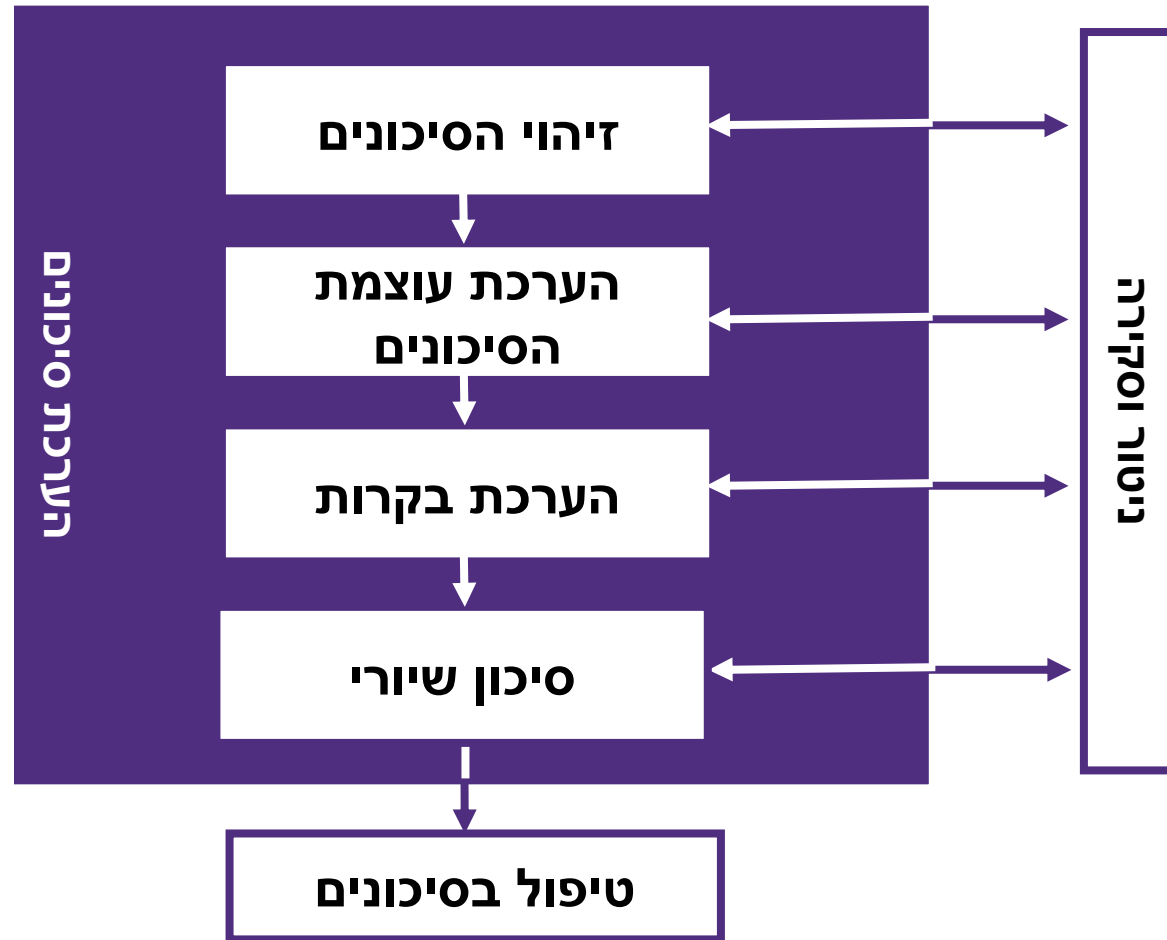


# מתודולוגיית סקר סיכונים



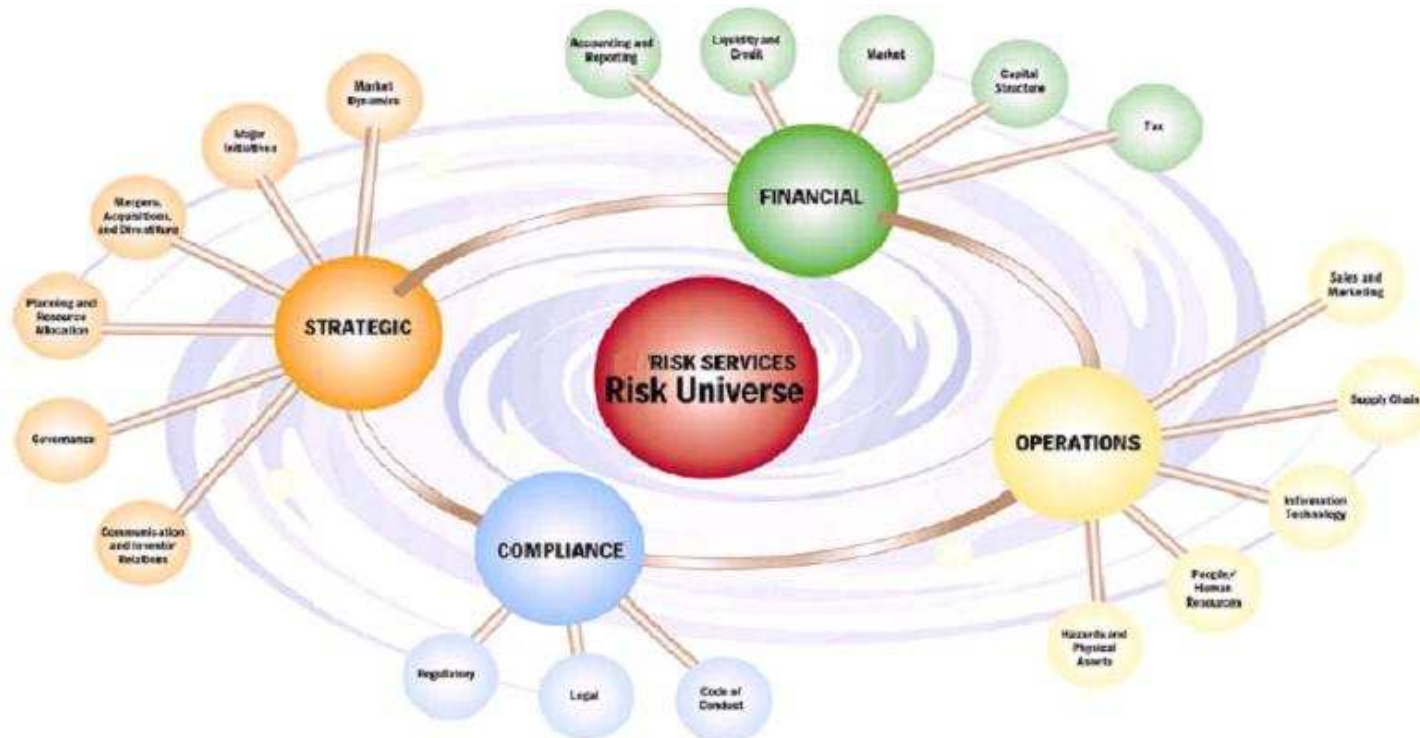
רו"ח דורון כהן, שותף,  
פאהן קנה ניהול בקרה בע"מ

# תהליך ניהול הסיכונים



# הגדרת עולם סיכונים של הארגון

לפני שמתחילים לטפל בסיכונים צריך לבדוק אילו סוגי סיכונים מאיימים על הארגון, כלומר: מהו "עולם הסיכונים" בו פועל הארגון?



# קטגוריות של סיכוני מפתח

## ✓ אסטרטגיים

### מינהל וארגון

Board Structure & Performance  
Tone at The Top  
Corporate Monitoring  
Organizational Structure

### תכנון והקצאת משאבים

Strategic Planning  
Budgeting  
Forecasting  
Acquisition and Divestiture

### בעלי עניין

Shareholder  
Business Partner  
Customer  
Supplier

### דינמיקת השוק

Competition  
Socio-Political  
Economic Factors

## ✓ תפעוליים

### שרשרת הערך

Design and Development  
Supply Chain and Logistics  
Production  
Marketing and Sales  
Service  
Support Processes  
Business Continuity

### נכסים פיזיים

Real Estate  
Plant and Equipment  
Inventory

### אנשים ותרבות

Culture  
Recruitment & Retention  
Development & Performance  
Health and Safety

### טכנולוגיות מידע

IT Security and Access  
IT Availability and Continuity  
IT Integrity  
IT Infrastructure

