נספח א'- גישת העבודה בביצוע סקרי סיכונים

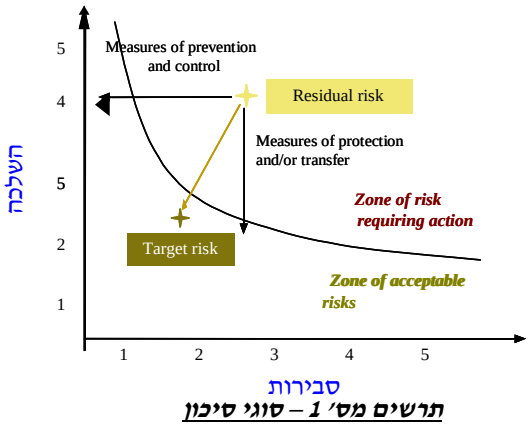
תמצית מתודולוגית סקר הסיכונים

כללי

כל ארגון כיום מתמודד עם אי-ודאויות אשר חושפות את הפעילות לסיכונים העלולים לפגום בפעילות העסקית השוטפת או לחילופין לחוסר ניצול של הזדמנויות עסקיות. מטרת תהליך סקר סיכונים כולל הנה מיפוי כלל החשיפות של הארגון והיכולת לנהל באופן יעיל את חוסר הודאות העסקית והתפעולית.

מתודולוגיות סקר הסיכונים, המוצגת להלן, עוצבה על בסיס סטנדארטיים בינלאומיים, כגון גישת ה COSO ונועדה לייעל את תהליך תכנון עבודת הביקורת הפנימית. מטרתו של תהליך סקר סיכונים הינו לבחון את רמות הסיכון של הפעילויות השונות בארגון באופן המאפשר יצירת מדרג לסיווג היחידות והנושאים השונים אשר יש לבקרם במהלך תכניות הביקורת הרב שנתיות. תיעדוף זה בא למנוע החלטה שרירותית של הארגון בכלל וביקורת הפנים בפרט לגבי סדר העדיפויות בתכנית הביקורת, כלומר באילו נושאים תתבצע ביקורת בשנת העבודה הקרובה ובאילו תתבצע ביקורת בעוד שנתיים, שלוש או ארבע שנים.

עפ"י סקר הסיכונים יהיה ניתן להגיע למיפוי כלל הסיכונים בארגון, כימות השלכתם ותכנון השקעת המשאבים לבדיקתם . מתודולוגית סקר הסיכונים המוצגת במסמך זה מנצלת את מירב הידע הקיים בתוך הארגון ושילוב של ידע חיצוני על ארגונים דומים והכול בכדי לקבל תוצאה סופית מדויקת ככל שניתן. מקורות הידע הם מגוונים כגון המנהלים והעובדים ביחידות השונות, נציגים מהביקורת הפנימית, מערכות המידע השונות ומסמכים רלוונטיים. בנוסף נבחנים מדדי השוואה על ארגונים דומים בארץ ובעולם. בדרך של שילוב כל מקורות המידע ניתן יהיה לספק מיפוי שלם על מצב ועוצמת הסיכונים.



תרשים מס' 1 – סוגי סיכון

סקר סיכונים כולל מאפשר להנהלת הארגון להגדיר את רמת הסיכון המובנה מעצם פעילותו השוטפת (**סיכון שורשי** – **inherent risk**), רמת הסיכון לה הוא חשוף כיום (**סיכון שיורי** **residual risk**) ואת רמת הסיכון לה הוא שואף להגיע (**סיכון מטרה** – **target risk**).

הגדרת סיכון

הגדרתו של סיכון משתנה לעיתים לפי הגישות השונות והמטרות השונות של תהליך ניהול הסיכונים. ההגדרה המילונאית של סיכון הינה "... החשש או האפשרות לאירוע אשר עלול לגרום לנזק או הפסד". בהגדרה זו באים לידי ביטוי הפרמטרים של האפשרות להתרחשות אירוע מסוים והנזק הפוטנציאלי הגלום באירוע זה.

בהגדרה העסקית של סיכון מתווספת גם הראיה של אי ההשגה של היעדים העסקיים ולכן ההגדרה הינה "... האפשרות להתרחשות אירוע כלשהו העלול לגרום לאי השגתם של היעדים העסקיים".

