

ניהול סיכוני סייבר



מה זה סיכון?

הגדרה המילונאית של סיכון:

“חשש או אפשרות לאירוע אשר עלול לגרום לנזק או להפסד”

במקרה של המשרד להגנת הסביבה ההתמקדות היא בסיכונים הבאים:

- ❑ פגיעה ברצפטור הציבורי
- ❑ פגיעה / נזק לאיכות הסביבה בישראל

על-סמך הגדרה זו, יש לאתר את המקומות שבהם ישנה חשיפה לנזקים כפי שהוגדרו בתחום הרגולציה של המשרד



מושגי יסוד בניהול סיכונים

Risk Management BASICS



✓ **גורם סיכון (HAZARD)** – משהו שיכול לגרום נזק. (למשל מיכל אמוניה...)

✓ **סיכון (RISK)** – הפעלת גורם הסיכון (למשל העלאת הלחץ במיכל לערכים מסוכנים)

✓ **רמת ההסתברות** להתממשות הסיכון. למשל רעידת אדמה: הנזק גדול, ההסתברות נמוכה
התקפת סייבר : נזק גדול והסתברות יותר גבוהה

✓ **התוצאה עקב התממשות הסיכון**

למשל הזרמת כמויות גדולות של חומ"ס אל הסביבה, מהו הנזק הסביבתי?!

קבוצות סיכונים

סיכונים אסטרטגיים



- פגיעה בתדמית
- פגיעה בלקוחות
- מתחרים
- פיתוח מוצרים

סיכונים פיננסיים



- תזרים מזומנים
- סיכוני אשראי
- סיכוני שער חליפין
- סיכוני ריבית והצמדה
- סיכוני מחיר נירות ערך

קבוצות סיכונים

סיכונים תפעוליים



- תפקוד לקוי של עובדים
- ליקוי במערכות מידע
- ליקוי בתהליכים אחרים בחברה
- **אירוע חומ"ס**

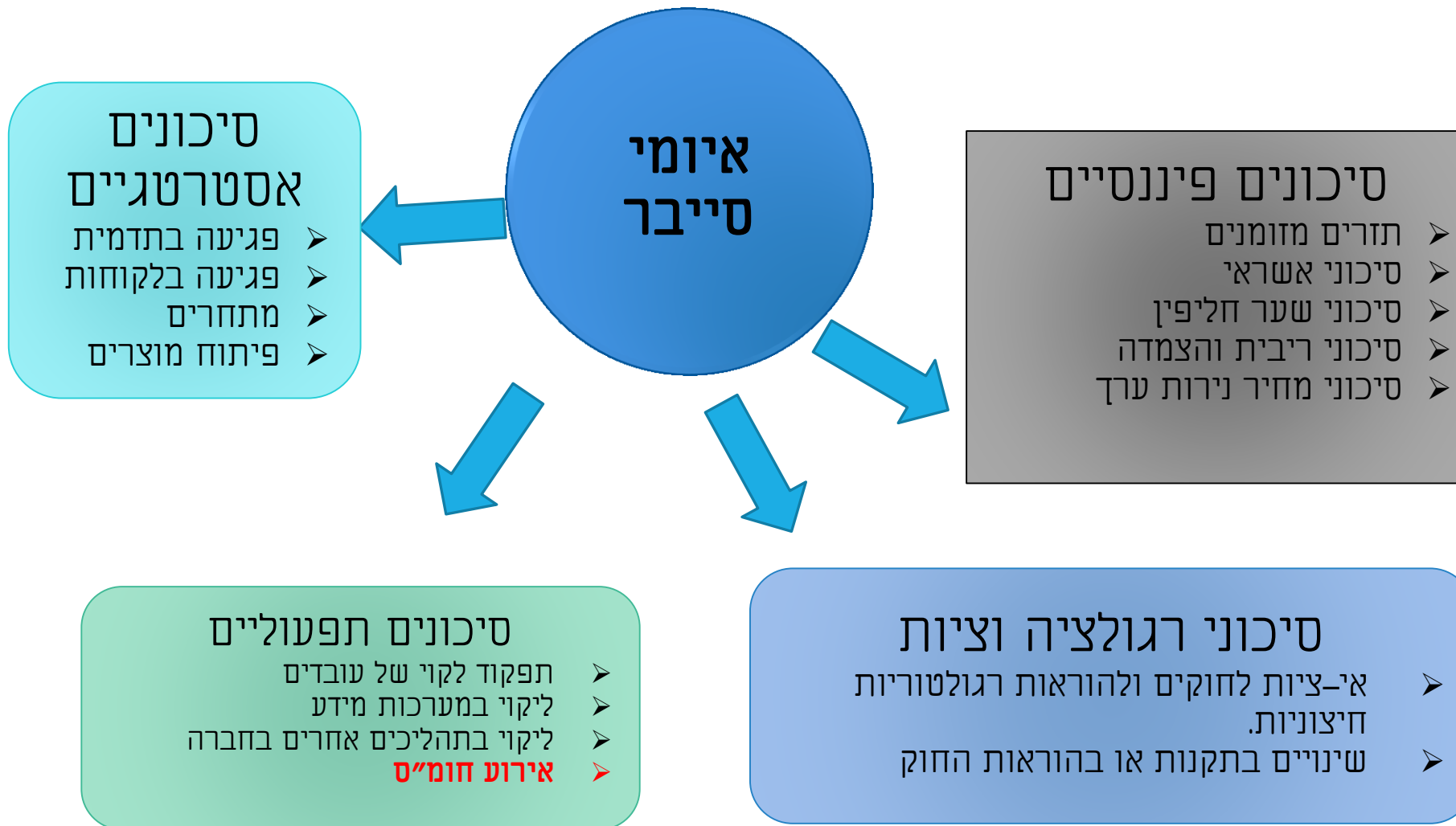
סיכונים רגולציה וציות

- אי ציות לחוקים ולהוראות רגולטוריות חיצוניות
- שינויים בתקנות או בהוראות חוק

חוק
חומרים
מסוכנים



סיכוני אבטחת מידע - הטריגר



Facts on Amazon



Amazon Company Overview	Values	Statistic
Net sales of Amazon in 2016	136bn USD	Details →
Net income of Amazon in 2016	2.371bn USD	Details →
Number of Amzon.com employees as in 2016	341,400	Details →
Biggest revenue segment of Amazon in 2016	Retail products	Details →
Year-over-year revenue growth of Amazon as of 2016	27%	Details →
Amazon's outbound shipping costs in 2016	16.2bn USD	Details →
Amazon's fulfillment expenses in 2016	17.6bn USD	Details →

Benchmark	Values	Statistic
Most popular online store in the United States in 2016	Amazon	Details →
Amazon's brand value in 2016	98.99bn USD	Details →
Unique monthly U.S. visitors to Amazon sites as of November 2016	184m	Details →
Share of direct traffic to Amazon.com as of April 2017	41.47%	Details →

אתר המכירות AMAZON

אתר מושבת



הפסד רווח ליום:
 $2.37B / 365 = 6.5M$

הפסד לשעה:
 $\$270,000$

הפסד לדקה: **$\$4500$**

שלב טרום – מיפוי נכסים



השאלות המרכזיות

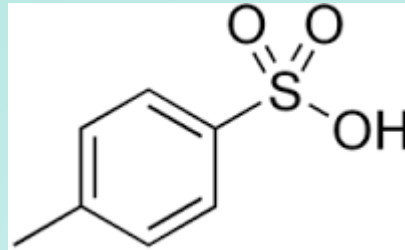
- על מה אנחנו רוצים להגן?
- על מה לבצע ניהול סיכונים?