## ✓ ציות

### סטנדרטים של התנהגות

### עסקית

Corporate Social Responsibility  
Ethics  
Fraud

### רגולציה

Trade  
Labor  
Environmental  
Privacy  
Product Integrity

### משפט

Contract  
Liability

## ✓ פיננסיים

### שוק

Interest Rate  
Foreign Currency  
Commodity

### אשראי ונדילות

Cash Management  
Funding  
Hedging  
Credit and Collectables  
Insurance

### חשבונאות ודיווח

Reporting and Disclosure  
Internal Control  
Tax

### מבנה ההון

Debt  
Equity

## שיטת ניתוח הסיכונים:

כל יחידה או תהליך נבחן באמצעות רשימת סיכונים פוטנציאליים מוגדרת. בגין כל סיכון נבחנים שני פרמטרים:

**1. עוצמה**

**2. הסתברות להתרחשויות**

עוצמת הסיכון נבחנה על בסיס:

- היקף הכספי הנובע מהתהליך המנותח
- חשיפה משפטית
- חשיפה לפגיעה במוניטין או נכסים בלתי מוחשיים אחרים.

## חישוב ההסתברות

- ההסתברות להתרחשות הסיכון נקבעת על בסיס מספר פרמטרים:
  - מורכבות התהליך
  - תדירות התהליך
  - חשיפה למעילות
  - מוטת שליטה
  - הערכת ההנהלה
  - פרמטרים נוספים שרלוונטיים לחברה הספציפית
- כל אחד ממרכיבי הסיכון, דורג בציון של 5 – 1:1 משקף רמת סיכון נמוכה ו-5 רמת סיכון גבוהה.

# חישוב רמת סיכון משוקללת

דוגמא לשקלול רמות סיכון :

רמת חשיפה			הסתברות					עוצמה			תיאור הסיכון		
ציון לתהליך	חשיפה לתהליך	עוצמה X הסתברות	סה"כ	הערכת ההנהלה	מוטת שליטה	חשיפה למעילות	תדירות	מורכבות	סה"כ	מוניטין/אחר	חשיפה משפטית	כספי	
				משקל						משקל			
				4	5	4	2	5		2	2	5	
				ציון	ציון	ציון	ציון	ציון		ציון	ציון	ציון	
<b>A</b>	15.06	A 15.83	3.85	5	4	1	4	5	4.11	5	1	5	<b>Y</b>

הסיכונים, מסווגים לרמות הבאות:

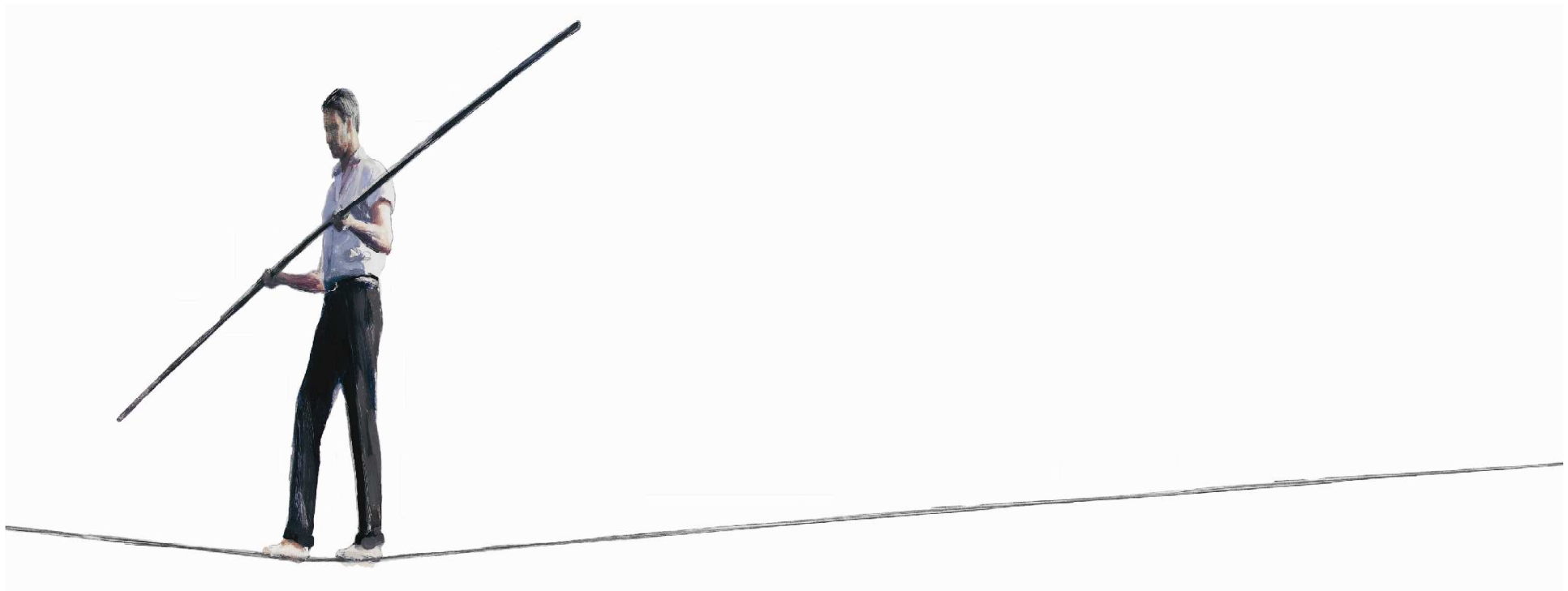
**A** - גבוהה ביותר      **B** - גבוהה      **C** - בינונית      **D** - נמוכה

