

# ביקורת IT לא רק למבקרי IT

**מנחה: גלית מור, אגף ביקורת מ"מ**

**בר וויס סלהוב, CRISC, CISA, ראש ענף ביקורת תשתיות, תהליכי IT  
ודגיטל –**

**חטיבת הביקורת הפנימית, בנק לאומי**

**אילנה שחורי, רו"ח, CIA, CISA, CRMA,**

**מנכ"ל משותף בחברת IS-IA**



# טכנולוגיה, טכנולוגיה, טכנולוגיה

כמעט כל תהליך מבוסס טכנולוגיה:

- שכפול דפים/תמונות

- שיחה עם רופא המשפחה

- פעולה בנקאית

- ניתוח פעילות שיימינג במשטרה

קניות בצ'ק

קניות בצ'ק?

הכל נעשה באמצעות מערכות/טכנולוגיה

מה תפקידו של מבקר הפנים בעולם החדשני הזה?

האם יש מקום לביקורת תהליכית ללא מבט על המערכת התומכת?

# תפקידו והכשרתו של המבקר הפנימי

מבקר מערכות מידע, מחזיק במקצוע מאוד מבוקש, חדשני, דינמי וטכנולוגי

אך האם זה מייתר את תפקידו של המבקר הפנימי - בוודאי שלא!!!

מבקר פנימי, מומחה בעולמות הביקורת ובעולמות עיסקיים

אם כן, מה בכל זאת השינוי המוצע?

במפגש היום- נציג מתודולוגיה :

- להרחבת היכולות והכלים של המבקר הפנימי

- להתמודדות עם העולם החדשני/הטכנולוגי

# מה המטרה?

מדוע השינוי נדרש?

הטכנולוגיה והמערכות מיושמות בכל תהליך

? אז מה בכל זאת?

ביקורת תהליכית ללא בדיקת המערכת התומכת הינה ביקורת חלקית

אז איך בכל זאת, ניתן לשדרג את הביקורת?

הכשרת מבקרים עם סל כלים מגוון יותר

ומה יקרה עם מבקרי IO?

הם יוכלו להתמקד בנושאים טכנולוגיים חדשניים:

סייבר, ענן, OPEN API, IOT, רשתות תקשורת, DR.....

# מה היתרונות בהרחבת היכולות של מבקר הפנים:

## יתרונות עבור מבקר פנים:

- ביקורת תהליכית-שמתייחסת למערכת התומכת - הינה ביקורת מקיפה ומקצועית
- ביקורת שמבוססת על כלים יותר מתקדמים ומעניינים
- שיקוף תמונה רחבה מקצה לקצה להנהלה ולוועדת הביקורת

## יתרונות עבור מבקרי IT:

- פינוי זמן להתמקד בטכנולוגיות חדשות
- התמודדות עם סיכוני IT מורכבים בביקורת על מערכות ליבה- חלף ביקורת

מערכת בסיסיות

# אתגרים בניהול השינוי:

נדרש:

- לשכנע את הארגון שמבקר פנימי מסוגל להתמודד עם ביקורת מערכת
- לרתום את המבקר להתמודד עם הכשרה חדשה ואתגר טכנולוגי
- להוכיח שהתוצאה הכוללת מביאה ערך מוסף לארגון
- לשכנע את מבקרי ה-IT שזה לא מחליף אותם, אלא מרחיב את היריעה

# השיטה:

- הגדרת מנהל פרויקט בארגון
- בניית תכנית ביקורת מערכות קצה
- הגדרת תכנית הדרכה
- התנסות בליווי של מבקר מערכות מנוסה
- הפקת לקחים
- הטמעה בשטח

# ולפרקטיקה...

מהי המתודולוגיה וכיצד מיישמים אותה?

אני מזמינה את:

בר וייס סלהוב

ואילנה שחורי

לחשוף את המתודולוגיה

ולספר על היישום בפועל ויתרונותיו



# חלוקה של המגרש....

מבקר מערכות מידע-  
מערכות טכנולוגיות  
מורכבות

מבקר פנימי-  
מערכת "קצה"

מערכת ליבה- מערכת  
רוחבית

מערכת נישתית

מערכת בעלת מורכבות  
טכנולוגית

מערכת פשוטה טכנולוגית

מיקוד טכנולוגי

מיקוד עסקי

היבטים טכנולוגיים מעמיקים  
- מחשוב ענן / תקשורת /  
ניהול בסיסי נתונים

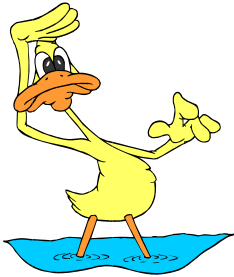
היבטי תהליכיים בהתייחס  
למערכת המידע

# 5 היבטים מתחום מערכות המידע שמומלץ לשלב במסגרת ביקורת תהליך עסקי:

1. מידת התאמת המערכת לצרכי הארגון
2. היבטי אבטחת מידע בסיסיים
3. בחינת הבקורות המיכוניות
4. היבטי זמינות ותפעול
5. המשכיות עסקית

1.