יש לבצע מיפוי על:

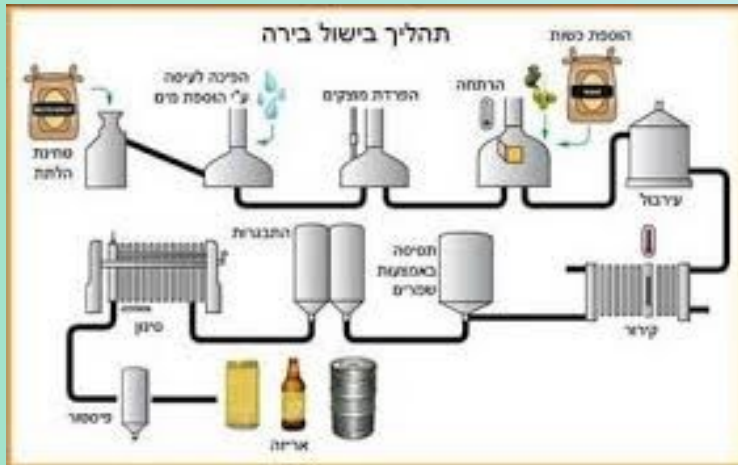
1. נכסים קריטיים
2. תהליכים קריטיים

במפעל חומרים מסוכנים: "תהליך מסוכן"

דוגמא לנכסים קריטיים בארגון



❖ **נוסחת** ייצור קוקה קולה



❖ **תהליך** ייצור בירה

דוגמא לנכסים קריטיים במפעל חומ"ס



❖ תהליך קירור באמוניה

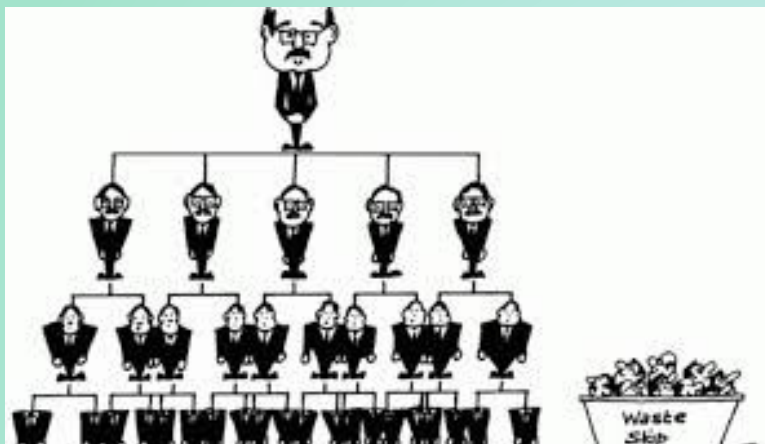
❖ תהליך עיקור ציוד רפואי

❖ תהליך ייצור תרופות

❖ תהליך ייצור חומר מסוכן (דשנים, חומרי ניקוי, חומרי הדברה)

❖ תהליך טיפול בשפכים, או טיפול במי התפלה

איך לבצע מיפוי נכסים



TOP DOWN



BOTTOM UP

מה עדיף?

TOP-DOWN

BOTTOM-UP

יתרונות	<ul style="list-style-type: none">• Starts with the needs of the organization• Provides a "big picture" to the customer and the designer	<ul style="list-style-type: none">• Quick• Leverages previous experience
חסרונות	<ul style="list-style-type: none">• Time consuming	<ul style="list-style-type: none">• Might miss some organizational requirements• High probability of failure

ניהול הסיכונים





1. דחיית הסיכון

2. קבלת הסיכון

3. מזעור הסיכון

4. העברת הסיכון לצד ג'

1. דחיית הסיכון

דחיית סיכון = ביטול הפרויקט



דוגמא מהחיים:

הימנעות מרכיבה על אופנוע
הימנעות מעישון

דוגמא מעולם הסייבר:

ארגון לא מאפשר לעובדיו גישה לאינטרנט
ארגון לא מאפשר גישה מרחוק אל הארגון

בעולם החומרים המסוכנים

מפעל מפסיק לעבוד עם אמוניה לצורך קרור ומיישם קירור בצורות אחרות (אתילן גליקול)

2. קבלת הסיכון

מודעים לסיכון ומקבלים אותו

סיבות:

עלות תועלת

הסיכוי להתממשות נמוך

דוגמא מהחיים:

שותים ונוהגים בתקווה שלא נתפס ולא נעשה תאונה במידה והסיכוי לתאונה יתממש, נקבל את הסיכון במלא עוצמתו

דוגמא מעולם אבטחת המידע

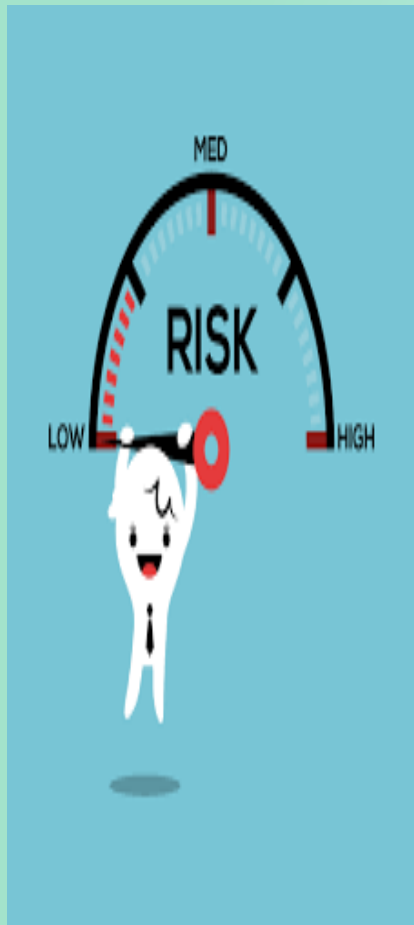
תיתכן החלטה בארגון גדול שלא מתקינים אנטי-וירוס במחשבים במידה ויגיע וירוס – הוא יכנס בוודאות לארגון השאלה כמה נזק יגרום.

בעולם החומרים המסוכנים

לא נוכל להרשות לעצמינו את קבלת הסיכון – מדובר בחיי אדם ופגיעה חמורה בסביבה – יציאה משליטה של המפעל.



**הנחת יסוד:
לא ניתן לבטל סיכון אלא למזער עד לסיכון שיוורי**



הסיכון	מזעור הסיכון	האם מבטל ללא סיכון??
וירוסים	התקנת אנטי-וירוס	לא
חדירה לאפליקציה	התקנת מוצר הגנה אפליקטיבית	לא
דליפת מידע חיוני לארגון	התקנת מוצר המונע דלף מידע	לא
פריצה פיסיית	מצלמות, מאבטחים	לא
		הנדסה חברתית

4. העברת הסיכון לצד ג' (TRANSFER)