# רשימת היחידות או התהליכים שנבדקו ודירוגם :

רמת סיכון				נושאים	יחידה
D	C	B	A		
			✓	שכר	יחידה X
		✓		רכש	
	✓			מערכות מידע - בקרות כלליות	
0	1	1	1	סה"כ	

הסיכון השיורי

## סיכון - בקרה



## הערכת רמת הבקרה וחישוב הסיכון השיורי

- ככלל על מנת להגיע למסקנה מבוססת אודות רמת הבקרה יש לבצע בדיקות מבססות כגון: בתהליך ביקורת פנימית.
- יחד עם זאת לא ניתן במסגרת סקר הסיכונים לבצע בדיקות פרטניות של כל הבקורות המיושמות בארגון.

## הערכת רמת הבקרה

עריכת טיב ואיכות הבקרה תתבצע ע"פ מדד משוקלל הלוקח בחשבון מספר פרמטרים לדוגמא:

- **בדיקה ישירה של הפעולה:** עד כמה הפעולות השוטפות נבדקות באופן ספציפי. לדוגמא, כל חשבונית נבדקת אל מול הזמנה, כניסה למחסן וכו' - בקרה טובה. אם הבקרה היא מדגמית – בקרה חלשה.
- **הפרדת תפקידים או ריכוז סמכויות:** הפרדת תפקידים גבוהה תגביר את איכות הבקרה. לעומת זאת, במצב שבו רוב הפעילות מנוהלת ע"י איש אחד ואינה מבוקרת ע"י מערכת חיצונית - בקרה חלשה.

## הערכת רמת הבקרה - המשך

- **פיקוח על ידי מנהלי העובד:** באיזו מידה קיים סיכון בהתחשב ברמת הפיקוח הנהוגה באותה פעילות שנסקרת. ככל שהפיקוח הדוק ויעיל יותר-בקרה חזקה יותר.

# הערכת טיב הבקרות לניהול הסיכונים ושקלול הסיכון השיורי:

על מנת לקבוע את רמת הסיכון השיורי מבוצע תחשיב כדלהלן:  
1. **רמת הסיכון המשולבת** ביחידה או בתהליך העסקי (עוצמה X (הסתברות)