על פי הגדרה זו, יש לבצע בתחילת התהליך הגדרה של היעדים העסקיים ובהתאם לכך ניתן לאתר את המקומות בהן ישנה חשיפה לנזק בהתאם ליעדים שזוהו.

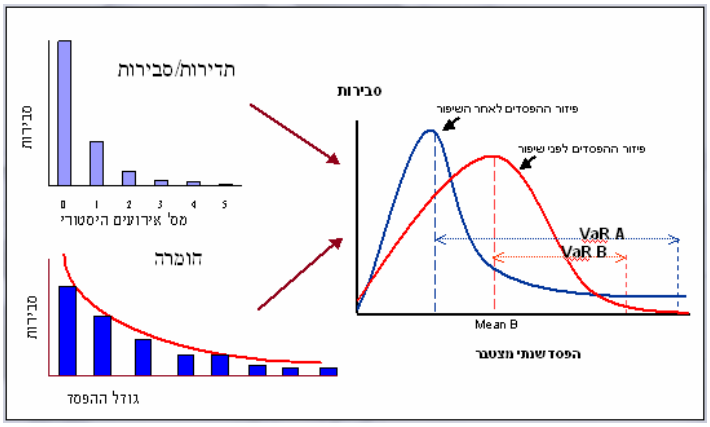
בסקר הסיכונים, הפרמטר של אי השגת היעדים העסקיים בא לידי ביטוי בד"כ במדידת מרכיב ההשלכה של הסיכון על פעילות הארגון, משמע בדרך של אובדן כספי ישיר כתוצאה מהוצאה לא מתוכננת או אובדן הכנסה או בדרך של אובדן כספי עקיף כתוצאה מפגיעה במוניטין, פגיעה בלקוחות, תביעה משפטית וכדומה.

מהו סיכון

סיכון הינו שילוב של מספר מרכיבים אשר יחדיו עלולים לגרום לתוצאה שהיא נזק כלכלי ישיר או עקיף לארגון. מצב מסוים או אירוע כלשהו נוצר כתוצאה משילוב של מספר גורמים פנימיים (תהליכי עבודה, מערכות מידע, עובדים וכדומה) או חיצוניים (קשורים לסביבת העבודה שבה פועל הארגון כגון שינוי כלכלי של השוק, שינוי סביבתי).

מרכיבי הסיכון:

- **גורם הסיכון** – מקור הסיכון (פנימי או חיצוני) - הגורמים השונים המעורבים בפעילות העסקית.
- **אירוע הסיכון** - תרחשי הסיכון בנקודת זמן מסוימת.
- **השלכת הסיכון** – הנזק הפוטנציאלי לארגון כתוצאה מהתממשות סיכון.



תרשים מס' 2 – כימות הסיכון

סיווג סיכונים

בהערכה וכימות של הסיכונים השונים ישנו שקלול של שני מרכיבים עיקריים: **מדד הסבירות ומדד ההשלכה.**

מדד הסבירות - מדד הסבירות מייצג את הסבירות והתדירות

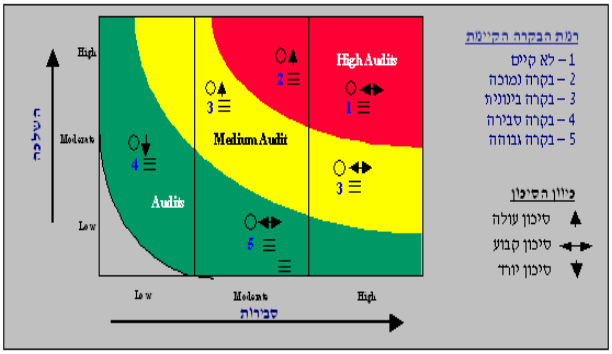
להתרחשותו של אירוע העלול להוביל לנזק לארגון. מדד זה נבחן ע"י שילוב של קטגוריות שונות אשר אי שלמות בקיומן, עלולה לגרום להתרחשותו של סיכון. למשל, בקטגורית משאבי אנוש נבחנים נושאים כגון רמת הכשרתם וכשירותם של העובדים לבצע את פעילותם השוטפת. במידה של חוסר כשירות העובד, ישנו חשש כי עלולות להתבצע טעויות בפעילות השוטפת ו/או חוסר היכולת לספק תמיכה ולשמור על רמת בקרה שלמה בתהליכים. רמת הציון בקטגוריות השונות נמדד ע"י שקלול של ציונים, בין 1 (נמוך) ל 5 (גבוה). ציונים אלה נאספים בסקר שנערך למנהלים ועובדים מהיחידות השונות אשר להם ידע על הפעילויות הנסקרות.