חברת ביטוח

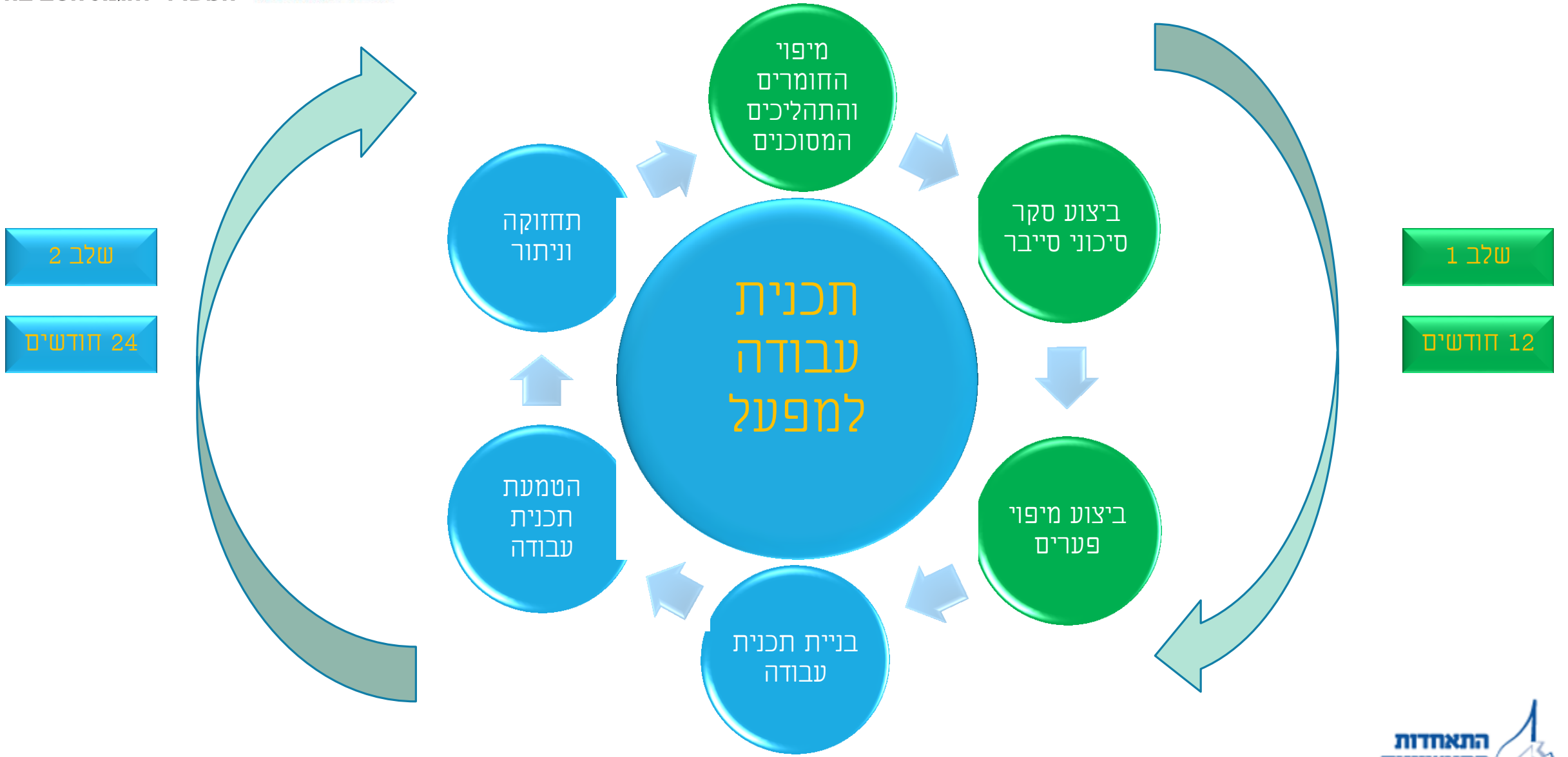
במקרה של התממשות האיום חברת הביטוח תכסה את הנזק

במפעלי חומרים מסוכנים האם ביטוח יכסה חיי אדם??

איך לבצע סקר סיכונים במערכות בקרה תעשייתיות המכילות חומרים מסוכנים ?



תכנית עבודה למפעל לעמידה בדרישות סייבר בהיתר הרעלים



מיפוי חומרים מסוכנים ותהליכים מסוכנים

שלב 1





נספח י"א – כמויות סף לחומרים מסוכנים

רגולציית הסייבר לפי מדריך זה, חלה על מפעלים המחזיקים בחומר מסוכן או בקבוצת חומרים מסוכנים המפורטת/ת בטבלה מטה (להלן: "הטבלה"⁸), בכמות העומדת בטווח שבין הסף התחתון לסף העליון הקבועים בטבלה לחומר המסוכן או לקבוצת החומרים המסוכנים.

מיפוי החומרים ואופן דרכי חישוב כמות החומר או קבוצת החומרים, נעשית בהתאם לרגולציה הגרמנית להגנת הסייבר (SEVESO). אופן חישוב הכמות תלוי בסוג החומר המסוכן ובתוצאותיו של תהליך בדיקה שלבי כמפורט להלן (יובהר כי עמידה בשלב מסוים מביאה להחלה של רגולציה ומייתרת את בדיקת יתר השלבים):

1. כמות של חומר מסוכן שמחזיק המפעל ומופיע בשמו המדעי לצד מספר ה-CAS (הייצוג המספרי הרשמי של החומר) המתאים לו בטבלה, יש לקבוע בהתאם לכמות המותרת להחזקה שנקבעה בהיתר הרעלים שניתן למפעל. ככל שהכמות המותרת להחזקה בהיתר הרעלים עומדת בטווח שבין הסף התחתון לסף העליון שנקבעו לחומר המסוכן בטבלה, הרי שחלה על המפעל, על כל החומרים המסוכנים בו (בין שנכנסו לטווח הספים ובין שלא) רגולציית סייבר.
2. בדיקה לפי קבוצת חומרים מסוכנים: חומרים מסוכנים שאינם מופיעים בשם המדעי בטבלה יש לבחון אם ניתן לקשר לקבוצת חומרים מסוכנים. כדי לבדוק אם חומר מסוכן שייך לקבוצת חומרים מסוכנים לפי הסיווג של הדירקטיבה האירופאית CLP מהמפורטות בטבלה, ניתן לעשות שימוש בגיליון הבטיחות (SDS) או להשתמש במאגרי מידע כדוגמת אתר [GESTIS Substance Database](#) או כל מאגר אחר. ככל שניתן לשייך את החומר לקבוצה של חומרים מסוכנים, יש לבחון האם הכמות המותרת של החומר שנקבעה בהיתר הרעלים שניתן למפעל, עומדת בטווח שבין הסף התחתון לסף העליון שנקבעו לקבוצת החומרים בטבלה. עמידה בטווח משמעה שחלה על המפעל רגולציית הסייבר, על כל החומרים המסוכנים בו (בין שנכנסו לטווח הספים ובין שלא).
3. בדיקה מצרפית לפי קבוצת חומרים מסוכנים: ככל ולא קיימת כמות העומדת בטווח הספים לאף אחד מהחומרים המסוכנים או לקבוצה של חומרים מסוכנים, יש לערוך בדיקה מצרפית של כמויות החומרים המסוכנים בהתאם לנוסחה שלהלן:

$$\frac{Q1}{QU1} + \frac{Q2}{QU2} + \frac{Q3}{QU3} + \dots \geq 1$$

Q_x = כמות החומר המסוכן x או הקטגוריה של חומרים מסוכנים

QU_x = כמות הסף (עליון או תחתון בהתאם הסף הנבחן) לחומר מסוכן x או הקטגוריה של חומרים מסוכנים המפורטים בנספח

מתוך מדריך ניהול סיכונים
אגף חומרים מסוכנים
המשרד להגנת הסביבה

1. מיפוי חומרים מסוכנים
בהתאם לנספח י"א

2.