2. **איכות הבקרות** אשר הוצבו אל מול הסיכונים

3. **שקלול רמת הסיכון השיורי:**

רמת סיכון ביחידה או בתהליך

X

איכות הבקרות

=

**סיכון שיורי**

**שלבי העבודה הלכה למעשה**

# שלב א'

- מיפוי הפעילות
- הגדרת היחידות ותהליכים המהותיים
- קביעת סדר עדיפות

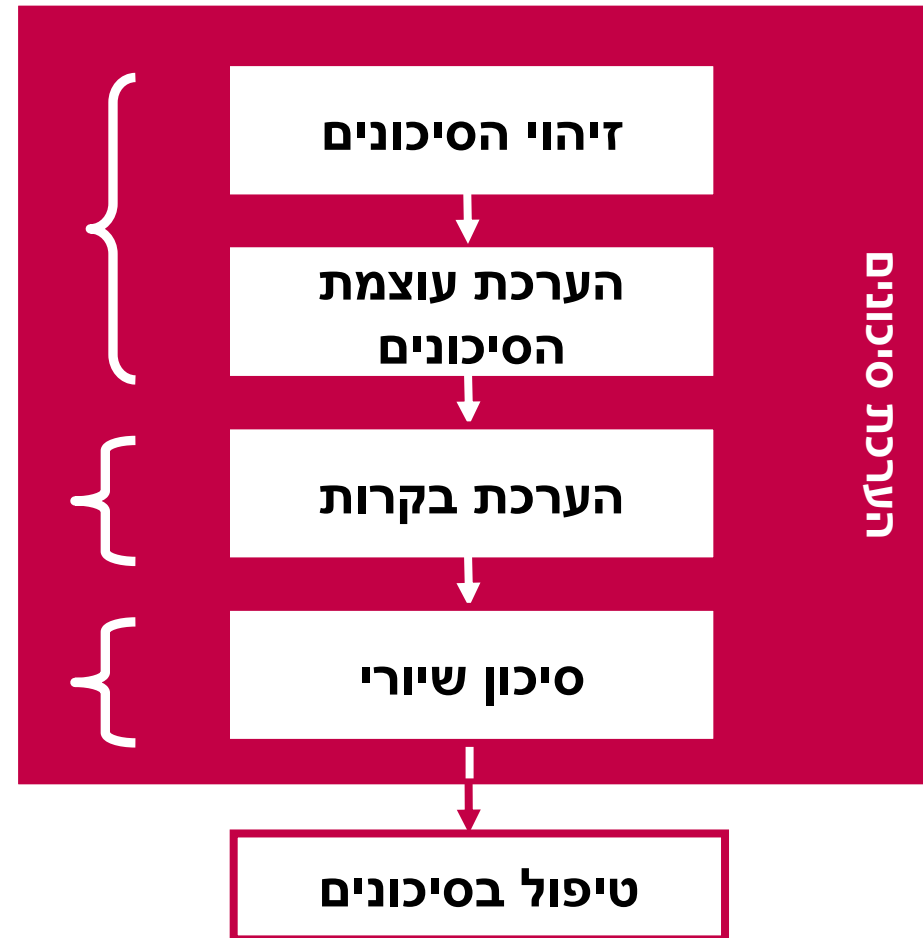


# איסוף המידע

- סקר סיכונים של המבקר הפנימי
- סקר סיכוני מעילות
- סקר סיכוני IT
- תיעוד ב- SOX

- SOX Testing ב- SOX
- דוחות ביקורת של מבקר הפנים

- השלמות



# זיהוי והערכת עוצמת הסיכונים בתהליך השכר

## סקר סיכונים של המבקר הפנימי

- תנאי השכר של עובד שהוקלדו למערכת השכר כוללים נתונים שגויים, כתוצאה מהעלאת שכר בלתי מאושרת
- החברה שילמה לעובדים בגין ימי היעדרות בשל שירות מילואים, אך לא גבתה כסף מהמוסד לביטוח לאומי

## סקר סיכוני מעילות

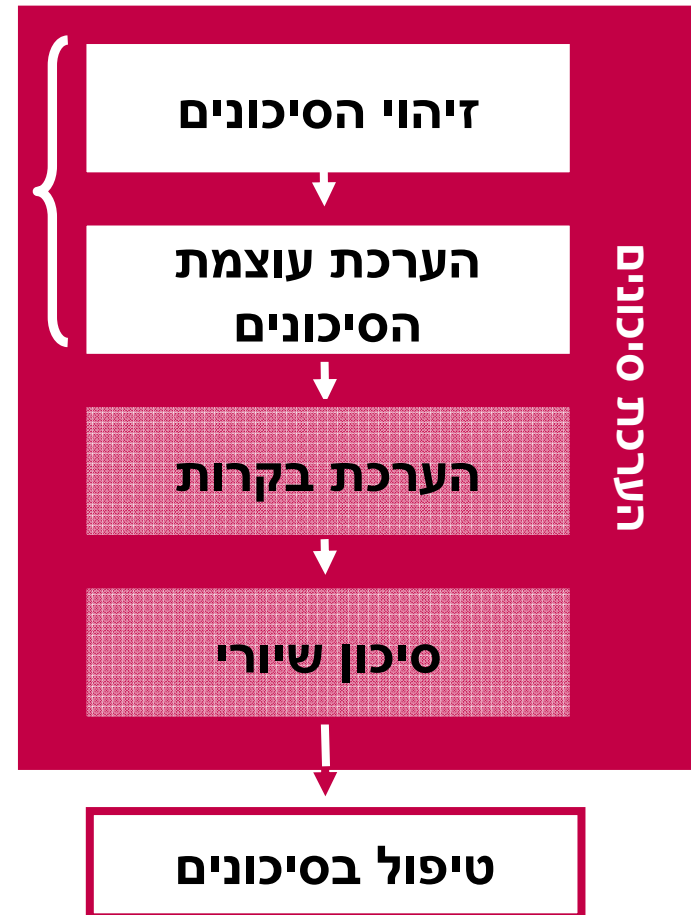
- תשלום שכר לעובד פיקטיבי
- ניצול פרצה במערכת המחשב להעלאת שכר לא מורשית לעובד

