי ממועצת המנהלים ומהנהלה הבכירה, ומגבילים את היכולת לבקש או לקבל מימון תקציבי נוסף בשל סדרי עדיפויות אחרים בתקציב הארגוני. לדוגמה, פונקציות ביקורת פנימית מסוימות במגזר הציבורי יכולות להגיש בקשות תקציב עצמאיות למועצת המנהלים או לגוף המחוקק שלהן לצורך אישור. תקציבים אחרים מהווים לעיתים חלק מהתקציב הכלל ארגוני, והקצאת התקציב לפונקציית הביקורת הפנימית נקבעת על ידי ראש הארגון, ולעיתים קרובות מאושרת על ידי גוף מחוקק חיצוני. בכל מקרה, המבקר הפנימי הראשי יכול לבקש ממועצת המנהלים את המשאבים הנדרשים.

סיכום

התקנים החדשים מביאים גִּשׁוֹרָה בסוגיות מגוונות, אך תרומתם העיקרית היא בכך שהם מהווים כלי פרקטי שימושי לטובת העוסקים במקצוע הביקורת הפנימית. אני בטוח שכלי זה ישמש אתכם, חברותי וחבריי המבקרים, שנים רבות קדימה, לצד הדרישות הנושאות שתתעדכנה לעיתים תכופות יותר.

צועדים אל העתיד

מאת:

בראיינט ריצ'רדס | CIA, CMA, הוא מנהל המרכז לאוטומציה של תהליכים חכמים במכללת ניקולס, בדאדלי, מסצ'וסטס.

ג'יי מייקל ג'קה | CIA, CPA, CPCU, CLU, הוא מייסד משותף וראש תחום הקריאייטיב של חברת Flying Pig Audit, Consulting and Training Services, שבסיסה בפניקס, אריזונה.

מאמר מתורגם מגיליון אפריל 2024, כתב העת Internal Auditor

כבר ידוע כי ארגונים משתמשים באוטומציה רובוטית של תהליכים (robotic process automation – RPA) ובבינה מלאכותית (AI) כדי לשפר את התהליכים שלהם. התוצאות מראות פוטנציאל אדיר, אולם עדיין לא ברור מה תהיה ההשפעה של כלים אלה על כוח העבודה העתידי. השאלה שמעסיקה כל מבקר פנימי היא: "האם כלים דיגיטליים יחליפו אותי?"

נראה שהתשובה היא "לא" וגם "כן". על פי פרק 3 בסדרת הפרסומים מאת ה- IIA ודלויט, Moving Internal Audit Deeper into the Digital Age, "כלים דיגיטליים, כגון סקריפטים מתוזמנים, AI-ו RPA, לא צריכים לפעול באופן מנותק, אלא במקביל לצוות הביקורת הפנימית ככוח עבודה דיגיטלי". דברים אלה מובילים לשאלת המשך חשובה: "כיצד תבצע העבודה לצד אותו כוח עבודה דיגיטלי?"

על פי הדוח של מכון מקינזי העולמי Generative AI and the Future of Work in America, "לעיתים קרובות ההתקדמות הטכנולוגית גורמת לשיבושים, אך מבחינה היסטורית, בסופו של דבר, היא הניעה צמיחה כלכלית ותעסוקתית". לכאורה, אמירה זו נכונה לגבי מקצוע הביקורת הפנימית, אבל היא מסתבכת כשמגיעים להיבט השיבוש.

מתחילים להבין מה עלול לקרות אחרי עיון בתחזיות תעסוקה של הלשכה האמריקאית לסטטיסטיקה של העבודה, המשלבות מגמות ב-RPA:

מספר המשרות העוסקות בעיקר במשימות חוזרות

פקידי הנהלת חשבונות, חשבונאות וביקורת והזנת נתונים

ירד ב- 151,400 עד לשנת 2032

קיטון של יותר מ-20%.

מספר המשרות בעלות ערך גבוה יותר בתוך המקצוע

המיוצגות בצורה הטובה ביותר על ידי הקטגוריות של רואי חשבון ומבקרים פנימיים ושל מדעני נתונים

יגדל ב- 67,400 וב-59,400 בהתאמה.

התפקידים בעלי ערך גבוה יותר יקבלו שכר גבוה יותר משמעותית.



כתוצאה מהשימוש ב-AI מקצוע הביקורת הפנימית יהיה בין עשרת המקצועות שיחוו מגמת ירידה חדה ביותר עד לשנת 2030



על אף שהנתונים של הלשכה לסטטיסטיקה כוללים השפעה מסוימת של טכנולוגיות מתפתחות, מכון מקינזי העולמי מספק ניתוח מעמיק יותר, מוסיף את ההשפעה של בינה מלאכותית יוצרת, מספק ניואנסים נוספים לגבי ההשפעה של RPA על עבודת הביקורת הפנימית, ובתוך כך מסבך את כל הסוגיה. על פי הדוח "בינה מלאכותית יוצרת ועתיד העבודה באמריקה", כתוצאה מהשימוש ב-AI מקצוע הביקורת הפנימית יהיה בין עשרת המקצועות שיחוו מגמת ירידה חדה ביותר עד לשנת 2030 צפויים להיות כ-600,000 פחות פקידי הנהלת חשבונות, חשבונאות וביקורת, וכ-100,000 פחות רואי חשבון ומבקרים פנימיים.

סדרת הפרסומים של ה-IIA ודלויט, "קידום הביקורת הפנימית עמוק יותר לתוך העידן הדיגיטלי", מספקת מודל איוש ארגוני חדש עבור תחום הביקורת הפנימית המאשש את האומדנים שמציע מכון מקינזי. מודל "הטרנספורמציה של כוח העבודה" מספק תובנות לגבי האופן שבו חלק מתפקידי הצוות והניהול יוחלפו בכוח עבודה דיגיטלי.

במובנים רבים, התרחיש הזה עדיין מראה פוטנציאל לעבודה חיונית של מבקרים פנימיים. אולם העבודה לצד כוח עבודה דיגיטלי כרוכה גם בסיבוכן משבש שהוא חדש לחלוטין למקצוע ודורש מבט אחר על הקריירה של מבקר פנימי.

נתיבים חדשים

בכוחן של טכנולוגיות כמו RPA ובינה מלאכותית לחולל טרנספורמציה בתחום הביקורת הפנימית, ובהחלט צפוי שזה מה שיקרה בעתיד. טרנספורמציה כזו תחייב שינוי בעבודה שהמבקרים הפנימיים מבצעים, דבר שעלול להשפיע על יכולתם למצוא תעסוקה. על מנת להמשיך ולספק ערך ללקוחות, ואף להעלות את הערך הזה לרמה חדשה, מבקרים פנימיים וצוותי הביקורת יידרשו לנצל את ה-RPA והבינה המלאכותית באסטרטגיה מושכלת.

כפי שמוסבר במאמר בשם "מעבר לאוטומציה", שפורסם בשנת 2015 בעיתון "הרווארד ביזנס ריווי" על ידי תומאס דבנפורט וג'וליה קירבי, מבקרים פנימיים יכולים לאמץ אסטרטגיית "אוגמנטציה" – להתמקד במשימות שבני אדם ממשיכים לבצע היטב, ולשפר ולהעמיק משימות אלו, במקביל לאוטומציה של משימות אחרות. המאמר מציע חמישה "נתיבי אוגמנטציה" עבור מבקרים פנימיים: התמחות בנישות צרות, התמקדות במיומנויות רכות, רכישת מיומנויות טכנולוגיות והפיכה למפתחים אזרחיים, ניווט אסטרטגיית הטכנולוגיה וחיזוי טרנדים עתידיים, ואימוץ תפקידי מנהיגות וראיית-על.

באמצעות פיתוח מיומנויות אלה, במקביל להטמעת טכנולוגיות חדשות, מבקרים פנימיים ימשיכו להיות רלוונטיים ואפילו יגבירו את ערכם בסביבת העבודה המשתנה. על ראשי הביקורת להוביל תהליך זה – לפתח את הצוותים בנתיבים המתאימים, ולהרכיב צוותים עם שילוב נכון של מיומנויות העתיד. כך, באמצעות גישת האוגמנטציה, מבקרים פנימיים לא רק ישמרו על תפקידם ועתידם במקצוע, אלא אף יגבירו את חשיבותם ויצליחו להעלות את ערכם לרמה חדשה המשלימה את הטכנולוגיות החדשניות

לצעוד למעלה המנהיג

תפקיד המנהיג הוא תפקיד שסביר להניח שהטכנולוגיה לא תוכל לגזול. הטכנולוגיה אומנם מסוגלת לעבד נתונים בצורה התומכת במנהיגים, אך היא עדיין חסרה את היכולת לחשיבה אסטרטגית, להנעת צוותים וליישוב מחלוקות.

תפקיד המנהיג תמיד כולל חשיבה אסטרטגית, ניתוח תמונה כוללת, פיקוח על פעילויות והובלת צוותים. עם זאת, בעידן הטרנספורמציה הדיגיטלית, מנהיגות גם דורשת הבנה של השינויים שהטכנולוגיה תחולל במחלקה, וסיוע למחלקה להסתגל לשינויים אלו – תפקיד שהטכנולוגיה כנראה לא תוכל לגזול מהמנהיגים.