נספח י"א

מיפוי חומרים מסוכנים

טבלת החומרים המסוכנים הנכללים בביצוע סקר סיכוני סייבר

חומר	מספר CAS \ משפטי סיכון (H) (הערה 0)	סך תחתון כמות השווה או העולה על (טון)	סך עליון כמות השווה או העולה על (טון)
עם תכונות סיכון לבריאות (H), מקטגוריות הסיכון הבאות:			
H1 ACUTE TOXIC - Category 1, all exposure routes	H300, H310, H330	5	20
H2 ACUTE TOXIC - Category 2, all exposure routes - Category 3, inhalation exposure route (הערה 7)	H300, H310, H330 H331	50	200
H3 STOT SPECIFIC TARGET ORGAN TOXICITY – SINGLE EXPOSURE STOT SE Category 1	H370	50	200
עם תכונות סיכון פיזיקאליות (P), מקטגוריות הסיכון הבאות:			
P1a EXPLOSIVES (8 הערה) - Unstable explosives or - Explosives, Division 1.1, 1.2, 1.3, 1.5 or 1.6, or - Substances or mixtures having explosive properties and do not belong to the hazard classes Organic peroxides or Self-reactive substances and mixtures, Type C, D, E or F or organic peroxides, Type C, D, E, or F	H200, H201, H202, H203, H205	10	50
P1b EXPLOSIVES (8 הערה) Explosives, Division 1.4	H204	50	200
P2 FLAMMABLE GASES Flammable gases, Category 1 or 2	H220, H221	10	50
P3a FLAMMABLE AEROSOLS (11.1 הערה) 'Flammable' aerosols Category 1 or 2, containing flammable gases Category 1 or 2 or flammable liquids	H222, H223, H229	150	500

מתוך מדריך ניהול סיכונים
 אגף חומרים מסוכנים
 המשרד להגנת הסביבה

מיפוי תהליכים מסוכנים



תהליך מסוכן אחד מאלו:

א- תהליך בעסק המכיל חומר מסוכן בכמות העולה על 2% מערך הסף התחתון המצוין בנספח י"א למדריך זה, לאותו החומר.

ב- תהליך הממוקם בסמוך לתהליך מסוכן כמוגדר בסעיף א', שתקרית בו עלולה לגרום לאירוע חומרים מסוכנים משמעותי בתהליך המסוכן כמוגדר בסעיף א' ("אפקט דומינו").

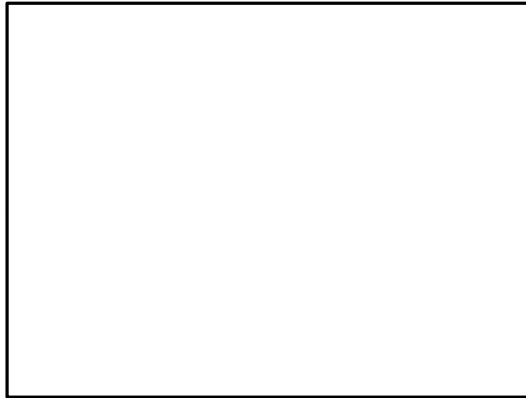
דוגמא 1 :

יש לי במפעל 60 טון אמוניה, מערכת האמוניה מכילה 4 תהליכים:
 תהליך א' : מכיל 30 טון
 תהליך ב' : מכיל 20 טון
 תהליך ג' : מכיל 1 טון
 תהליך ד' מכיל 9 טון
 על איזה תהליכים אבצע סקר סיכונים?

200	50	7664-41-7	Anhydrous Ammonia	.35
20	5	7637-07-2	Boron trifluoride	.36
20	5	7783-06-4	Hydrogen sulphide	.37

מיפוי החומרים המנוהלים / מבוקרים / ע"י מערכות ממוחשבות

דוגמא למערכות ממוחשבות



3.

מיפוי החומרים המנוהלים/מבוקרים
ע"י מערכת ממוחשבת

- עמדות HMI
- בקרים מכל הסוגים
- סנסורים המחוברים בתקשורת ETHERNET
- רכיבי שטח המחוברים בתקשורת ETHERNET
- רכיבי נוספים כלשהם המחוברים בתקשורת ETHERNET



חישוב הנזק המתקבל כתוצאה מאירוע חומרים מסוכנים

שלב 2

הנזק מחושב לפי **WCS** – WORST CASE SCENARIO

נזק = IMPACT יסומן מעתה באות **I**

סוגי נזקים:

○ זיהום הסביבה

○ פגיעה בבריאות הציבור עקב התרחישים הבאים:

• פיזור גזים רעילים – יחושב על פי ערכי PAC

• פוטנציאל לפיצוץ (UVCE) – יחושב על פי ערכי לחץ (הדף) ביחידות BAR

• אפקט דליקה / כדור אש (BLEVE) – יחושב על פי ערכי קרינה יחידות קילוואט למטר רבוע במשך 60 שניות



טבלת חישוב הנזק

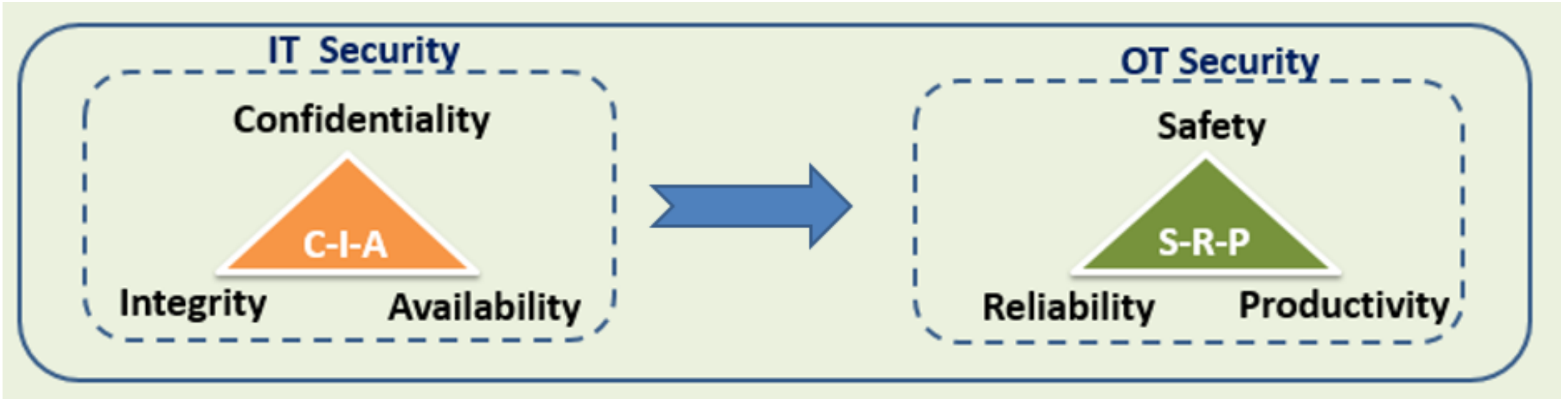
נספח א' במדריך הסייבר לתעשייה

שאלה	1	2	3	4	ציון (1-4)
הנזק מוערך באחד או יותר מהקריטריונים להלן:					
S (Safety)	1. בריאות הציבור: ללא פגיעה ברצפטור ציבורי	1. בריאות הציבור: ללא פגיעה ברצפטור ציבורי	1. בריאות הציבור: פוטנציאל פגיעה ברצפטור ציבורי	1. בריאות הציבור: פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 3	
מהי מידת הנזק לבריאות הציבור או לסביבה שעלולה להיגרם עקב פגיעה בבטיחות המערכת שבבעלות העסק?	2. סביבה: ללא פגיעה בסביבה	2. סביבה: פוטנציאל לאירוע חומרים מסוכנים שעלול לגרום לפגיעה בסביבה	2. פוטנציאל לפיצוץ (UVCE): לחץ מרבי 0.28 באר	2. פוטנציאל לפיצוץ (UVCE): לחץ מרבי לרצפטור ציבורי של 0.28 באר	
C (Confidentiality)			3. פוטנציאל לאירוע דלקה (BLEVE)	3. פוטנציאל לאירוע דלקה (BLEVE)	
מהי מידת הנזק לבריאות הציבור או לסביבה שעלולה להיגרם עקב חשיפת מידע על מערכת ממוחשבת המנהלת/מבקרת חומרים מסוכנים שבבעלות העסק?			3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע	
I (Integrity)			קרינה בעוצמה מקבילה לזמן קצר יותר	קרינה בעוצמה מקבילה לזמן קצר יותר	
מהי מידת הנזק שייגרם לבריאות הציבור או לסביבה עקב שיבוש המידע ברכיב התעשייתי או עקב שיבוש התהליך שהרכיב התעשייתי הוא חלק בלתי נפרד ממנו ?					
A (Availability)					
מהי מידת הנזק שייגרם לבריאות הציבור או לסביבה עקב השבתת הרכיב התעשייתי או תהליך ממוחשב?					