מדד ההשלכה - מדד זה מייצג את פוטנציאל הנזק העלול להיגרם לחברה במידה ויתממש סיכון כלשהו. מדד זה נמדד בפרמטרים של כסף וזמן. מדד ההשלכה הנו מדד המייצג את החשיפה של הארגון מהיבט של מידע, היקף כספי, התאמה לחוק, שביעות רצון הלקוחות, מורל ופעילות העובדים ועוד. באמצעות שאלון ההשלכה ניתן לדרג את רמת הקריטיות של הנושא המטופל. לכימות ההשלכה ישנם מספר מרכיבים:

- **היקף כספי פוטנציאלי** – היקף הכסף אשר מנוהל בנושא הנבדק.
- **השפעה מסחרית על החברה** – אובדן לקוחות ופגיעה ביכולת התחרותיות של החברה.
- **השפעה על מוניטין החברה** – הנזק התדמיתי אשר עלול להיגרם לחברה ומנהליה.
- **השפעה רגולטורית** – הסיכון לאי עמידה בהוראות חוק.
- **חשיפה חשבונאית** – הסיכון לטעויות דיווח בדוחות הכספיים.
- **משאבי אנוש**- השפעה על מוטיבציית העובדים ואמינות החברה בעיני העובדים.

בניית תכנית עבודה

בהתאם לתוצאות סקר הסיכונים ולדוח המפורט נחל בבנית תכנית העבודה הרב שנתית. לתכנית זו יתווספו גם שיקולי המבוקר כגון ציפיות המבוקר. תכנית העבודה תבנה על בסיס הפרמטרים: עוצמת הסיכון (שילב של סבירות והשלכה), רמת הבקרה, כיוון הסיכון.



תרשים מס' 3 – עיצוב תכנית עבודה

כפי שמוצג בתרשים 5 שלהלן ניתן לראות כי תכנית העבודה כולל שיקולים של: מתי יש לבדוק אותם, ומהם הנושאים המומלצים לבדיקה בכל אחד מהם, סיוג הבדיקות בהתאם לבקרות הקיימות ו/או לסיכונים שאותרו וכמובן בהתאם לנזק הפוטנציאלי (השלכה).

להלן פירוט השלבים העיקריים בביצוע סקרי סיכונים עפ״י מתודולוגית PwC :

1. שלב 1 – הכרת הארגון והייעדים העסקיים + הנעת הפרוייקט

שלב ראשון בפרויקט הינו איסוף מידע ראשוני לצורכי לימוד והבנת הצד המבוקר. במקביל, אנו מבצעים שלב של תכנון מפורט לפרויקט והנעת צוות הפרויקט. בחלק זה יקבעו מטרות ויעדי הפרוייקט באופן מפורט ותקבע תכנית עבודה מפורטת כולל הגדרת אבני דרך, לוחות הזמנים ותוצרים. באופן מפורט יבוצעו הפעילויות הבאות :

- קביעת תכנית עבודה מפורטת לפרויקט.
- קביעת לוחות זמנים.
- הגדרת צוות הפרויקט ונציגי הפרויקט מטעם כנף.
- קביעת התוצרים ותוצרי הביניים.
- הגדרת הסיכונים לפרויקט ואת רמת מעורבות נציגי כנף בפרויקט.
- פגישת פתיחה עם צוות הפרויקט ונציגי כנף להתנעת הפרויקט והצגת גישת העבודה.

2. שלב 2 – מיפוי תהליכים ויחידות עסקיות

המידע בנאסף בשלב 1 משתמש לצורך הגדרת עולם הביקורת(Audit Universe). עולם הביקורת מורכב הן מיחידות ארגוניות, תהליכים, מערכות מידע ונושאים חוצי ארגון. כל נושא שכזה ממופה לאחר מכן בתהליך סקר הסיכונים לדרגת החשיפה והסיכון בנושא זה כדי לאפשר לביקורת הפנימית לקבוע את תכנית העבודה השנתית והרב שנתית בהתאם לנושאים אלו. יש לציין כי לעיתים, במהלך הסקר עצמו, מתווספים נושאים נוספים לעולם הביקורת כישות ביקורת ואשר לא נכללו בשלב המקדים. נושאים אלו בד״כ עולים כנושאים חוצי ארגון אשר עלו כגורם סיכון נוסף.