זה לא אומר שכל מי ששואף לתפקיד ניהולי חייב להיות ראש מחלקת ביקורת. אלא שאנשים המאמצים גישה זו מזהים הזדמנויות להתקדם לתפקידי ניהול בכל רמה – מנהיג צוות, מפקח, מנהל, דירקטור וכדומה. בין אם מחפשים נתיב לתפקיד ראש מחלקה, ובין אם בוחרים להמשיך בביקורת על מנת לרכוש מיומנויות למנהיגות – רשימת כישורי המנהיגות תישאר רלוונטית.

להצלחה כמנהיג נדרשות מיומנויות כמו פיתוח אסטרטגי, פיתוח כוח אדם, מוטיבציה וכישרון עסקי. מנהיגים מנוסים גם מצביעים על הזדמנויות התפתחות אישית שמציעה הביקורת הפנימית, כמו ניהול פרויקטים, תקשורת עם בעלי עניין וסיוע לחברי צוות. מי שרוצה להתקדם בתחום זה צריך להתחיל בלימודי תעודה, וכן לשקול לעשות תואר שני במנהל עסקים ולימודי המשך נוספים.

כמו כן, התנדבות במועצות וועדות של לשכת המבקרים הפנימיים יכולה לסייע בפיתוח כישורי מנהיגות. לבסוף, חונכות היא גישה נפוצה ומוצלחת ללמוד את השלבים המורכבים של נתיב מאתגר זה.

פיתוח אזרחי תפקיד המפתח האזרחי

מפתחים אזרחיים מזהים הזדמנויות לנצל אוטומציה של תהליכים רובוטיים (RPA) ובינה מלאכותית בתוך מחלקתם, לומדים טכנולוגיות אלו, ומיישמים אותן על מנת לשפר את הפעילות הכוללת. זהו תפקיד מצוין עבור מבקרים פנימיים שרוצים לבנות פתרונות אוטומציה. הם יבינו כיצד התוכנות פועלות, ויישמו אותן על מנת לשפר את ביצועי המחלקה.

אולם אנשים אלו הם יותר מבוני פתרונות בלבד. הם גם משתמשים בידע שלהם בביקורת הפנימית בנושאי סיכונים, בקרות וכו', כדי לסייע במעקב אחר פתרונות טכנולוגיים במחלקה ולהתאים אותם להבטחת יציבות התוכנות. לאחר בניית התוכנות, באחריותם לוודא כי הן פועלות כמתוכנן. דרך נוספת היא לעקוב אחר שינויים בתוכנות, נתונים נכנסים ותהליכים נלווים, ולוודא כי התפוקות עדיין מספקות למחלקת הביקורת הפנימית את המידע הדרוש. אנשים אלו הם קריטיים לפעילויות הביקורת הפנימית העתידיות, כולל הערכה וניטור של סיכוני טכנולוגיות אלו המיושמות מחוץ למחלקה.

התפקיד דורש ידע בנתונים ובטכנולוגיות המשמשים לתכנון ובניית תוכנות, אך הוא גם דורש מיומנויות של אנליסטים כדי להבין כיצד שינויים בתוכנות ישפיעו על התפוקות. הוא גם דורש כמובן את היכולת ליישם את המיומנויות שנרכשו כמבקרים פנימיים (הערכות סיכונים, בקרות, ניתוח תהליכים) לעבודת פיתוח יישומים.

לעובדים שכבר בונים ומפעילים וכן לניתוח נתונים יש הרבה ממיומנויות אלו. השלמת הדרכה בכלים חדשים כמו RPA או בינה מלאכותית יוצרת, תוסיף יכולות ניתוח, אוריינות דיגיטלית ופתרון בעיות, ותשדרג מנחתי נתונים קיימים למפתחים אזרחיים.

מבקרים פנימיים יכולים
לאמץ אסטרטגיית
"אוגמנטציה" – להתמקד
במשימות שבני אדם
ממשיכים לבצע היטב,
ולשפר ולהעמיק משימות
אלו, במקביל לאוטומציה
של משימות אחרות.



לצעוד בנתיב צר המומחה

בכל ארגון ישנם תחומים ייחודיים שבהם לא סביר שהטכנולוגיה תבצע את העבודה - תחומי ידע ספציפיים שבהם הזמן והמאמץ הנדרשים לבניית פתרונות לכריית מידע עולים על התועלת. יש אנשים שאוהבים להיות המומחים המוחלטים, אפילו בתחום צר ביותר. אלו הם אנשים שבונים מוניטין באמצעות התמחות בעומק של קילומטרים וברוחב של סנטימטרים.

האתגר הוא למצוא נישה הדורשת התמחות בתחום כה ספציפי עד שלא ניתן למכר אותה, אך הוא עדיין חשוב מספיק כדי שהארגון יזדקק למידע זה. בתחום הביקורת הפנימית, נישה זו עשויה להיות הצורך בידע מעמיק בתהליך או במחלקה ספציפיים, כמו השייך או משאבי אנוש. העובד יהפוך למומחה הצוות בכל הנוגע לנושאים אלו.

דוגמה נוספת לתחום התמחות צר היא ציור לרגולציה. אומנם יש תוכנות המסוגלות לזהות חוקים ותקנות חדשים, אך למומחה שהנישה שלו היא סוגיות רגולטוריות יש כוח לבצע בחינות מעמיקות כדי לזהות בתקנות אלה התאמות שאחרים ומחשבים אינם מזהים, ולפרש התאמות והבדלים אלו בהיבטים של סיכונים והצורך לבצע ביקורת.

ההכשרה והידע הנדרשים לתפקיד זה תלויים מאוד בנישה עצמה. הניסיון הדרוש כולל הבנה של הארגון והדרך שבה נישה זו היא חלק בלתי נפרד מהצלחתו. העובד נדרש לעבור לימודים והכשרה אינטנסיביים בתחום ההתמחות, ולהיות מעודכן במגמות המתפתחות.

לצעוד ביחד:

המתמחים בתחומי הביקורת הפנימית וניהול סיכונים

אנשים המזדהים עם תפקיד זה הם אלה הממשיכים להתמקד בעבודת הליבה של הביקורת הפנימית תוך התמקדות במיומנויות רכות - מיומנויות שאינן רציונליות בלבד ואינן ניתנות למיכון. אנשים אלו מפתחים את היכולות הבין-אישיות והתוך-אישיות המבדילות בין עבודת הביקורת הפנימית לבין משימות הניתנות למיכון. התפקיד הזה מייצג עבודה עם בינה מלאכותית ואוטומציה של תהליכים רובוטיים, (RPA) שימוש במידע שהם מספקים, ושימוש במיומנויות הרכות בתחום הביקורת הפנימית, הכול כדי לספק את הערך הגלום בכל ביקורת.

המיומנויות הרכות של מבקרים פנימיים תורמות להצלחתם בכל התחומים. אפילו תהליך בסיסי כמו ניהול ראיונות הוא דוגמה לאופן שבו המתמחים בתחומי הביקורת וניתוח הסיכונים משתמשים במיומנויות רכות שטכנולוגיית ה-RPA אינה מסוגלת לשחזר. ניהול טוב של ראיון דורש מבקר פנימי מנוסה שמצטיין בתקשורת ובהתחברות עם אחרים. כשמשלבים מיומנויות אלו עם האינטואיציה שמבקרים פנימיים ותיקים מפתחים, הם יודעים מתי אדם אומר אמת, מתי הוא מוסר אמת חלקית, ומתי הוא לא דובר אמת בכלל. כל תהליכי הביקורת הפנימית דורשים אינטואיציה כזו ואת הטכניקות הנלוות העומדות בבסיסה. אנשים כאלה משפרים את הצוות, ומביאים את נקודות החוזק לכל התחומים שאינם ניתנים למיכון.

העובדים בתפקיד זה יתחילו עם הבנה מעמיקה של התהליכים והיישומים הקיימים בתחומי הביקורת הפנימית וניהול הסיכונים. בנוסף, הם יצטרכו לחזק באופן מתמיד את המיומנויות הרכות - אינטליגנציה רגשית, ניהול מערכות יחסים, ניהול שינויים, תקשורת - וכן את המיומנויות הפסיכולוגיות והחברתיות המהוות את הרכיב האנושי של הביקורת הפנימית. תכונות אלה מאפשרות למבקר הפנימי להבין את פעולותיהם ותגובותיהם של האנשים שעמם הוא עובד.

לצעוד קדימה העתיד

התפקיד הזה משלב תכונות של מנהיג ושל מפתח. מדובר במומחה טכנולוגי שתמיד רוצה לעמוד בחוד החנית. זהו גם מנהיג בעל חזון שלומד, חוזה ומנבא את העתיד שניתן לבנות באמצעות טכנולוגיות חדשות, ופועל לתכנון ויישום של טכנולוגיות חדשות אלה. כפי שניסחו זאת דבנפורט וקירבי, אדם זה "מוביל את המכונות לשלב הבא". זהו אדם שאינו חושש ממה שטכנולוגיות מסוגלות לבצע; זהו אדם הפועל לקביעת המשימות הבאות שלהן. אנשים כאלה מחפשים עתיד שטרם קיים.