# מידת התאמת המערכת לצרכי הארגון ומידת השימוש בה



על מה נסתכל

❖ מערכת ידידותית, קלה לשימוש וכוללת את המידע הנדרש לשם ביצוע הפעילות העסקית.

❖ המשתמשים שותפים בתהליך הגדרת הדרישות והמבדקים של המערכת וקיימת תוכנית הדרכה והטמעה אפקטיבית.



**בזבוז משאבים וחוסר יעילות.**

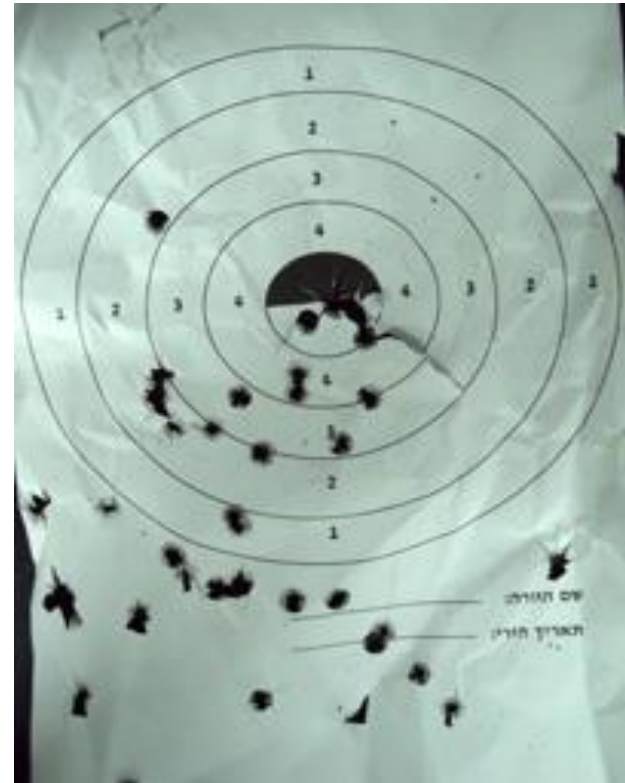
**רמת שימוש נמוכה עם המערכת ויצירת תהליכי עבודה מקביליים למערכת באופן שיצור סיכון תפעולי לפעילות הארגון.**

# ונעבור לשטח...

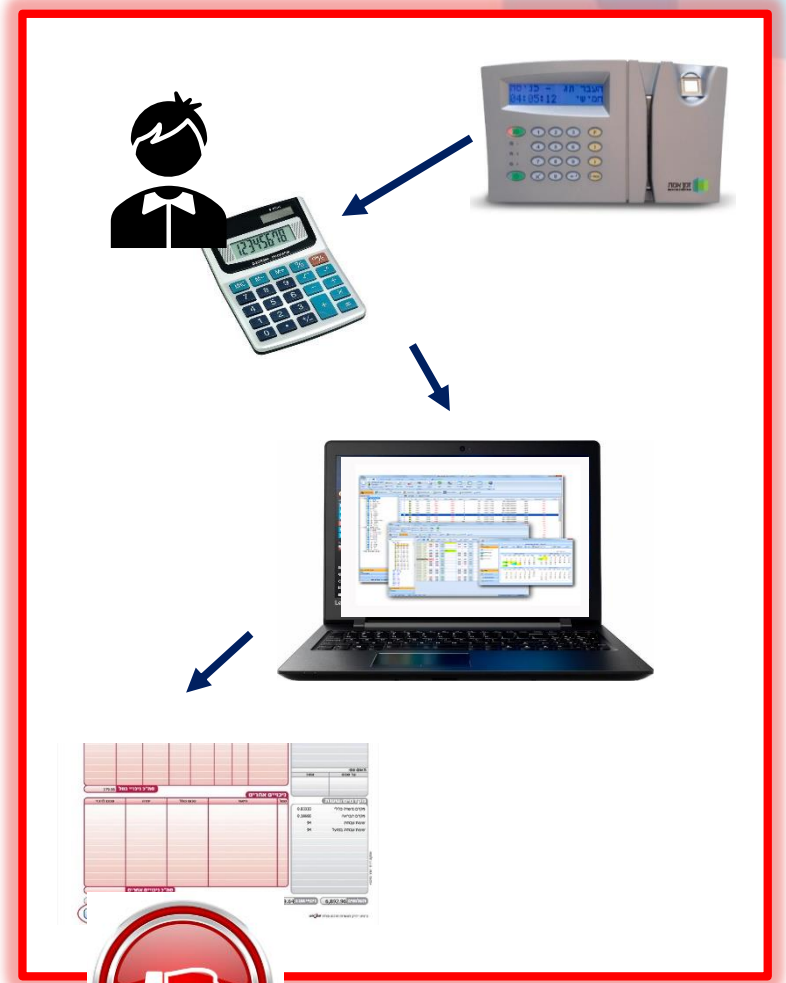
# ממציאים את הגלגל?