כאמור, בהתאם לחלוקה זו מתבצע סקר הסיכונים ונקבע דירוג תדירות הביקורת.

בשלב זה אנו מבצעים את הפעילויות הבאות :

- מיפוי נכסים ארגוניים אשר כוללים :
  - יחידות הארגוניות
  - תהליכים
  - מיפוי מערכות המידע התומכות
  - נושאים חוצי ארגון
- הערכה ודירוג של נכסים אלו לפי רמת הקריטיות של כל נושא (בד״כ רמת הקריטיות והמהותיות נקבעת על בסיס פרמטרים של ההשפעה על פעילות הארגון ז״א היקף כספי,

מימד זמן וכדומה). דירוג המהותיות מאפשר הפעלה של שיקולי עלות תועלת בהמשך הפרויקט ובניתוח הסיכונים ובניית תכנית העבודה.

3. שלב 3 – ביצוע סקר הסיכונים

בשלב זה מתבצע תהליך סקר הסיכונים ומיפוי החשיפות בנושאים השונים בכנף על בסיס הישויות אשר נקבעו בשלב הקודם. סקר הסיכונים הינו תהליך של סקירת מוקדי הסיכון, נקודות החשיפה ופוטנציאל הנזק אשר עלול להתרחש.

4. שלב 4 – ניתוח הממצאים וכימות הסיכונים

בתום השלבים הקודמים אנו נחל בשלב של ניתוח הממצאים והכנת מפת הסיכונים הכוללת את הערכת עוצמת הסיכון. הערכת הסיכונים נעשית על בסיס שני מדדים עיקריים: מדד **הסבירות** ומדד **ההשלכה**.

מדד הסבירות מייצג את האפשרות להתרחשות אירוע כלשהו ו/או התדירות של אירועים אלו, מדד ההשלכה מייצג את הנזק הפוטנציאלי לארגון בהיבט של מידע, כספים, התאמה לחוק, לקוחות, עובדים וכדומה. בכדי שנוכל לאמוד את האפשרות של אירוע מסוים להתרחשותו ואת השלכתו על העסק אנו מבצעים תהליך של ניתוח המידע הקיים בארגון ומחוצה לו ובוחנים את מצב הנכסים השונים בכל נקודת זמן. אמור, בהגדרת הנכסים נכללים גם: תהליכים, פעילויות שונות, משאבי כ"א, משאבי מחשב, נכסי מידע, אתרים שונים, מוניטין וכדומה. כימות הסיכונים והחשיפות מתבצע על בסיס שקלול של מדדים ומשקלות המתקבלים מהראיונות והשאלונים השונים יחד עם השוואה אל מול מאגרי מידע הבוחנים את התדירות והכמות הסטטיסטית של אירועים שקרו בעבר.