עבור הביקורת הפנימית, אלו יהיו האנשים שלא רק יסייעו לקבוע כיצד להשתמש בכלים באופן המיטבי, אלא גם יחפשו את הכלים הבאים. למעשה, בעבודתם למציאת דרכים חדשות ומשופרות לביצוע עבודת הביקורת על ידי מכונות, הם פועלים למעשה להפוך את תפקידם האנושי לביקורת הפנימית למיותר. עם זאת, הם ימשיכו לסייע לאנשי הביקורת הפנימית לפתח מיומנויות וגישות חדשות. הם יחפשו את המשימות שמחשבים אינם מסוגלים לבצע כעת, ויחפשו דרכים להכשיר מחשבים לבצען, הכול כדי להבטיח שהביקורת הפנימית תספק ערך רב יותר ללקוחותיה.

בדומה למפתח, תפקיד זה דורש מיומנויות טכנולוגיות והבנה בזיהוי תרחישי שימוש, פריסת תוכנות וממשל טכנולוגי. אדם כזה גם צריך לדאוג להישאר בחזית הטכנולוגיה ולחקור תרחישי שימוש חדשים. בנוסף, עליו לפתח ולשפר כישורי מנהיגות כמו יצירתיות, חדשנות, פיתוח אסטרטגיה וחזון.



העתיד יהיה מזהיר עבור מבקרים פנימיים המפתחים מיומנויות שמוערכות בארגונים שעוברים טרנספורמציה דיגיטלית.



ההשלכות הרחבות יותר

ישנה חפיפה בין חמש הקטגוריות. לכן ההליכה בכיוון אחד אינה מונעת רכישת ידע ותרגול של היבטים מקטגוריות אחרות. גישות מוצלחות יכללו שפע של שילובים ורמות שונות של התמקצעות. בחינה של הגישות השונות מסייעת להבין כיצד להתקדם בצורה מיטבית. כל המבקרים הפנימיים צריכים להעריך אילו צעדים הכי מתאימים לכישוריהם, לתחומי העניין שלהם ולשאיותיהם. מבקרים פנימיים יכולים לחפש הזדמנויות לשפר את מיומנויותיהם בנתיב הרצוי בהתייעצות עם ראשי הביקורת הפנימית.

הבנת התפקידים והעבודה הכרוכה בהם חשובה גם עבור ראשי הביקורת הפנימית. כל מנהל יצטרך להבין את נתיבו, אך ישנם שני שיקולים נוספים. ראשית, ראשי הביקורת הפנימית צריכים לפעול בתוך המחלקה כדי להבטיח שכולם ממשיכים בנתיב המתאים להם ביותר. פיתוח כישרונות הוא חלק חשוב מעבודתו של כל מנהל, ולכן חשוב מאוד שהוא יסייע למבקרים הפנימיים למצוא הזדמנויות לצמיחה אישית, יספק להם משוב ויעמיד את המשאבים הנדרשים לכך. שנית, ראשי הביקורת הפנימית צריכים לבחון את הרכב המחלקה. בחינת שילוב של חמשת הנתיבים הללו בתוך כל מחלקה הוא המפתח להצלחה. כמובן, כל זה אינו מתייחס לפונקציות ביקורת בסיסיות, אך ראשי הביקורת הפנימית עדיין צריכים לזהות את הפערים ולקבוע כיצד ניתן למלא אותם ממקורות אחרים בארגון.

פוטנציאל לעתיד מזהיר

הטכנולוגיה מביאה הזדמנויות ואתגרים חדשים לעולם הביקורת הפנימית. כאשר עבודה דינית נמחקת מתוכן העבודה, נפתחות הזדמנויות ליצירת ערך נוסף. למידה מתמשכת, עבודה עם טכנולוגיה, חשיבה ביקורתית, גמישות ותושייה, כל אלה יהפכו לחשובות יותר מתמיד. העתיד יהיה מזהיר עבור מבקרים פנימיים המפתחים מיומנויות שמוערכות בארגונים שעוברים טרנספורמציה דיגיטלית.



ביקורת מעקב אחר יישום המלצות

מאת:

איתן כהן | רו"ח, CIA, מנהל המחלקה
לביקורת פיננסית ומעקב יישום המלצות

יחידת הביקורת הפנימית בחברת החשמל

היקף יישום המלצות המבקר הפנימי עשוי ללמד רבות על אפקטיביות עבודת המבקר, על האמון של המבוקרים וההנהלה בעבודתו, ועל השפעתו בארגון. לא בכדי שיעור יישום המלצות המבקר ומועד יישומן יכולות ללמד על מעמדו של המבקר הפנימי בארגון וכיצד הוא נתפס בעיני המבוקרים. שיעור גבוה של יישום המלצות מעיד, בין היתר, כי המבקר נתפס כגורם מקצועי בארגון, בהמלצותיו יש ערך מוסף לשיפור פעולות הארגון, וכי הארגון קשוב לעבודת הביקורת. עם זאת, שיעור היישום אינו המדד היחיד וקיימים מדדים נוספים שלא נרחיב עליהם במאמר זה.

פעילות מעקב אחר יישום ההמלצות הוגדרה כחלק בלתי נפרד מתפקידו של המבקר הפנימי במספר הוראות. כך למשל, רשות החברות הממשלתיות הגדירה חובת מעקב אחר יישום המלצות הביקורת במספר סעיפים בחוזר רשות בנושא "מערך הביקורת הפנימית בחברות הממשלתיות וחברות בת ממשלתיות" (2019-8-1):

סעיף 5(יב) קובע בין תפקידי מערך הביקורת הפנימית, מעקב אחר תיקון הליקויים שהועלו בדוחות ביקורת של המבקר הפנימי, מבקר חיצוני או של גורמי פיקוח אחרים.

סעיף 15(א) קובע כי מערך הביקורת הפנימית יעקוב באופן שוטף אחר יישום המלצותיו על ידי הנהלת החברה בהתאם להחלטת ועדת הביקורת או הדירקטוריון, וזאת על מנת לבדוק את איכות תיקון הליקויים ועל מנת לדווח על כך לוועדת הביקורת או לגורם רלוונטי אחר.

סעיף 14(ו) לחוזר מגדיר חובת דיווח חצי שנתית לוועדת הביקורת על יישום ההמלצות.

גם בתקנים המקצועיים הבינלאומיים (IIA) של לשכת המבקרים הפנימיים העולמית, נמצא ביטוי לחובה זאת. תקן 2500 קובע כי המבקר הפנימי חייב להקים ולתחזק מערכת למעקב אחר התקדמות היישום של התוצאות שדווחו להנהלה. בנוסף תקן A1.2500 קובע כי המבקר הפנימי חייב למסד תהליך מעקב לשם ניטור והבטחה שפעולות ההנהלה מיושמות באופן אפקטיבי או שההנהלה הבכירה נטלה סיכון של אי-נקיטת פעולות.

בתקנים המקצועיים הגלובליים החדשים שפורסמו בתאריך 9.1.2024 וייכנסו לתוקף בתאריך 9.1.2025 נקבע בתקן 15.2 כי המבקרים פנימיים חייבים לוודא כי ההנהלה יישמה את המלצותיהם או את תוכניות הפעולה של ההנהלה, בהתאם למתודולוגיה ממוסדת שנקבעה בתקן.

מטרת המאמר היא לסקור את הדרכים האפשריות ליישום חובת המבקר כאמור לעיל, אולם בטרם ניגש לעניין נתעכב מעט על פעולות המבקר שקודמות לעריכת המעקב ושיש בהן להשפיע על שיעור יישום ההמלצות על ידי המבוקרים. לפי גישת הביקורת הפנימית בחברת החשמל, שיעור יישום ההמלצות ומועד יישומן תלוי במידה רבה במורכבות התהליכים והעומס הניהולי הכרוכים בכך. ומכאן נגזרת אחריותו של המבקר הפנימי לבסס את ממצאי הביקורת ולערוך את דוחות הביקורת ואת המלצותיו באופן ברור ופשוט, כך שיביאו את המבוקר להבנה שנוכח וראוי ליישם את המלצות הביקורת גם אם התהליך מורכב.

נוסף על כך, מבקר פנימי טוב אינו נמדד בדוחות ביקורת עבי כרס וגדושי ממצאים אלא ההיפך הוא הנכון. דווקא דוחות קצרים הכוללים את הממצאים המהותיים ביותר, בהתאמה לסיכוני הארגון, יגבירו את שיתוף הפעולה מצד ההנהלה והמבוקרים בתהליך יישום ההמלצות. בהקשר הזה נציין כי מניסיונו הצפת המבוקרים בהמלצות לא גוררת שיעורים גבוהים יותר של יישומן בבחינת "תפסת מרובה, לא תפסת". נעמוד על כך בהמשך המאמר.