$$I = \text{Max} (1-4) = 1 \text{ to } 4$$

הנתונים לקוחים מתוך חוזר מנכ"ל - מדיניות מרחקי הפרדה במקורות סיכון נייחים - מהדורה מעודכנת
<http://www.sviva.gov.il/subjectsenv/hazardousmaterials/riskmanagement/documents/hm-distance-polcy.pdf>

SRP TRIAD



בטיחות

אמינות

יעילות

פיזור גאזים רעילים – ערכי PAC

PAC – Protection Action Criteria

PAC1 - Potential for dispersal of hazardous substances, accompanied by a **reversible** public health impact

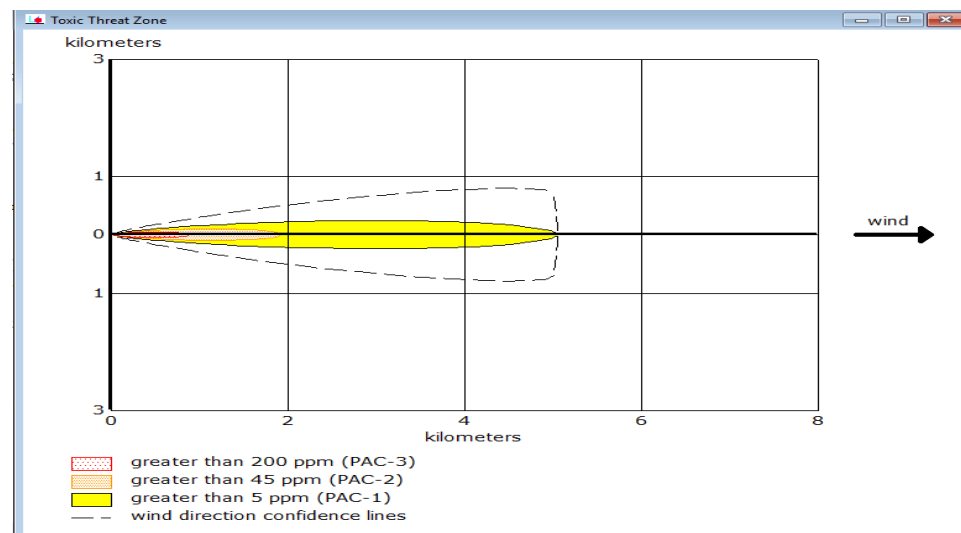
PAC2 - Potential for dispersal of hazardous substances, accompanied by **irreversible** damage to public health

PAC3 - Potential for dispersal of hazardous substances, with **fatal impact** on public health

*It's about an hour's exposure

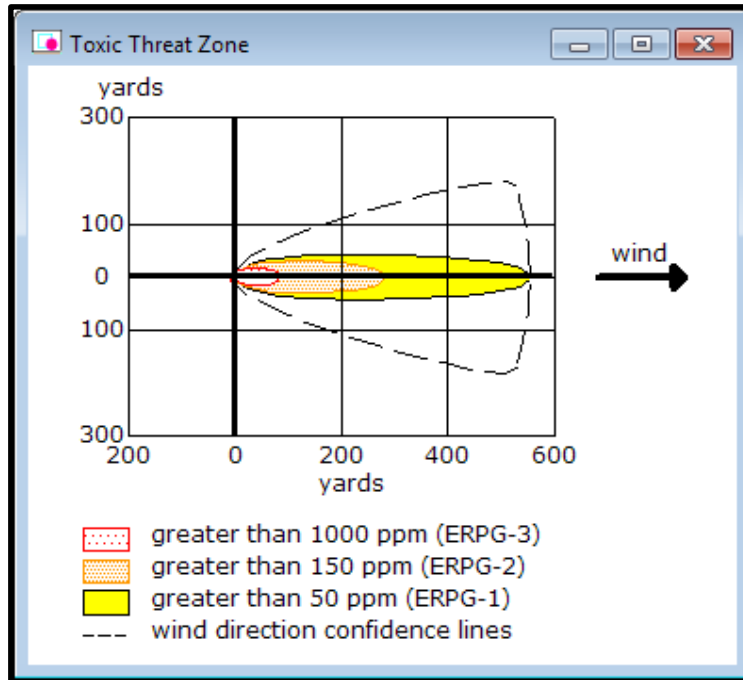


<https://www.weizmann.ac.il/safety/he/%D7%AA%D7%A8%D7%92%D7%99%D7%9C-%D7%97%D7%95%D7%9E%D7%A8%D7%99%D7%9D-%D7%9E%D7%A1%D7%95%D7%98%D7%A0%D7%99%D7%9D-1962014-hazardous-materials-drill>

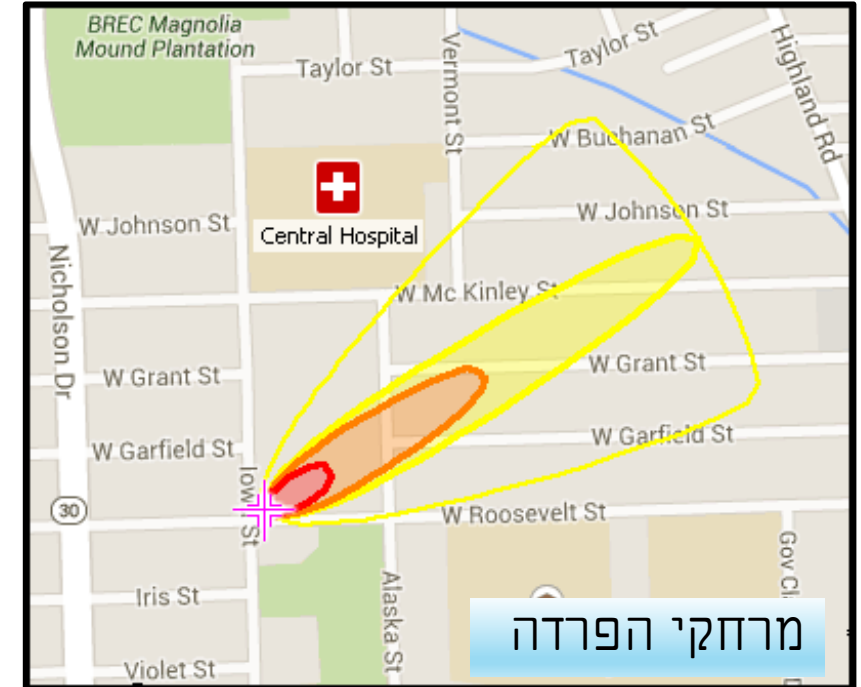


PAC Software

ALOHA 5.4.7



MARPLOT 5.1.1



INPUT:

- Atmospheric conditions: wind direction and intensity
- Location: precise details of the location (Including height above sea level)
- Container: shape and dimensions of the container of hazardous material
- Spreading Algorithm (Gaussian dispersion, Heavy Gas dispersion)

שלב 3 חישוב ההסתברות להתממשות הנזק

נספח ב' - טבלה לקביעת מידת החשיפה (P) של עסק המחזיק חומרים מסוכנים

בטבלה זו יש לענות על כל 36 השאלות שבעמודת "פרמטר נבדק" על ידי מתן ציון מ-1 עד 4. לאחר מתן ציונים לכל השאלות, יש לחשב את מידת החשיפה על ידי סיכום כל הציונים וחישוב ממוצע לכל הטבלה. התוצאה המתקבלת היא רמת החשיפה – P.