## סקר סיכוני IT

- קבצי אקסל בהם נערכו חישובים והזנות בגין רכיבי שכר מיוחדים לא נקלטו בשלמותם במערכת השכר
- לא בוטלו הרשאות במערכות לעובדים שעזבו

## סיכונים שעלו במסגרת שלב התיעוד ב-SOX

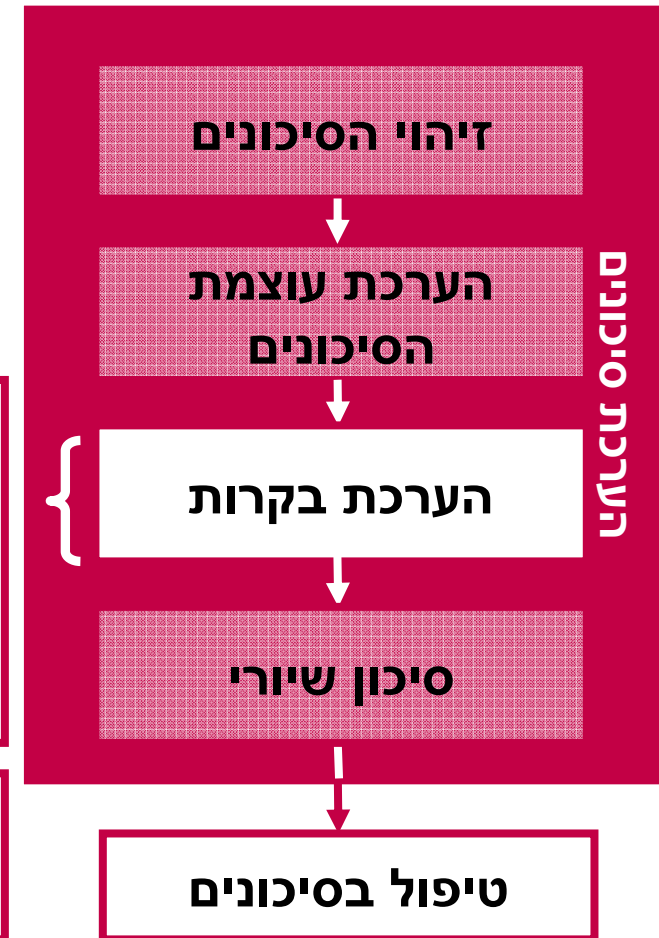
- פקודת השכר שגוייה. הסכום נטו לתשלום, כפי שמופיע במערכת השכר, שונה מהסכום שנשלח למס"ב לצורך ביצוע התשלום