# קלעו למטרה?

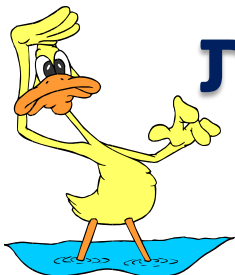


# התערבות ידנית?



# נא להוציא ניידים, בוחרן פתע!





## 2. היבטי אבטחת מידע-ניהול הרשאות



### על מה נסתכל

❖ ניהול הרשאות – על בסיס הצורך לדעת ואשר יבטיח הפרדת תפקידים נאותה.

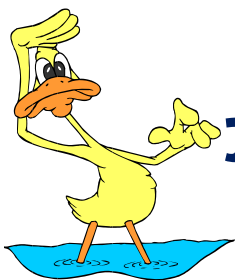
❖ בקרה אחר הרשאות – קיומו של תהליך בקרה שוטף אחר ההרשאות המוגדרות במערכת.



**הרשאות עודפות עלולות להוביל לפעילות שאינה מורשית  
ובניגוד לסמכויות שהוגדרו וכן למעילות והונאות**

# מי יכול ללחוץ על הכפתור?





# היבטי אבטחת מידע – אבטחה פיזית

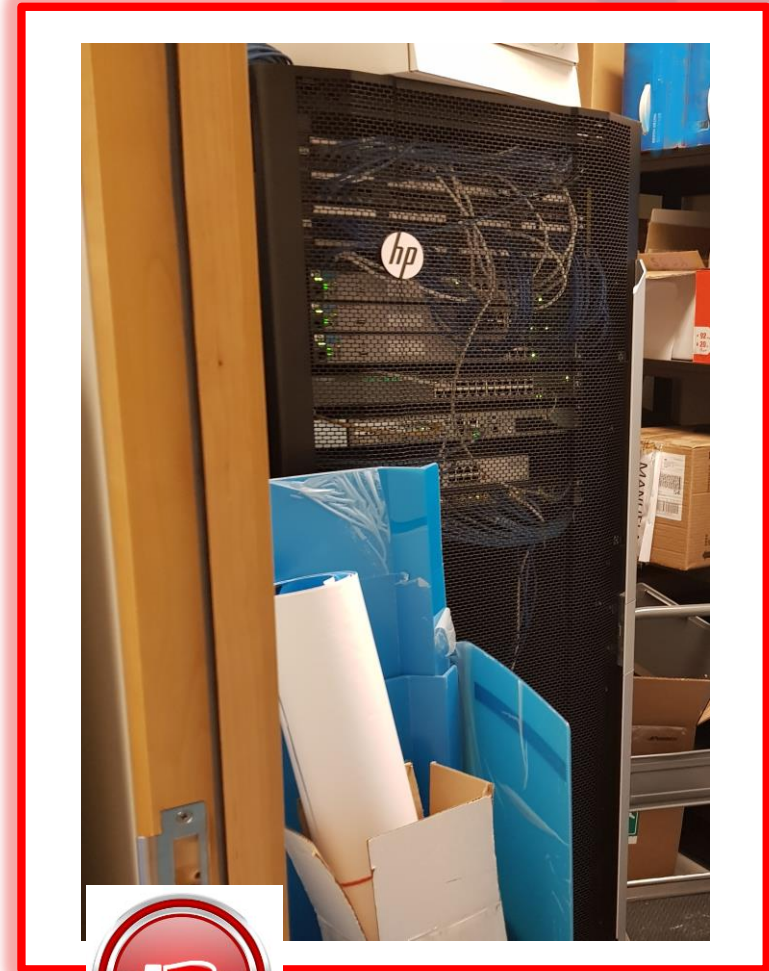
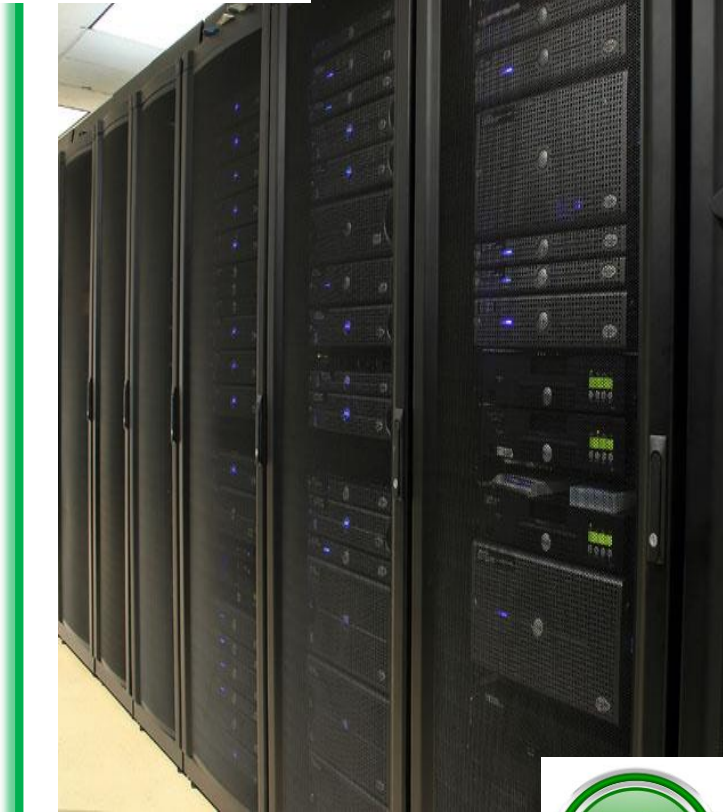
## ❖ על מה נסתכל