5. שלב 5 – הכנת דוח מסכם, מתן המלצות ובניית מודל לוגי ממוכן

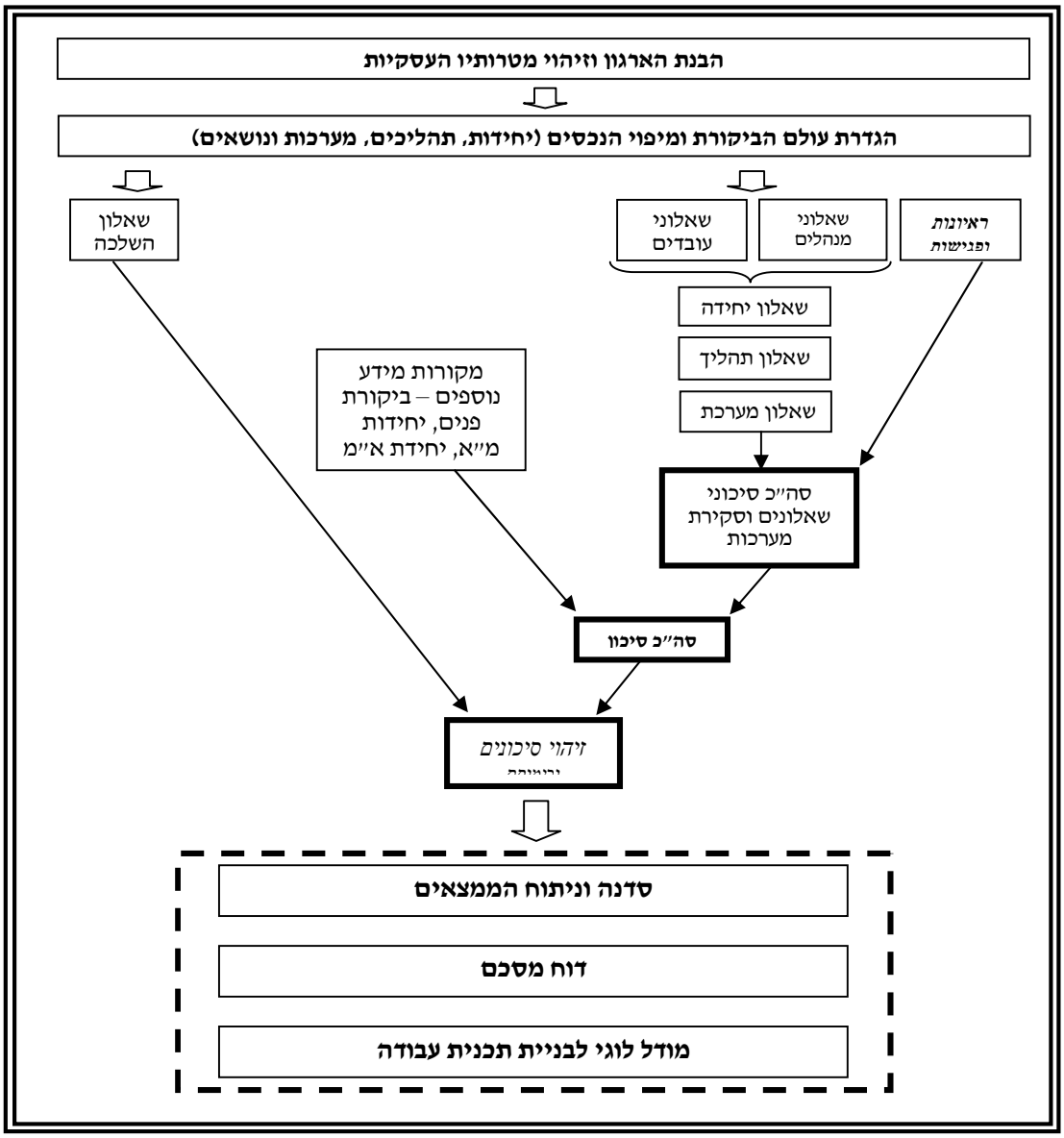
הדוח יורכב משני חלקים עיקריים:

(1) תמצית המנהלים אשר תכיל את תרשים מפת הסיכונים וטבלא מרכזת של הממצאים (הסיכונים) אשר הוגדרו ברמת חומרה גבוהה.

(2) החלק השני יהיה דוח מפורט אשר יכיל פירוט של כל הממצאים יחד עם הצגת היחידה או התהליך המבוקר, פירוט והסבר על הממצא, פירוט של דירוג הסיכון ופירוט על המלצתינו לפתרון.