שיעור יישום
המלצות המבקר
ומועד יישומן
יכולות ללמד על
מעמדו של המבקר
הפנימי בארגון
וכיצד הוא נתפס
בעיני המבוקרים



בהוראות המזכרות לעיל אין קביעה על אופן עריכת ביקורת מעקב יישום המלצות. לכן בפרקטיקה פותחו מספר שיטות שארגונים נוקטים בהן בעריכת ביקורת מעקב יישום ההמלצות, ובהן:

- עריכת ביקורת חוזרת/ביקורת מעקב אחר כל דוח ביקורת במהלך השנה העוקבת שלאחר הפצת הדוח המקורי;
- עריכת ביקורת חוזרת/ביקורת מעקב על חלק מדוחות הביקורת או חלק מהמלצות הביקורת. כלומר מיקוד בדוחות או בהמלצות הנוגעות לתהליכים מהותיים ומשמעותיים בארגון. הביקורת על ההמלצות הללו תיערך במהלך השנה העוקבת שלאחר הפצת הדוח המקורי.
- העברת האחריות למבוקרים – המבוקר מדווח לביקורת על יישום ההמלצה, והמבקר הפנימי עורך בדיקה מדגמית של ההמלצות שדווחו כמימוש, אחת לתקופה, לצורך בחינת הדיווח.

במאמר מוסגר יצוין כי גם לעיתוי עריכת המעקב יש השפעה על שיעור יישום ההמלצות. בדרך כלל עורכים ביקורת מעקב יישום המלצות בשנה העוקבת להפצת הדוח המקורי, בין היתר על מנת לאפשר למבוקר זמן סביר לתקן את הליקוי שנמצא בביקורת וליישם את ההמלצה. עם זאת, יש להתאים את מועד עריכת המעקב לסיכונים הגלומים בממצא. כך למשל, ממצא והמלצות הנוגעים לסיכונים בטיחות יבדקו בלוח זמנים קצר יותר (לפעמים גם במהלך הביקורת עצמה). מאידך, ישנן המלצות הנוגעות לתהליכים שמעצם טבעם דורשים לוחות זמנים ממושכים, כמו פיתוח מערכות ממוחשבות. כאן ראוי שבתיאום עם המבוקרים יידחה מועד עריכת המעקב.

בכל תהליך ומועד שיבחר המבקר לערוך את המעקב, יהיה עליו גם להתמודד עם השאלה "מה דינה של המלצה שלא יושמה?".

גישה שלפיה מעצם עריכת ביקורת המעקב יוצא המבקר ידי חובתו, בין שההמלצה יושמה ובין אם לאו, חוטאת למטרת עריכת מעקב אחר יישום ההמלצות. המטרה שלנו במעקב אינה לאסוף נתונים סטטיסטיים על שיעור יישום ההמלצות, אלא לייצר שינוי שיסייע לשפר ולתקן תהליכים לטובת הארגון. לדעתנו, לאורך זמן גישה שלפיה מעצם עריכת ביקורת מעקב פעם אחת, יצא המבקר ידי חובתו, עשויה דווקא להביא לירידה בשיעור יישום ההמלצות, ובהתאמה לפגיעה באפקטיביות הביקורת הפנימית על כל המשתמע מכך.

על מנת להתמודד עם מורכבות הנושא של ביקורת פנימית, בחברת החשמל החליטו לעקוב אחר יישום ההמלצות באופן המשלב כמה מהדרכים המקובלות, ושיש בו, לשיטתנו, כדי לתת מענה לסוגיות שונות שהועלו במאמר זה. שיטה זאת מכונה "ביקורת מתמשכת".



דוחות קצרים הכוללים את הממצאים המהותיים ביותר, בהתאמה לסיכוני הארגון, יגבירו את שיתוף הפעולה מצד ההנהלה והמבוקרים בתהליך יישום ההמלצות



אפרט בקצרה את התהליך מראשיתו ועד סופו:

מעקב סלקטיבי בהתאם לחשיבות הממצאים: מעקב אחר יישום המלצות מהותיות בלבד – תהליכים מהותיים וחשובים, בעלי סיכון גבוה, שיביאו ערך מוסף לארגון. הליך זה נעשה תחת בקרה ואישור מראש של המבקר הפנימית הראשית.

הזנת המלצות למערכת ממוחשבת: הזנה של דוחות/המלצות שאושרו לצורכי מעקב (מערכת מעקב החלטות). המערכת שקופה לכל מטות היחידות בחברה והן רשאיות לצפות בהן, להוסיף מידע רלוונטי, לדווח סטטוס יישום ולצרף מסמכים תומכים.

ביקורת מעקב על המלצות שיחידות החברה דיווחו כמיושמות: מקום שבו המבוקר מדווח על יישום ההמלצה, רק לביקורת הפנימית יש הרשאה לסגירת ההמלצות במערכת הממוחשבת, זאת לאחר עריכת בדיקה עצמאית שאכן ההמלצה יושמה.

ביקורת מעקב על המלצות שהיחידות לא דיווחו עליהן כמיושמות: מדי שנה ובהתאם למועדים שהוגדרו ליישום ההמלצה, הביקורת הפנימית עורכת מעקב אחר ההמלצות הפתוחות שנותרו במערכת. במקום שבו טרם יושמו ההמלצות, נשוב ונבדוק את יישומן מדי שנה עד ליישומן המלא או עד שתתייתרנה.

בנוסף, על מנת "לעודד" את המבוקרים ליישם את המלצות הביקורת אנו עושים שלוש פעולות עיקריות:

1 מדי תקופה, אנו בוחרים נושא מהותי שלגביו עדיין קיימות המלצות פתוחות במערכת הממוחשבת. הנושא משולב בסדר היום של ועדת הביקורת לצורך מתן דיווח של היחידה המבוקרת לוועדה. הרבה פעמים עצם שילוב הנושא בסדר היום מאיץ את הטיפול של היחידות בהמלצות לשם דיווח על השלמתן במערכת.

2 מדי שנה, במסגרת הצגת הדוח השנתי של הביקורת הפנימית למנכ"ל ולוועדת הביקורת של הדירקטוריון, אנו מציגים תמונת מצב השוואתית של סטטוס יישום המלצות מדוחות הביקורת ברמה יחידתית: לכל יחידה בארגון מוצג היקף ושיעור ההמלצות שיושמו במהלך השנה, המלצות הנמצאות בתהליך יישום, והמלצות שטרם יושמו, והכול בחיתוך לפי שנת מתן ההמלצה. לעיתים עצם עדכון היחידות כי המידע הנ"ל צפוי לעלות לוועדה מהווה זרז ליישום ההמלצות.

3 מדי תקופה וכתלות במשאבים, הביקורת בוחרת נושא מהותי שעליו נערך בעבר דוח ביקורת ולגביו קיימות המלצות פתוחות במערכת הממוחשבת. בנושא זה אנו עורכים ביקורת חוזרת – ביקורת מעקב מורחבת.

בשיטת ביקורת מעקב זו אנו מדגישים את חשיבות נושא יישום המלצות הביקורת הפנימית בתודעת יחידות הארגון, מביאים לקשב מצד הנהלת הארגון, לשיפור תהליכים, ולמימוש הערך המוסף הגלום בעבודת הביקורת הפנימית. ככל ששיעור יישום ההמלצות המהותיות של הביקורת בקרב הארגון גבוה יותר, כך גוברת האפקטיביות של הביקורת, ובהתאמה תרומת הביקורת הפנימית לארגון.

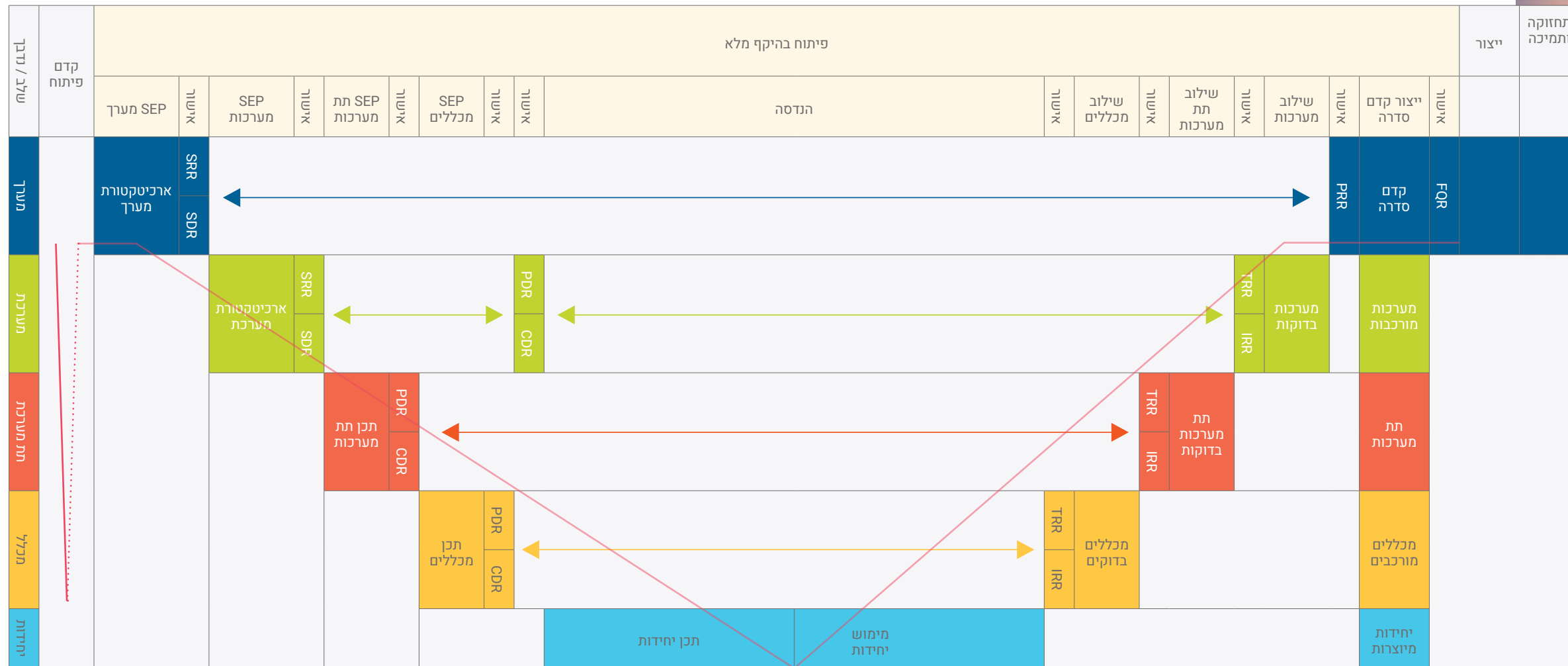
מתודולוגיה לביקורת פנימית בפרויקטים טכנולוגיים