- ❖ מדיניות "שולחן נקי" – איחסון מידע רגיש במקום מאובטח
- ❖ גישה למתחמים רגישים - גישה למורשים בלבד, יישום אמצעי הגנה פיזיים (בקרת כניסה, מצלמה).
- ❖ יישום אמצעי הגנה סביבתיים



**פגיעה בחיי אדם, אובדן מידע,  
מניעת שירות עסקי ודלף מידע.**

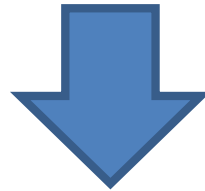
# רצוי ומצוי....



# שאלה לקהל...

# 3. בקרות מיכוניות

- ❖ בקרות קלט – תפקידן למנוע הזנת נתונים שגויים או לא מתאימים
- ❖ בקרות עיבוד – תפקידן לוודא שלמות ודיוק עיבוד הנתונים
- ❖ בקרות פלט – תפקידן להבטיח שנתוני המערכת יועברו ליעדן בצורה המיטבית תוך שמירה על אמינות הנתונים



**בקרות מיכוניות חסרות עלולות לפגוע באיכות הנתונים הקיימים במערכת ובמערכות אחרות ובכך ליצור סיכון תפעולי משמעותי לארגון.**

# בקורות קלט לדוגמא

אימות נתונים

הגדרות הודעת קלט התראת שגיאה

הצג הודעת קלט בעת בחירה בתא

כאשר תא נבחר, הצג הודעת קלט זו:

כותרת: \_\_\_\_\_

מרכז עלות \_\_\_\_\_

הודעת קלט: \_\_\_\_\_

הזן קוד מרכז עלות בן 3 ספרות מ- 100 עד 1999

ביטול אישור נקה הכל

אימות נתונים

הגדרות הודעת קלט התראת שגיאה

הצג התראת שגיאה לאחר הזנת נתונים לא חוקיים

כאשר משתמש מזין נתונים לא חוקיים, הצג התראת שגיאה זו:

סגנון: \_\_\_\_\_

עצור \_\_\_\_\_

הודעת שגיאה: \_\_\_\_\_

ביטול אישור נקה הכל

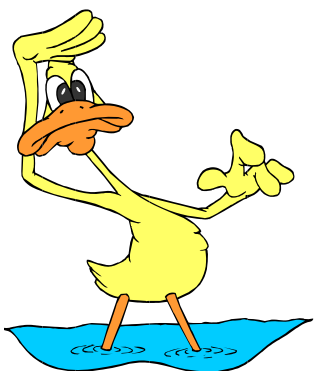
# בקורות עיבוד ובקורות פלט - אז מה ואיך לבדוק?