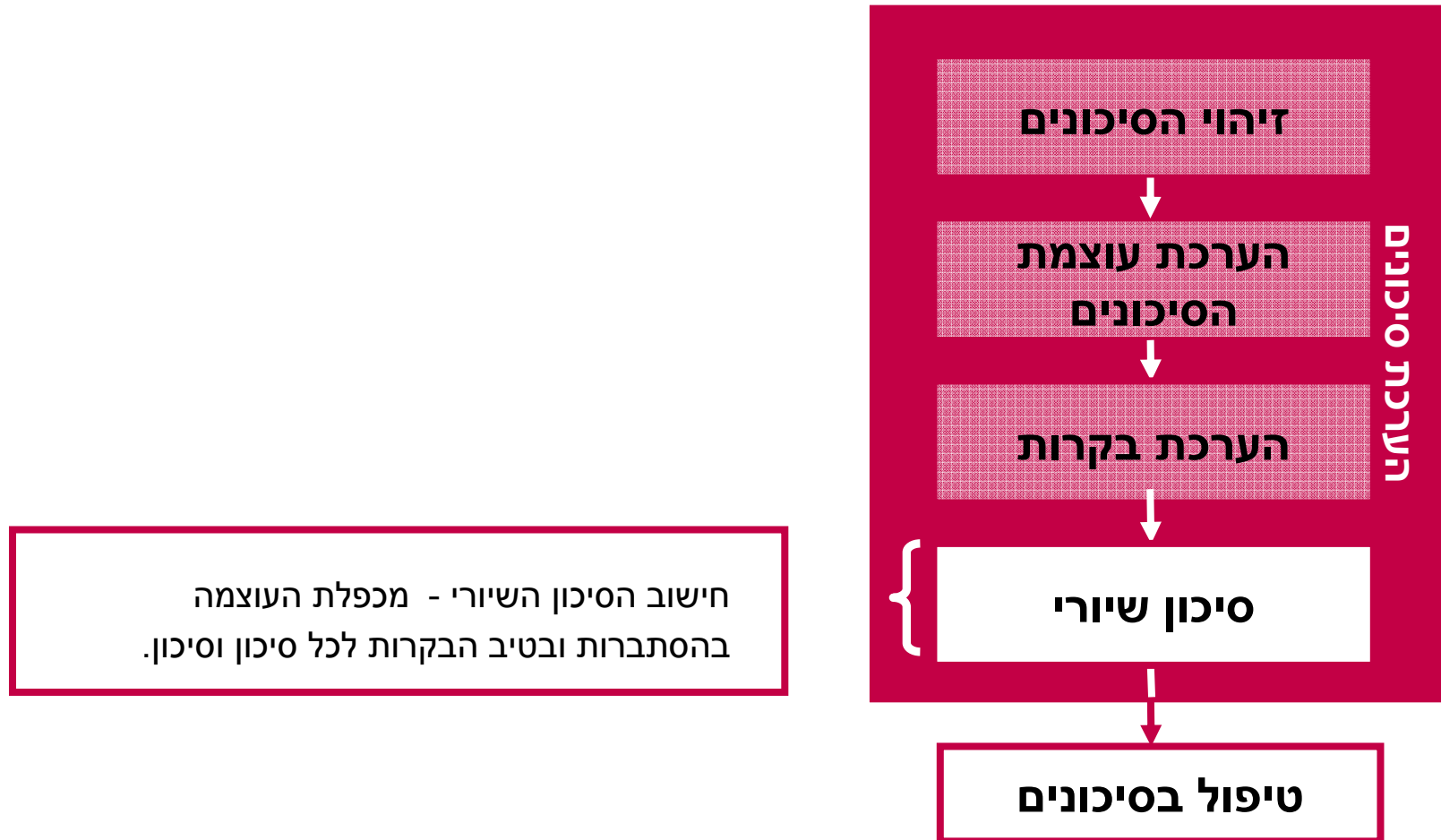
# הערכת הבקורות בתהליך השכר

- דוחות ביקורת של המבקר הפנימי**
- מצאנו כי לא קיים חוזה העסקה לאחד העובדים של החברה.
  - מצאנו כי חוזה העסקה עם העובדים חתום על ידי מורשה חתימה אחד מטעם החברה, למרות שעל פי פרוטוקול מורשי החתימה של החברה דרושות שתי חתימות.
  - בדקנו את נאותות ביצוע עדכוני שכר של העובדים, ומצאנו מקרים בהם לא היה תיעוד לאישור.

- SOX Testing - ב-SOX**
- הסכום נטו לתשלום, כפי שמופיע במערכת השכר, נמצא זהה לסכום שנשלח למס"ב לצורך ביצוע התשלום



# סיכון שיורי בתהליך השכר



# השלמות לצורך הערכת הסיכונים בתהליך השכר

זיהוי סיכונים שלא הופיעו באף אחד מסקרי הסיכונים והערכתם

בחינת תקפות בקרות שלא נבדקו

זיהוי הסיכונים שהחברה מעוניינת לנטרל, הגדרת הטיפול הנדרש בהם והעברת האחריות לטיפול למנהל בכיר

זיהוי הסיכונים

הערכת עוצמת הסיכונים

הערכת בקרות

סיכון שיורי

טיפול בסיכונים

הערכת סיכונים

# תודה על ההקשבה