מאת:

ד"ר גדי קרביץ | סגן לביקורת הנדסה בפרויקטים ברפאל

תהליך הנדסת מערכת (Systems Engineering Process) הוא תהליך מולטי-דיסציפלינארי, הוליסטי ורציף לאורך כל מחזור החיים של הפרויקט. ברוב הארגונים הטכנולוגיים הגדולים, היישום של תהליך זה מתבצע בהתאם למודל "V", כמתואר באיור 1. מכיוון שתהליך זה עוסק במערכת הנדסית כוללת של הפרויקט, קיים קושי לבדוד משתנים באופן מוחלט, ולפיכך נוצר קושי לבקרו באופן אפקטיבי. כל רכיב/שלב במערכת תלוי ברכיבים/שלבים אחרים, ולכן ביקורת אפקטיבית אינה יכולה לרוב להסתפק בביקורת על תהליך הנדסי בדיד. מבקר פנימי מוכרח לבחון את התהליך לאורכו, בדגש על ממשקים בין תתי-מערכות שונות של המערכת הראשית, תוך שימת דגש מיוחדת על אפקטיביות של תהליכים הנדסיים רוחביים.

כל פרויקט טכנולוגי נדרש להכין תוכנית מפורטת לניהול הנדסת מערכת של הפרויקט ולבצע בקרה ומעקב קפדני אחר אבני הדרך והפעילויות ההנדסיות שנקבעו בתוכנית זו.



אחד המרכיבים הקריטיים (אם לא הקריטי ביותר) להצלחתו של כל פרויקט טכנולוגי הוא ניהול הנדסי נכון ויעיל של הפרויקט בכל אחד משלביו ולאורך כל מחזור חייו. היות שלבית הפרויקט הטכנולוגי מושתתת על תהליכים הנדסיים, ניהול לא תקין של תהליכים אלה יגביר את הסיכון לנזקים פיננסיים של הפרויקט, לעיכובים באספקתו ולקוח, ולפגיעה משמעותית במוניטין של החברה. במקרים קיצוניים ניהול לא תקין של תהליכים הנדסיים/הנדסת מערכת של הפרויקט אף יכול להביא לקריסת הפרויקט ולסגירתו לאלתר. על מנת למנוע נזקים אלה,

כל פרויקט טכנולוגי נדרש להכין תוכנית מפורטת לניהול הנדסת מערכת של הפרויקט (SEMP - System Engineering Management Plan), ולבצע בקרה ומעקב קפדני אחר אבני הדרך והפעילויות ההנדסיות שנקבעו בתוכנית זו. מכיוון שניהול תהליך הנדסי הוא כה קריטי, גם לביקורת הפנימית בארגון הטכנולוגי יש אחריות לבקרו ולוודא כי תהליכים אלה אכן מתקיימים בפרויקט ומבוצעים באופן יעיל ואפקטיבי.

איור 1 | תהליך הנדסת מערכת במחזור חיי הפרויקט

מאידך, באופן טבעי אין למבקר אפשרות לבחון ולבקר את כל תהליכי הנדסת המערכת בפרויקט, ולכן חשוב שיכיר את הנקודות הקריטיות של הפרויקט, הנקודות שדרכן ניתן לבקר את התהליך באופן מקומי ולהסיק מביקורת זו מסקנות בנוגע לכלל התהליך. אי לכך, המטרה המרכזית של מאמר זה היא להציג בפני המבקר הפנימי העוסק בביקורת טכנולוגית, את הנקודות הקריטיות שיעזרו לו לבקר טוב יותר פרויקטים הנדסיים/מערכתיים, עתירי טכנולוגיות (הכוונה היא לטכנולוגיות מולטי-דיסציפלינאריות המשלבות אלמנטים של תוכנה, קושחה, אלקטרוניקה, מכניקה, בקרה, אלקטרואופטיקה, אנטנות, פניאומטיקה, אלקטרו-מכניקה, מערכות הנעה וכו').

באופן עקרוני ומופשט, אפשר לתאר פרויקט טכנולוגי באמצעות שישה שלבים/תהליכים מרכזיים, שבהם משתלבים תהליכים הנדסיים/הנדסת מערכת לאורך כל מחזור החיים של הפרויקט:

שלב 1
תהליך הצעת מחיר וסקר חוזה

שלב 2
תהליך פיתוח/תכן המוצר

שלב 3
ניסויים ובדיקות להוכחת תכן

שלב 4
תהליך שילובים מערכתיים וניסוי שדה

שלב 5
תהליך ייצור המוצר ושרשרת אספקה

שלב 6
תהליך תמיכה ותחזוקת המוצר.

נציין כי מאמר זה מתייחס לפרויקטים סטנדרטיים המכילים לרוב את כל השלבים שצוינו לעיל. עם זאת, יש לזכור שקיימת אפשרות שפרויקטים מסוימים/מיוחדים לא יכילו את כל השלבים, כגון פרויקטים שעוסקים במחקר או/ו פיתוח, פרויקטי שדרוג, פרויקטי ייצור או/ו תחזוקה וכו'. בפרויקטים אלה המבקר יבחן/יבקר רק את השלבים הרלוונטיים לסוג הפרויקט.

באופן טבעי אין למבקר אפשרות לבחון ולבקר את כל תהליכי הנדסת המערכת בפרויקט, ולכן חשוב שיכיר את הנקודות הקריטיות של הפרויקט, הנקודות שדרכן ניתן לבקר את התהליך באופן מקומי ולהסיק מביקורת זו מסקנות בנוגע לכלל התהליך

בהמשך אתאר מספר נושאים קריטיים המומלצים לביקורת פנימית טכנולוגית/הנדסית בכל שלבי הפרויקט שצוינו לעיל (בדגש על נושאים הנדסיים/טכנולוגיים, כמוכן בנוסף על נושאים לוגיסטיים, תפעוליים, משפטיים, רגולטיביים, פיננסיים וכו' שלא נעסוק בהם במאמר נוכחי). אני משוכנע כי בנושאים אלו הביקורת הפנימית תתרום רבות להורדה שיטתית ומבוקרת של הסיכונים בפרויקטים ובארגון כולו.

שלב 1

תהליך הצעת מחיר וסקר חוזה

נושאים לביקורת הנדסית

1. SOW
2. מפרט טכני
3. דגם עלות

מהות הביקורת הנדסית

1. ודאו קיום מסמך הגדרת תכולות העבודה של הפרויקט (SOW), כחלק בלתי נפרד מהחוזה.
2. ודאו קיום מפרט טכני כחלק בלתי נפרד ממסמך SOW, העונה לדרישות הלקוח.
3. ודאו קיום דגם עלות הנדסי לפרויקט, שעליו מבוססת הצעת מחיר ותחזיות פיננסיות אחרות של הפרויקט.