# שאלת הכה את המומחה





## 4. זמינות ותפעול

על מה נסתכל

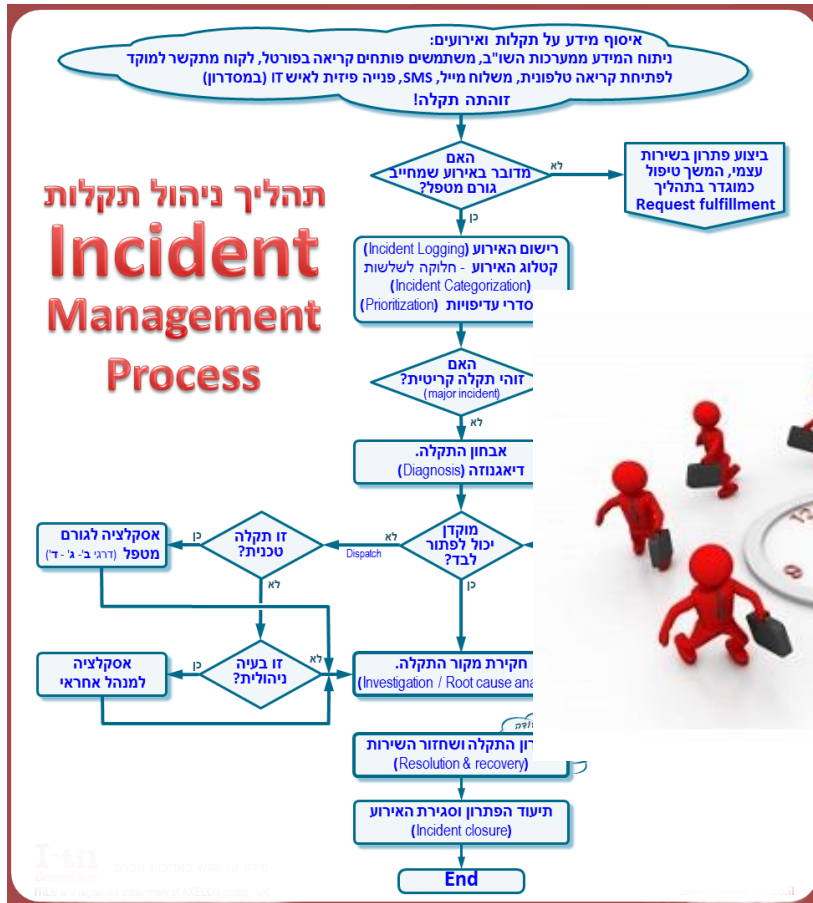


- ❖ היקף התקלות
- ❖ מוקד הזיהוי של התקלה (משתמש או יחידת התפעול/IT)
- ❖ תהליך ומשך הזמן לטיפול בתקלות
- ❖ ביצוע הפקות לקחים בעקבות התקלה



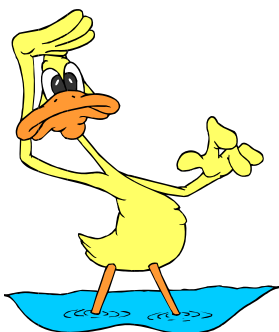
**זמינות המערכת מהווה יעד מרכזי במטרה לאפשר רציפות עסקית ומניעת פגיעה בארגון ובלקוחותיו .**

# נקודות לבחינה בנושא זמינות ותפעול..



# שאלה אחת לפני הסוף





## 5. המשכיות עסקית



על מה נסתכל

- ❖ האם המערכת הוגדרה כמערכת קריטית לארגון ואם כן האם משולבת בתוכנית ההמשכיות העסקית של הארגון ובתוכנית התרגולים?
- ❖ האם העובדים מודעים ומכירים את תוכנית ההמשכיות העסקית?



**העדר היערכות להתמודדות עם מצבי חירום עלולה להוביל לנזקים תפעוליים גדולים**

# יודעים מה לעשות בשעת חירום?



# ולסיום סיומת...



k7080876 www.fotosearch.com



**בר וויס סלהוב**

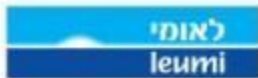
**052-9426187**

**[Bar.Waiss@BankLeumi.co.il](mailto:Bar.Waiss@BankLeumi.co.il)**

**אילנה שחורי**

**054-8088023**

**[ilana@is-ia.co.il](mailto:ilana@is-ia.co.il)**



לאומי איתך.