יש לבצע את הניתוח לפי טבלה זו בנוגע לכל התהליך המצוין במיפוי התהליכים המסוכנים ובנוגע לכל מערכת ממוחשבת בכל אחד מתהליכים אלה.

רמת חשיפה / פרמטר נבדק	1	2	3	4	ציון (4-1)
1. מספר עובדים החשופים למערכות אדם - מכונה (HMI) המנהלות/מבקרות חומרים מסוכנים	עד 5	6 - 10	11 - 50	יותר מ-50	
2. מספר עובדים בעלי גישה לבקרים המנהלים/מבקרים מערכת חומרים מסוכנים	עד 10	11 - 25	26 - 50	יותר מ-50	
3. אחריות הטיפול במערכות אדם - מכונה (HMI) בבקרים	רק עובדים פנימיים	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	נגישות לגורמים נוספים	
4. אחריות הטיפול המשפיעים על מערכת חומרים מסוכנים	רק עובדים פנימיים	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	נגישות לגורמים נוספים	
5. מספר עמדות אדם-מכונה (HMI) שיש בעסק	1	2 - 5	6 - 10	יותר מ-10	
6. מספר בקרים הקשורים לחומרים מסוכנים בעסק	עד 5	6 - 10	11 - 50	יותר מ-50	
7. תקשורת בין רשת מנהלית לרשת תפעולית	אין - קיים ניתוק פיזי ברמת כבילה בין הרשתות	יש באמצעות חומת אש ודיודה חד-כיוונית	יש באמצעות חומת אש בלבד	יש ללא אמצעי בקרה	
8. האם מתאפשרת גישה לאינטרנט מסביבת הבקרים התעשייתיים?	לא	יש חיבור, אבל בדרך כלל מנותק. מופעל לצורך תמיכה מרחוק	כן, אך עם בקרת חומת אש וסינון תוכן או רכיבי אבטחה נוספים	כן	

נספח ב' במדריך הסייבר לתעשייה

הסתברות (PROBABILITY)

ערך ההסתברות מייצג גם את משטח החשיפה (Attack Surface)

אנו מסמנים את ההסתברות באות P

$$P = \text{Average} (1-36) = 1 \text{ to } 4$$

קובץ אקסל לחישוב רמת החשיפה לארוע סייבר (P) באתר המשרד

ציון	4	3	2	1	רמת חשיפה ← פרמטר נבדק ↓
1	מעל 50	10-50	5-10	עד 5	מספר עובדים החשופים למערכות אדם-מכונה (HMI) הקשורות לחומרים מסוכנים
3	מעל 50	25-50	10-25	עד 10	מספר עובדים בעלי גישה לבקרים המשפיעים על מערכת חומרים מסוכנים
2	נגישות גם לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	אחריות הטיפול במערכות אדם - מכונה (HMI)
2	נגישות גם לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	אחריות הטיפול בבקרים המשפיעים על מערכת חומרים מסוכנים
4	מעל 10	5-10	1-5	1	מספר עמדות אדם – מכונה (HMI) שיש בעסק
1	מעל 50	5-10	1-5	1	מספר בקרים הקשורים לחומרים מסוכנים בעסק
2	קיימת ללא אמצעי בקרה	קיימת באמצעות חומת אש בלבד	קיימת באמצעות חומת אש ודיודה חד כיוונית	לא קיימת	תקשורת בין רשת מנהלית לרשת תפעולית
3	ק	כן אך עם בקרת חומת אש וסינון תוכן או רכיבי אבטחה נוספים	חיבור קיים, אבל בדרך כלל מנותק. מופעל לצורך תמיכה מרחוק	לא	האם מתאפשרת גישה לאינטרנט מסביבת הבקרים התעשייתיים?
1	לא מתבצע	מתבצע באופן מועט	מתבצע באופן רחב	מתבצע באופן מלא וקבוע	עדכון קושחה בבקרים
1	לא מתבצע	מתבצע באופן מועט	מתבצע באופן רחב	מתבצע באופן מלא וקבוע	עדכון תוכנה בבקרים ובמערכות ICS גלויות.
2	נגישות גם לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	אבטחה פיזית למערכות אדם - מכונה (HMI)
4	נגישות גם לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	אבטחה פיזית לבקרים הקשורים לחומרים מסוכנים
4	נגישות גם לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	אבטחה פיזית לרכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה)

ציון החשיפה לכל נכס הינו הציון הממוצע שהתקבל ל-36 השאלות

$$P = \text{Average} (1-36)$$

שלב 4 חישוב רמת הסיכון במערכת ממוחשבת המחוברת לחומ"ס

רמת נזק (I)	הסתברות (P)	1	2	3	4
4	4	7	10	13	16
3	3	6	9	12	15
2	2	5	8	11	14
1	1	4	7	10	13

Risk = P + 3*I
 INCD (Israel National Cyber Directorate)

שאלה	1	2	3	4
S (Safety)	1. כבידות: ללא פגיעה ציבורי	2. כבידות: ללא פגיעה ציבורי	3. כבידות: ללא פגיעה ציבורי	4. כבידות: ללא פגיעה ציבורי
C (Confidentiality)	2. סביבה: ללא פגיעה בסביבה	2. סביבה: ללא פגיעה בסביבה	3. סביבה: ללא פגיעה בסביבה	3. סביבה: ללא פגיעה בסביבה
I (Integrity)	2. סביבה: ללא פגיעה בסביבה	2. סביבה: ללא פגיעה בסביבה	3. סביבה: ללא פגיעה בסביבה	3. סביבה: ללא פגיעה בסביבה
A (Availability)	2. סביבה: ללא פגיעה בסביבה	2. סביבה: ללא פגיעה בסביבה	3. סביבה: ללא פגיעה בסביבה	3. סביבה: ללא פגיעה בסביבה
ציון	1	2	3	4
שם הבודק	תפקיד	תאריך	ציון	חתימה

רמת חשיפה < V	1	2	3	4	ציון (1-4)
1. מספר עובדים החשופים למערכות אדם-מכונה (HMI) הקשורות לחומ"ס	עד 5	6-10	11-50	מעל 50	
2. מספר עובדים לוקרים המשפיעים על מערכת חומ"ס	עד 10	11-25	26-50	מעל 50	
3. אחריות במערכות אדם-מכונה (HMI)	רק עובדים פנימיים	קבועים חיצוניים	ספקים חיצוניים מודדמים	ספקים חיצוניים מודדמים	נגישות גם לזרמים חסמים
4. אחריות הטיפול במערכות אדם-מכונה (HMI)	רק עובדים פנימיים	קבועים חיצוניים	ספקים חיצוניים מודדמים	ספקים חיצוניים מודדמים	נגישות גם לזרמים חסמים
5. מספר עובדים אדם-מכונה (HMI) הקיימות במפעל	1	2-5	6-10	מעל 10	
6. מספר בקרים חשופים לחומ"ס במפעל	עד 5	6-10	11-50	מעל 50	



חישוב רמת הסיכון של המערכת

$P * I$ vs $P + 3 * I$

$P + 3 * I$	$P * I$	ערך הסתברות P	ערך אימפקט I
4	1	1	1
5	2	2	1
6	3	3	1
7	4	4	1
7	2	1	2
8	4	2	2
9	6	3	2
10	8	4	2
10	3	1	3
11	6	2	3
12	9	3	3
13	12	4	3
13	4	1	4
14	8	2	4
15	12	3	4
16	16	4	4