שלב 2

תהליך פיתוח/תכן מוצר

נושאים לביקורת הנדסית

1. תוכנית פיתוח לפרויקט
2. תוכנית הנדסת מערכת לפרויקט
3. סקרי תכן

מהות הביקורת הנדסית

1. ודאו קיום תוכנית פיתוח של הפרויקט, המכילה בין היתר את הנושאים הנדסיים הבאים: מסמך תיאור המערכת שעומדים לפתח, דרישות הנדסיות העונות על דרישות הלקוח, אבני דרך המכילות סקרי תכן, תוכניות הנדסיות לדיסציפלינות המקצועיות (כולל אבני דרך חוזיות ותוכניתיות), תוכנית ניהול סיכונים הנדסיים וכו'.
2. ודאו תוכנית הנדסת מערכת ברמה פרויקטלית, המכילה בין היתר: תוכנית לניהול דרישות הנדסיות, תוכנית לניהול תצורה/שינויים הנדסיים, תוכנית פיתוח תוכנה, תוכנית בטיחות ואמינות, תוכנית הנדסת אנוש, תוכנית חסינות/סייבר, תוכנית בינה מלאכותית AI (הכוללת לפחות התייחסות לנושאים הבאים: הגנת פרטיות, הבטחת המוצר לאימות מאגרי מידע פתוחים, עקיבות על מקורות מידע ושקיפות, ביצוע סקרי הבטחת איכות לתוכנות AI, הגנות בפני אפילויות, יכולת בקרת איכות-מבדקים חיצוניים, יכולת בקרה והשגחה אנושית על מערכות AI, ניהול סיכונים AI, סקרי בדיקותיות והערכה, הקפדה על רובוסטיות של מערכות AI וכו'), תוכנית הבטחת איכות, הנחיות הנדסיות בנושאים הקשורים לפיתוח המוצר, ייצורו ותחזוקתו, וכו'.
3. ודאו קיום סקרי תיכון במהלך תהליך הפיתוח, כולל סיכומי סקרים ומעקב משימות שהועלו במהלך הסקר, לצורך ביצוע פעילות מתקנת. להלן הסקרים הנהוגים בפרויקטים טכנולוגיים גדולים: סקר להצגת הדרישות המערכתיות (SRR), סקר ראשוני של קונספט המענה לדרישות (SDR - לרוב מהווה אישור נקודת עבודה ראשונית של הפרויקט), סקר לבחינת התכן הראשוני של מערכת/מכלול (PDR) - כולל בחירת חלופות מרכזיות, סקרי אינטגרציה של המערכת ובדיקות להוכחת תהליך תכן, כולל סקר מסכם הסוקר את עמידת המערכת בכל המפרטים (FQR). הסקר מבוסס על בדיקות לאישור תכן (QUAL) שבוצעו ברמת מערכת ובדיקות לאישור תכן (POD) ברמת מכלולים/תת-מכלולים, פריטי קצה וכו'. בנוסף על סקרים אלה, מומלץ לבקר גם סקרי תכן ייעודיים לתוכנה (כגון סקרי דרישות, סקרי קוד, סקרי בדיקות תוכנה, סקרי אינטגרציה וכו'), וכן סקרים שבוצעו על ידי ספקים חיצוניים (אם היו כאלה).





הכנס המקצועי השנתי של הביקורת הפנימית 2025 Save the Date

יום חמישי, 23 בינואר 2025
LAGO, ראשון לציון

שלב 3

ניסויים ובדיקות הוכחת תכן

נושאים לביקורת הנדסית

1. תהליך ייצור אב טיפוס
2. תוכנית לאימות ותיקוף תכן (V&V)

מהות הביקורת הנדסית

1. ודאו תקינות תהליך ייצור ואישור אב טיפוס לצורך בדיקה ואישור התכן.
2. ודאו קיום תוכנית לאימות ותיקוף התכן וביצוע בדיקות פיתוח בהתאם לתוכנית זו.

שלב 5

תהליך ייצור המוצר ושרשרת אספקה

נושאים לביקורת הנדסית

1. סקר מוכנות לייצור
2. אישור קדם סדרה
3. תהליך ייצור והרכבה של המוצר
4. בדיקות קבלה ואספקת המוצר ללקוח

מהות הביקורת הנדסית

1. ודאו קיום ואישור סקר מוכנות לייצור (PRR), כולל סיכום הסקר ומעקב משימות שהועלו במהלכו, לצורך ביצוע פעילות מתקנת.
2. ודאו ביצוע תהליך אישור קדם סדרה (FAI), המוודא השלמת כל התנאים הנדרשים לתחילת הייצור הסדרתי של המוצר.
3. ודאו ביצוע תהליך ייצור שוטף, בחינה והרכבה של המוצר, בהתאם לסימוכני הייצור/הוראות הרכבה/ שרטוטים וכו' (כולל תהליכי הבטחת איכות, כגון ניהול תצורה/שינויים, ניתוח תקלות, מעקב פעילות מתקנת, קיום מבדקים/תחקירים פנימיים, ביקורת מכנית/אופטית/אלקטרונית לפריטי קצה המיוצרים אצל ספקים חיצוניים), וכן ניהול מערכת כיוול ציוד בקו הייצור.
4. ודאו קיום מערכות בדיקה (צב"דים) וביצוע בדיקות קבלה למוצר (ATP) לפני אספקתו ללקוח.

שלב 4

תהליך שילובים מערכתיים וניסויי שדה

נושאים לביקורת הנדסית

1. תוכנית שילובים וניסויים מערכתיים

מהות הביקורת הנדסית

1. ודאו קיום תוכנית שילובים וניסויים מערכתיים, וכן ביצוע ניסויים ובדיקות לאישור תכן (כולל בדיקות QUAL שבוצעו ברמת מערכת ובדיקות אישור תכן POD ברמת מכלולים/תת-מכלולים/פריטי קצה) בהתאם לתוכנית זו ומפרטים טכניים נלווים.

שלב 6

תהליך תמיכה במוצר ותחזוקתו

נושאים לביקורת הנדסית

1. תוכניות תמיכה ותחזוקת מוצר
2. שירות לקוחות

מהות הביקורת הנדסית

1. ודאו קיום תוכנית תמיכה כוללת לפרויקט (ILS), תוכנית אחזקתיות והתיישנות של המוצר.
2. ודאו קיום ויישום תהליך תחזוקה מונעת/ שבר למוצרים שסופקו ללקוח, במסגרת אחריות או/ו חוזה תחזוקה.

היות שביקורת טכנולוגית, כפי שתוארה לעיל, מתבצעת לרוב מול גורמים טכניים/הנדסיים בארגון העוסקים באופן ישיר או עקיף בתהליכים טכנולוגיים/הנדסיים לאורך כל שלבי הפרויקט, עומק הביקורת של כל נושא ונושא בטבלה תלוי מאוד ברקע ההנדסי של המבקר הפנימי. במקרים שאין למבקר רקע הנדסי מתאים, מומלץ מאוד להיעזר במומחה תוכן חיצוני או פנים-ארגוני.

אבטחה נאותה וביקורת של מכשור רפואי במוסדות רפואיים

מאת:

רפאל גולוב | CIA, CRISC, CISA,
CISM, CDPSE, CCAK, GICSP

בבתי החולים המודרניים ישנם אלפי מכשירים רפואיים מסוגים שונים ושל יצרנים שונים. הרבה מהם מחוברים לרשתות בית החולים. לחלק ניכר מהמכשירים הללו קיימת גישה מרחוק מצד היצרנים שלהם לצורך ניטור, שליטה ועדכון, לעיתים אף ללא ידיעת המוסד הרפואי. היעדר הגנה נאותה במכשירים רפואיים עלול להביא למצב של פגיעה בחיי אדם, השבתת בית החולים, דליפת מידע אישי, ונזק קשה למוניטין של המוסד הרפואי.



הרגולטורים הרלוונטיים בעולם המערבי מאמצים בשנים האחרונות מודל של חלוקת אחריות לנושאי הגנת הסייבר של מכשור רפואי בין הגורמים הבאים:

יצרני מכשור רפואי, הנדרשים
לייצר מכשור שמתאפיין
ב-cyber and privacy by
design.



בתי החולים, שנדרשים
ליישם הגנת סייבר נאותה
על התשתיות שלהם ולעדכן
ולתחזק מכשור רפואי בהתאם
להוראות היצרנים.



משתמשי קצה (סגל רפואי
ומטופלים), שנדרשים למלא
את הנחיות המדריך למשתמש
(הכולל הוראות המתייחסות
לאבטחת מידע והגנת
הפרטיות).

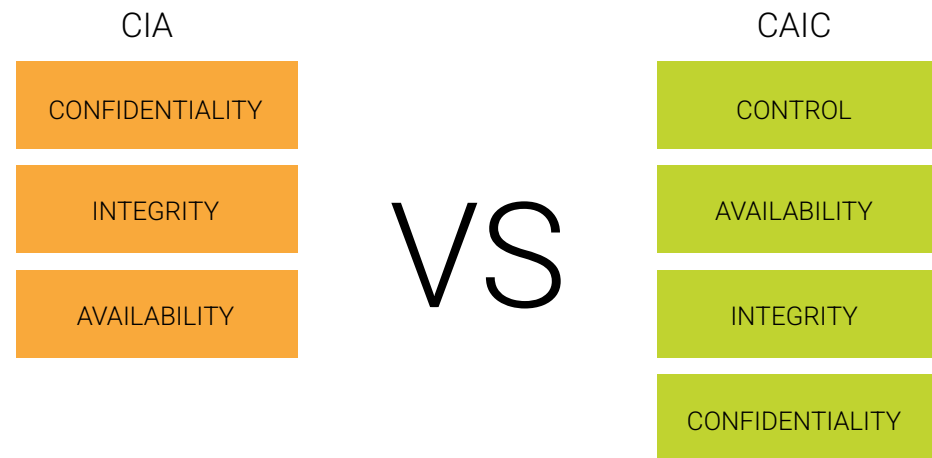


גופי הגנת הסייבר המגזרים
והמדינתיים, שבאחריותם
לנטר ולהרתיע גורמי תקיפה
מאורגנים שמבקשים לפגוע
במערכת הבריאות. בישראל,
למשל, גוף כזה הוא מערך
הסייבר הלאומי.