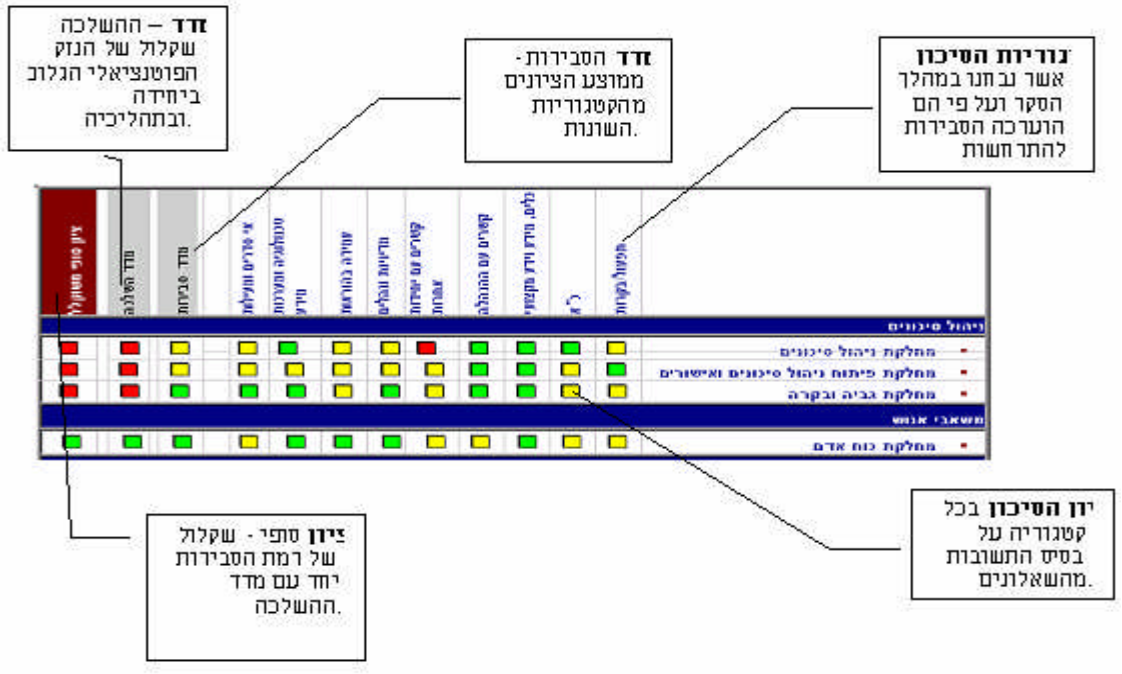
על בסיס הבנת מפת הסיכונים של כנף תוכל הביקורת הפנימית לבנות תוכנית עבודה רב שנתית לביקורת פנים הכוללת את היישויות שייבדקו, מתי יש לבדוק אותן, ומהם הנושאים המומלצים לבדיקה בכל אחד מהם.

כחלק מתוצרי הפרויקט נספק לביקורת הפנימית בכנף את המודל של הערכת הסיכון ובניית תכנית העבודה. מודל זה יהיה על בסיס אקסלים ויאפשר לנציגי כנף לתחזק את סקר הסיכונים בהמשך ולעצב את תכנית העבודה של הביקורת הפנימית.



נספח ב' – דוגמת תוצרים

תמצית סיכונים – Heat-Map



תרשים מס' 9 תרשים Heat-Map – מקרא והסברים –

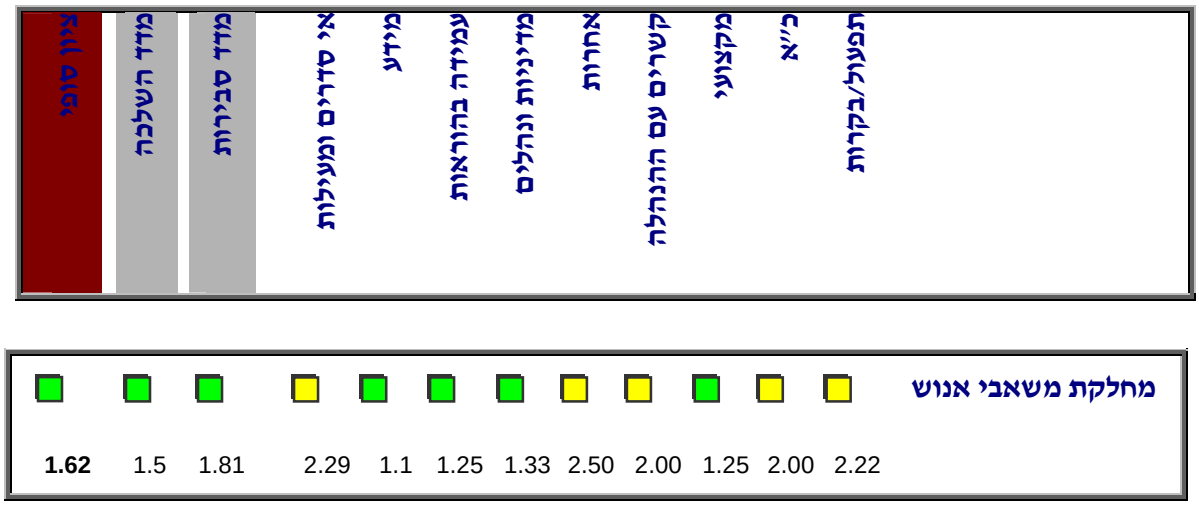
		מכפיל הסיכון	ציון סופי	חדד	ציון סתפי										
				60%	40%										
משאבי אנוש															
	א'	2.7	1.62	1.50	1.81	2.29	1.44	1.25	1.33	2.50	2.00	1.25	2.00	2.22
חטיבה מערכות מידע															
	א'	10.5	3.45	4.00	2.62	2.29	3.44	2.75	3.00	3.00	1.67	1.75	3.13	2.56
	ב'	7.3	2.88	3.33	2.20	3.00	1.89	2.68	2.67	3.00	1.50	1.25	2.00	1.83
	ג'	8.4	3.01	3.33	2.53	2.43	2.67	3.33	2.33	3.00	2.33	1.50	2.97	2.22
חטיבה א'															
	א'	3.2	1.78	1.67	1.94	2.43	1.22	2.08	1.67	2.00	1.50	1.63	3.13	1.83
	ב'	5.0	2.19	2.00	2.48	3.25	1.89	2.67	2.83	3.00	1.50	1.88	2.10	3.17
	ג'	2.5	1.55	1.33	1.86	1.67	1.44	1.88	1.83	3.00	1.50	1.25	2.25	1.94
חטיבה ב'															
	א'	7.5	2.73	2.67	2.83	2.29	2.89	3.17	2.67	4.00	2.67	1.88	3.53	2.39
	ב'	7.4	2.70	2.67	2.76	3.29	2.89	2.58	3.33	3.50	2.17	2.13	2.40	2.56
	ג'	5.7	2.45	2.67	2.13	2.29	1.44	2.67	2.00	3.00	1.83	1.50	2.33	2.11
אגף כספים															
	א'	4.3	2.14	2.33	1.85	1.80	1.22	2.71	1.77	3.00	1.58	1.25	1.45	1.89
	ב'	5.4	2.41	2.67	2.03	2.29	2.11	2.29	2.17	3.00	1.25	1.25	1.77	2.11
כללי		6.2	2.57	2.80	2.21	2.50	1.88	2.51	2.27	2.96	1.73	1.54	2.28	2.22