קביעת רמת הבקרות

שלב 5

נספח ג' במדריך הסייבר לתעשייה

רשימת הבקרות					
מס' הבקרות בפרק זה	בדיקה	רמה	המלצות / הערות	פירוט	בקרה נדרשת
3	1.1 האם בוצע מיפוי חומרים מסוכנים. 1.2 האם בוצע מיפוי מערכות המחשוב והבקרה.	1	1.2 ב. מומלץ להיוועץ באנשי מקצוע בתחום החומים על מנת לברר אם מערכת ממוחשבת שאינה מטפלת בחומים אבל עשויה להתלקח או להתפוצץ עקב התקפת סייבר (למשל דוד קיטור בעל בקר מתוכנת) - מסכנת חומים בסביבתה.	1.2 המיפוי יכול: רשימת המחשבים - בציון תפקידם והמערכות המותקנות עליהם לצורך תפקידם; עמדות HMI/אוטומציה/ייעודיות/משולבות מכונה - בציון דגם וגרסת תוכנה; בקרים ומרכזות גלאים - בציון דגם, גרסת קושחה/תוכנה וסוג התקשורת (Ethernet, WiFi, טלפון, אחר); רכיבי IoT/IIoT וגלאים בציון דגם, מקום וסוג התקשורת אליהם; רכיבי הרשת (מתנים, נתבים, נקודות גישה אלחוטיות, חומת אש) בציון דגם וחיבורם לרשתות אחרות/אינטרנט.	מיפוי מערכות וכתובת מדיניות אבטחת מידע למערכות מחשוב ובקרת חומ"ס 1.1 בעל העסק יבצע מיפוי כל החומרים המסוכנים אשר מטופלים במערכות ממוחשבות. 1.2 בעל העסק יבצע מיפוי כל מערכות המחשוב, הרשת, הבקרה, החישה והאוטומציה בעסק ואלה הן: א. הנוגעות לאחסון, שימוש, זרימה, ייצור, שינוע, השמדה וגילוי חריגות ודליפות של חומרים מסוכנים. ב. העוללות לגרום או לתרום לפריצת חומרים מסוכנים בפעולה זדונית או לא תקינה בהם. ג. הנוגעות לרישום מלאי ולוגיסטיקה של חומרים מסוכנים.
1	1.6 הבדיקה מספק.	4			בדיקת חדרות (Penetration Test) 1.6 יש לבצע אחת לשנתיים בדיקת חדרות בעזרת מומחה אבטחת מידע, אשר תכלול לפחות: א. בדיקת עמידות מערכות המחשוב ובקרת החומים להתקפה מחוץ לעסק. ב. בדיקת עמידות מערכות המחשוב ובקרת החומים להתקפה מרשת ה-IT בעסק. ג. בדיקת עמידות מערכות המחשוב ובקרת החומים לתוקף בעל גישה פיזית לעמדות תפעול ולארונות התקשורת והבקרים.

פוטנציאל הסיכון	חבילת הבקרות בהתאם לפוטנציאל הסיכון	כמות הבקרות לחבילה זו
4-7	1	41
8-11	2	59
12-14	3	81
15-16	4	92



איזה בקרות להטמיע ?

נתון: נניח שקיבלנו בחישובים $P=2.6$, $I=3$

$$\text{RISK} = P + 3 * I = 2.6 + 3 * 3 = 11.6$$

חישוב הסיכון :
מעגלים כלפי מעלה – Risk = 12

הערה: קיימת אופציה לנסות להוריד את רמת החשיפה P ולהגיע לרמה יותר נמוכה

אם $\text{RISK} = 12$ אנו בחבילת בקרות 3

כמות בקרות להטמעה: 81

יתכן שחלק מהבקרות כבר קיימות נניח 50

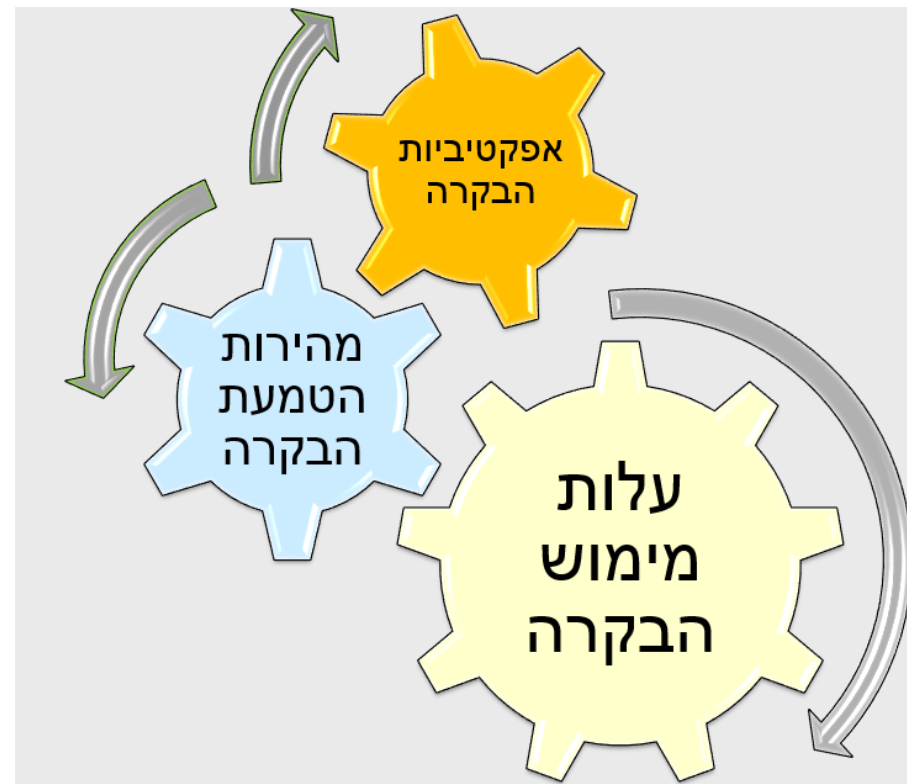
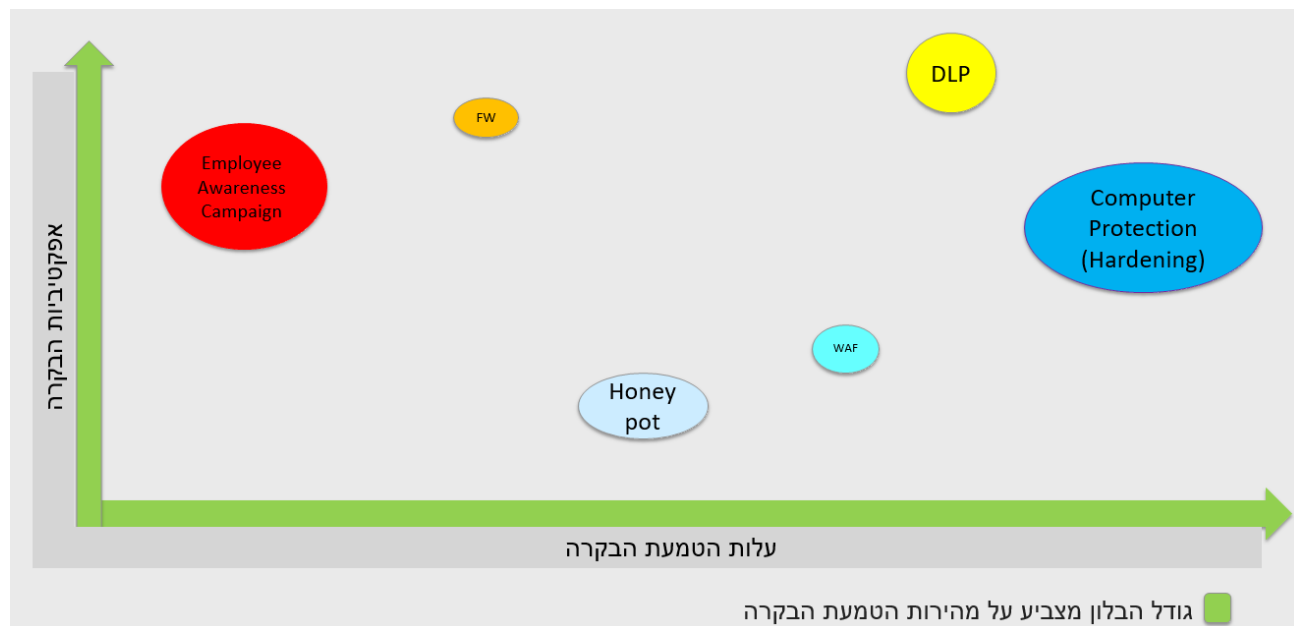
יש להטמיע את הדלתא : $81 - 50 = 31$