המאמר יעסוק בהבנת חולשות אופייניות של מכשור רפואי (מודרני ומורשת) ובמתן כלים להערכת חומרת חולשות אלו. מטרת המאמר היא לספק למבקר הפנימי כלים יישומיים לביצוע ביקורת יעילה יותר בתחום הגנת הסייבר של המכשור הרפואי.

המורכבות של יעדי הגנת הסייבר על מכשור רפואי מומחשת באיור הבא (CAIC אל מול CIA המסורתי):

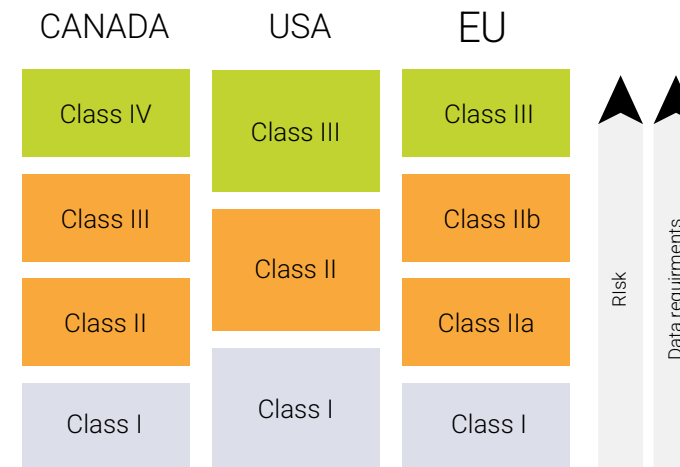


הכוונה באיור הזה היא כי למכשור רפואי התווסף יעד "CONTROL" (ניטור ובקרה) בנוסף על אמינות, זמינות וסודיות מעולם אבטחת המידע ה"מסורתי", כאשר לא בהכרח חל שינוי בחשיבות המרכיבים הללו.

חולשות הגנת סייבר אופייניות במכשור רפואי

מומחי אבטחת המידע נוטים להצביע על החולשות הבאות המאפיינות מכשירים רפואיים רבים:

- היעדר נראות של המכשור הרפואי ברשת ובמערכות ניטור. ציוד ומכשור רפואי לא מחוברים לרוב לאמצעי ניטור ובקרה.
- היעדר הבנה לגבי התנהגות נורמלית ואנומלית של מכשיר רפואי. גם אם המכשיר מנוטר בדרך כלשהי, נדרשת הבנה מעמיקה בנוגע לאופן הפעילות שלו על מנת להבין האם תפקודו משובש כתוצאה מאירוע סייבר.
- השפעה ישירה על בריאות המטופל ועל תהליכים רפואיים. הצורך בזמינות גבוהה ובתגובה מיידית של מכשיר רפואי עלול להשפיע, למשל, על היכולת להתקין בו אמצעי אבטחת מידע, היות שהדבר עלול לגרום לעיכוב במענה ולצורך את משאבי המערכת (כגון מעבד, זיכרון, רוחב פס).
- היעדר נראות של המכשור הרפואי ברשת ובמערכות ניטור. ציוד ומכשור רפואי לא מחוברים לרוב לאמצעי ניטור ובקרה.
- היעדר משאבים ויתרות לתיקון חולשות (אין עודף מכשירים בשביל להשבית מכשיר שנשלח לשדרוג מרכיבים פגיעים).
- בנוסף, בדרך כלל רשת של בית חולים היא מאתגרת להגנה. לא מדובר ברשת אחת בשילוב של עשרות רבות של רשתות שונות כגון (IoT) Internet of Things, Operational Technology, מערכות ניהול בניין (חניונים, מעליות), בטיחות וביטחון, מצלמות במעגל סגור ועוד. מכשירים רפואיים יכולים להשתייך לרשתות פחות מאובטחות שלא נמצאות באחריות סגל ה-IT.
- תוכנה, מערכות הפעלה (לעיתים גם חומרה) ופרוטוקולים ייעודיים לא מאובטחים, בדגש על מכשירי מורשת. מכשירים רבים הם תולדה של פיתוח ארוך של מספר גופים או של חברות קטנות שנקנו על ידי חברות גדולות יותר במרוצת השנים. במקרים רבים נבחרו רכיבי נישה ונעשה פיתוח עצמאי של קושחה ותוכנה.



מטרות הגנת הסייבר על מכשור רפואי

מכשירים רפואיים מסווגים למספר קטגוריות בהתאם לרמת סיכון פוטנציאלית למטופל (או למפעיל), וכתוצאה מכך יש הבדל בכמות הבקורות ובסוג הבקורות שיש ליישם בפיתוח המכשיר ובהפעלתו ובתהליך האישור הרגולטורי של המכשיר. ככלל, מקובל לייחד כשלוש קטגוריות מרמת סיכון נמוכה לגבוהה, כמוצג באיור הבא:

דוגמה למכשיר Class I מרחום ביתי



דוגמה למכשיר Class III מכונת הנשמה



מכשיר שמסווג כ-Class I מייצר רמת סיכון נמוכה למטופל או למפעיל, ואילו מכשיר שמסווג כ-Class III עלול לייצר סיכון גבוה למטופל או למטפל.

פעולות אבטחת המידע נועדו לשמור על סודיות, אמינות וזמינות של נכסי המידע הארגוניים. אולם בעולם המכשור הרפואי קיימות מטרות שונות במקצת:

שמירה על קניין רוחני

פיתוח של מכשירים רפואיים הוא בדרך כלל מלאכת מחשבת של אנשי מקצוע רבים במשך שנים ארוכות. "הנדסה לאחור" של מכשיר רפואי עלולה לאפשר לגורם זדוני פגיעה כלכלית קשה ביצרן מכשור רפואי ובמכוני המחקר המעורבים בפיתוחו.

מניעת חשיפת מידע אישי של מטופלים, עובדים, קבלנים וצדדים שלישיים נוספים.

מידע רפואי של מטופלים נחשב לרגיש ביותר, ולכן זליגתו מחוץ לכותלי המוסד הרפואי עלולה לגרום לפגיעה קשה במוניטין ולסנקציות רגולטוריות כבדות.

הבטחת פעילות תקינה ורציפה של מכשירים רפואיים

כל מכשיר רפואי באשר הוא נועד למטרה אבחונית או טיפולית מסוימת. מצב שבו המכשיר לא זמין או לא פועל כמצופה עלול להסב נזק למטופל ולשבש את התהליך הטיפולי בו.

מניעת מצב של שימוש במכשיר כמשטח תקיפה כנגד מכשירים ורשתות אחרים בבית החולים

בדרך כלל מכשירים רפואיים אינם נמצאים במצב מנותק. אחיזה של התוקף במכשיר אחד עלולה לאפשר לו להתבסס ברשתות בתי החולים ולזלוג לכיוון מכשירים אחרים, חיוניים יותר לתהליך הטיפולי.

דגשים לביקורת בנושא הגנת הסייבר של מכשור רפואי

הבנת חלוקת האחריות לניהול נכסי המכשור רפואי. בתוך כך יש לברר את הסוגיות הבאות:

מי במוסד הרפואי אחראי על אבטחת מכשור רפואי?

האם ישנו נוהל או נוהג מיוחד לאבטחת מכשור רפואי?

האם נושא הגנת הסייבר מקבל התייחסות בתהליכי הרכש של מכשור רפואי?

האם קיימת הגדרה של השימוש המיועד (intended use) לכל מכשיר ומכשיר והאם השימוש בפועל תואם להגדרה זו?

האם ידועה ומתועדת רשימת הסיווגים (הרגולטוריים) של המכשור הרפואי?

האם ידוע מתי מכשיר רפואי מגיע ל-end-of-life ו-end-of support?

האם קיים פירוט של רכיבי המכשור הרפואי (תוכנה, קושחה, חומרה, אביזרים)?

האם ידועה הזהות של יצרני המכשיר, של גורמי האחזקה ושל המשתמשים?

לאילו רשתות משויך מכשור רפואי והאם קיימים תרשימים של רשתות אלו? מי מנהל אותן וכיצד הן מוגנות ומנוטרות?

האם למוסד הרפואי קיים תהליך התמודדות עם אירוע סייבר במכשיר רפואי וטכנולוגי?

אמצעים ותהליכים הגנת סייבר של יצרן מכשור רפואי. בתוך כך יש לעבור על רשימת התיגו הבאה:

האם קיימת התייחסות לנושאי אבטחת המידע והגנת הפרטיות במדריך למשתמש (IFU)?

האם קיימת התייחסות לנושאי אבטחת המידע והגנת הפרטיות ב-service manual שמיועד לאנשי השירות?