	MAX	AVG	MIN
	4.11	2.41	1.33
Var -		0.48	

	MAX	AVG	MIN
	5.00	2.54	1.00
Var -		0.96	

	MAX	AVG	MIN
	4.00	2.23	1.00
Var -		0.49	

דוגמת תיאור מפורט של הסיכונים ביחידה מסוימת



דירוג סיכון במשאבי אנוש

- **סבירות** – סבירות בינונית (1.81) מתוקף רמת הבקרות בקטגוריות הסיכון השונות.
- **השלכה** – השלכה בינונית (1.50) מתוקף הנזק הפוטנציאלי הגלום בפעילות של המחלקה.

- **שקלול ציון סופי -** המחלקה מדורגת בסיכון בינוני (1.62) הנובע משקלול של דירוג בינוני בהשלכה הצפויה מנזק פוטנציאלי ודירוג בינוני בציון הסבירות להתרחשותם.

סקירת פעילות היחידה

מחלקת משאבי אנוש מדווחת ישירות לXXX. המחלקה עוסקת בחמישה תהליכים עיקריים:

- גיוס עובדים.
- הדרכת עובדים.
- פיתוח והכשרת עובדים.
- קידום וניוד עובדים.
- טיפוח ורווחת הפרט.
- פיטורי עובדים.

סיכונים עיקריים בתהליכי העבודה

- **גיוס עובדים אשר יהוו סיכון מבחינת אמינות ויושר -** חרף כל הבקרות הקיימות בתחומי הפעילות של החברה ניתן לצפות שעובדים יצליחו להתגבר ולעקוף את הבקרות אם ירצו בכך ויתאמצו. נתגלו אירועים של הוצאת מידע שלא כדין, וסביר

שאירועים נוספים כלל לא נחשפו. כמו-כן, קיים חשש לגניבות כסף ורכוש. האמצעים שננקטו להתמודדות עם סיכון זה כוללים – (1) נתקבלה החלטה שכל עובד יעבור מבדק אמינות עם קבלתו לעבודה ; (2) עובדים חדשים מוחתמים על הצהרות סודיות והסכמה לבדיקת פוליגרף אקראית או תקופתית; (3) ביצוע בדיקת רענון בעת שינוי מעמד/תפקיד, כאשר התפקיד החדש הוא בתחום שהוגדר כבעל רמת סיכון גבוהה יותר ; (4) הוגברה מודעות מנהלים.

- גיוס עובדים אשר לא יתאימו לפעילות המקצועית של החברה.
- הדרכת עובדים שלא משיגה את יעדיה.
- אי שביעות רצון עובד מתגמול/טיפוח.
- תחלופה גבוהה וחוסר נאמנות.