האם המכשיר הרפואי מכיל אמצעי אבטחת מידע לוגיים ומאיזה סוג? כיצד הם מנוהלים ומתוחזקים?

האם יצרן המכשור הרפואי מקיים תהליך של פיתוח מאובטח שכולל Software Threat Modeling ו-failure modes and effects analysis, מבדקי חדירה חיצוניים למכשיר הרפואי (בהתאם לסיווג המכשיר והשימוש המיועד שלו)?

האם יצרן המכשיר מנהל מעקב ומבצע עדכון על חולשות אבטחה במכשירים ששווקו?

האם קיימת אותנטיקציה הדדית בין הרכיבים השונים של המכשיר הרפואי?

קישוריות של המכשיר הרפואי והגישה אליו מרחוק:

אילו יכולות קישוריות קיימות למכשיר רפואי ולטובת מה (ניטור/עדכונים/אחר)?

מתי הקישוריות מתרחשת?

כיצד נעשתה הגבלת קישוריות?

האם ליצרן המכשיר או לנותן התמיכה יש גישה מרחוק? אם כן, האם בית החולים מודע לכך ונותן הסכמה לביצוע הקישוריות? האם היא קצובה בזמן?

האם נעשה שימוש במדיה נתיקה? אם כן, כיצד היא "מזוכה"?

מידע אישי שעשוי להימצא במכשיר. על המבקר הפנימי לברר את האספקטים הבאים:

האם המכשיר הרפואי שומר מידע אישי של המטופלים ושל המטפלים? אם כן, האם קיימת הצדקה לכך?

האם בוצעה הגבלת יכולת שמירת מידע אישי לא חיוני?

האם המידע האישי מוצפן?

למשך כמה זמן מידע אישי נשמר?

כיצד מידע אישי נמחק מהמכשיר?

האם ליצרן המכשיר/נותן התמיכה יש יכולת לייצא מידע אישי של המטופלים והמטפלים?

עדכוני תוכנה וקושחה שנדרשים הן לצורך טיוב הגנת הסייבר על המכשיר והן לטובת המיות רגולטורי. כאן יש שני תתי-נושאים:

האם ליצרן המכשור הרפואי קיימת תוכנית להתקנת עדכוני תוכנה (פונקציונליות, תיקון באגים)?

האם תהליך העדכון מתואם עם בית החולים וייחודי לסביבת המוסד הרפואי?

סיכום

המאמר מהווה אשנב לעולם סיכוני סייבר של מכשור רפואי במוסדות רפואיים. הוא מספק נקודת פתיחה לביצוע ביקורת בסיסית בתחום. נושאים מתקדמים יותר ידרשו היכרות מעמיקה עם הרגולציה הרלוונטית ותהליכים רפואיים.

אם המבקר הפנימי נדרש לבצע ביקורת בתחום לראשונה, מומלץ להתמקד תחילה במכשור יישן יותר, בעל סיווג כ-Class III ושתומך בתהליכים רפואיים קריטיים (כגון מכונות הנשמה).

President's Note



Doron Ronen | CPA, CIA, CRMA, QAR, CRISC, CSX-F, CDPSE, CFE, MA, LLM
President of IIA Israel – Institute of Internal Auditors

All of us, as a nation, are in the midst of a turbulent period. We hope that you and your families are healthy and are remaining optimistic and that together, we will prevail. We convey our heartfelt condolences to the bereaved families, wish the wounded a speedy recovery, and wish for the swift return of our hostages and soldiers. We also express our support for the defense forces who are fighting on our behalf.

Wartime is a difficult and complex period for all Israelis. Nevertheless, we believe that it is very important to continue the IIA's routine activities, to maintain professionalism and provide solutions to all internal auditors.

Accordingly, I will briefly update you about highlights of our activities:

The professional committee published guidelines – “**Internal auditing during times of crisis (the Swords of Iron war)**” and recommendations for synergetic work by audit committees as a tool for business continuity in times of crisis. The IIA's new **Global Internal Audit Standards** have been published, were translated by the professional committee and disseminated to members. In an article I wrote in this issue, I review the changes and innovations in the Global Internal Audit Standards.

The Conferences and Education Committee led extensive activities through a variety of courses, workshops, seminars and conferences, and initiated and coordinated studies at several academic institutions.

The main theme of our successful **annual conference** was **AI**. The guest of honor, State Comptroller, CPA Matanyahu Englman, described the innovations in the State Audit in 2024. Dr. Ziv Katzir, the head of Israel's National Program for Artificial Intelligence, reviewed the activities of his unit. The professional sessions included lectures on such topics as MRI tools, ChatGPT, the use of AI during internal auditing, the digital bang, risk management, and more.

We continued strengthening our relations with the **regulators** and with other **professional bodies**. We met with the director of the Ministry of Justice's unit regulating the internal auditing profession to discuss legislative amendments. We published a paper on the subject of wartime auditing in collaboration with the Israel's Directors Union. **The various professional committees and forums** also proceeded with their activities.

I congratulate the editorial board headed by **Lior Segal** for this issue and the professional articles on the subject of **AI**.

In closing, I appeal to anyone who has not yet done so, to **join the IIA** so that we can continue augmenting our extensive activities to strengthen the profession and its practitioners.

Best wishes for good health, resilience, accomplishments and growth, and that we swiftly achieve peaceful times.

Best wishes for the speedy recovery of the wounded and for the swift return of our hostages and soldiers.

Happy new year,

Yours faithfully,
Doron Ronen

Editor's Note



Lior Segal | MBA, CIA, CRMA, QAR, CISA, CISM, CRISC, CDPSE

I am excited to present Issue 18 of IIA Israel's Internal Auditor, which is dedicated to the topic “IA with AI.”

This is the first issue I have had the privilege of editing, and I would like to thank my colleagues heading the editorial board, Shalom Cohen, Gershon Lewinsky and Dror Bar Moshe. Thanks also to Sharon Witkowski Tabib, who faithfully and devotedly edited 15 issues of the magazine.

The subject of artificial intelligence is of considerable importance because it is changing our world and inviting numerous opportunities and challenges. In an era when data and algorithms have become an integral part of organizations' decision-making processes, internal auditors must attain a thorough understanding of the uses of AI and its associated risks as an audit subject. AI is also an important and efficient tool for performing internal audits. Its automation, data analysis and pattern recognition capabilities can augment the effectiveness of audits and therefore, in this digital age, it is essential for internal auditors to acquire proficiency in the use of AI. The subject of AI was also a significant theme during conferences held this year by IIA Israel and by the global IIA.

Among the articles included in this issue, I call your attention to the following articles:

- In the article “Artificial intelligence and internal auditing,” the author elaborates on several areas where AI can be useful during internal auditing.
- In the article “AI tools in the service of internal auditing,” the authors maintain that AI can offer significant advantages by automating internal audit activities, by improving audit quality and value and by providing continuous monitoring and assurance.
- In the article “Looking to the future – AI, ChatGPT and internal auditing,” the author analyzes the impact of AI, and presents the opportunities and challenges relevant to internal auditing.
- In the article “Does our title define us?” the authors wrestle with the question of whether the organizational title affects the perception of other personnel in the organization – or even our own perception – of the nature of our role or our place in the organization.
- The article “Growing Threat” argues that the more that organizations use AI, the more they risk being overwhelmed by cybersecurity and privacy threats.

This issue also contains several other interesting and helpful articles.

I would like to thank the professional committee and its chairman, Doron Ronen, for the project translating the Global Internal Audit Standards into Hebrew. The new standards, which were preceded by a lengthy discussion process by the IIA Standards Board, have a tremendous impact on all those engaging in internal auditing, and we will most likely address them in future issues.

My thanks to all members of the magazine's editorial board.

I am echoing the best wishes conveyed by the President of IIA Israel, Doron Ronen, and hope for the swift return of our hostages and of all evacuated residents to their homes.

Lior Segal

Editor _____ **Lior Segal** | Advocate, CPA, MBA, CIA, CRMA, QAR, CISA, CISM, CRISC, CDPSE

Editorial Team _____ **Dror Bar Moshe** | CPA, LLM, CIA, CISA, CRMA, CRISC, CFE, CSX - F, CDPSE, AWS - CP

Gershon Levinsky | CRMA, MBA, CPA

Shalom Chohen | CPA, CIA

Dr. Noam Koriat | PHD, CISA

Sharon Witkowski Tabib | CPA, CIA, CRMA

Oren Shachar | CPA, CIA, CISA, MBA

David Agranat | CPA (Isr.), CIA

Eyal Oron | Adv

Nancy Zakak Abu Elnaser | CPA, MA, QAR

Nava Halamish | CPA, MA

Dr. Gabi Sayag | D.E.A

Boaz Aner | CPA, CIA, MA

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

Eran Shahaf | Adv, MBA

Assaf karmon | CIA, CISA

Institute of Internal Auditors _____ **Inna Golderbiter** and **Adi Hazot**

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: **03-3742627** | 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



THE INTERNAL AUDITOR JOURNAL

לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA Israel - Institute of Internal Auditors



ת.ד. 29281, תל אביב, 6129201 | טל. 03-3742627
www.theiia.org.il