יש לנו 31 בקרות להטמעה

הערה: במידה ובקרה מסויימת קשה להטמעה מבחינת לוחות זמנים, עלויות, חוסר במשאבים אחרים על העסק להציע בקרה מפצה אשר נותנת מענה ראשוני עד להטמעה מלאה של הבקרה הנדרשת – כל זאת באישור יחידת הסייבר בתעשייה

פוטנציאל הסיכון	חבילת הבקרות בהתאם לפוטנציאל הסיכון	כמות הבקרות לחבילה זו
4-7	1	41
8-11	2	59
12-14	3	81
15-16	4	92

המשאבים בארגון מצומצמים – במה לטפל קודם???





<http://www.robi-steiner.co.il/why-there-is-a-gap>

בשלב זה יש לבצע אנליזת פערים (GAP ANALYSIS)

✓ מניהול הסיכונים, ידוע לנו איזה בקרות נדרשות

✓ יש לבצע השוואה מול הבקרות הקיימות

✓ יש ליישם את הדלתאות

תכנית עבודה

שלב 7



<https://www.pexels.com/>

בשלב זה יש לכתוב תכנית עבודה

מומלץ כי תכנית העבודה תכלול את הדברים הבאים:

- ✓ שם המערכת
- ✓ בקרות נדרשות להטמעה על פי תכנית מיפוי פערים
- ✓ פירוט שלבי ביצוע להטמעת כל בקרה ובקרה
- ✓ אחראי ביצוע לכל בקרה ובקרה
- ✓ משאבים נדרשים לכל בקרה ובקרה
- ✓ לוח לסיים כל בקרה ובקרה
- ✓ נושאים נוספים לפי שיקול דעת העסק

רשימת הבקרות

נספח ג'

קבוצות הבקרות – על פי תקן NIST CSF

5 משפחות בקרות: (CYBERSECURITY FUNCTIONS)

- זיהוי – IDENTIFY
- הגנה – PROTECT
- איתור – DETECT
- תגובה – RESPOND
- התאוששות – RECOVER

רמות של בקרה

מרבית	מחמירה	מתקדמת	בסיסית	בקרה
				בקרת גישה
				אבטחת רשת



שלב 8 בקרה וניטור



<https://www.pexels.com/>

לאורך כל התהליך יש לבצע בקרה וניטור על:

- ✓ שלבי התהליך
- ✓ סיום כל שלב ושלב בלויז
- ✓ מילוי דרישות הרגולטור:
 - מינוי ממונה הגנת סייבר
 - השלמת מסמך מדיניות הנהלה
 - תצהיר לסיום סקר סיכונים
 - תצהיר לסיום הטמעת בקרות.






תרגיל דוגמא

במפעל אמוניה כ-60 טון המחולק בין 3 חדרי מכונות כל חדר מכונות מהווה תהליך בפני עצמו מחובר למערכת מחשוב ומנוהל ע"י מערכת HMI ייעודית לאותו תהליך מפריד הטיפות בכל מערכת מהווה את המיכל הגדול ביותר ומכיל חצי טון

להלן נתונים לגבי אמוניה:



NFPA 704

Diamond	Hazard	Value	Description
	 Health	3	Can cause serious or permanent injury.
	 Flammability	1	Must be preheated before ignition can occur.
	 Instability	0	Normally stable, even under fire conditions.
	 Special		

PACs (Protective Action Criteria)

Chemical	PAC-1	PAC-2	PAC-3	
Ammonia (7664-41-7)	30 ppm	160 ppm	1100 ppm	LEL = 150000 ppm

(DOE, 2016)

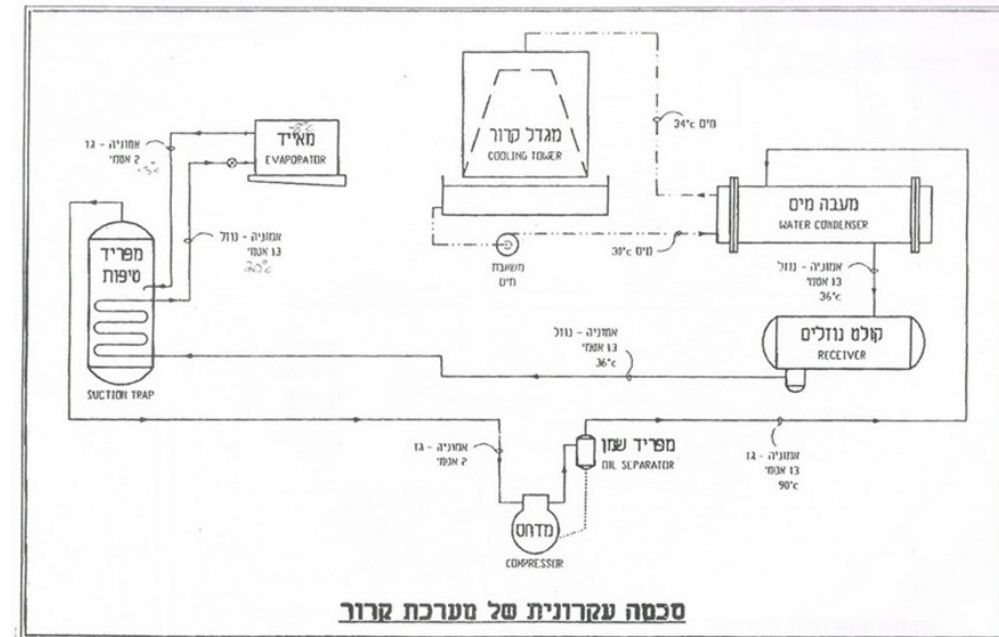
מהנדס הבקרה, איש ה-IT והקב"ט מלאו את קובץ רמת החשיפה (P), ענו על 36 השאלות בקובץ והגיעו לערך ממוצע: $P = 2.6$

מהכנסת נתוני המיכלים, נתוני מזג אויר, נתוני פיזור הגז ועוד לתכנת האלוהה מסתבר שמגיעים לערך של 200PPM באוויר איזה חבילת בקרות יש להטמיע על מערכת הקירור?

עמדת אדם מכונה במפעל



סכימת הקירור במפעל



תשובה:

$P=2.6$

$I=3$

$RISK=2.6+ 3*3= 11.36 \Rightarrow 12$

כמות הבקורות לחבילה זו	חבילת הבקורות בהתאם לפוטנציאל הסיכון	פוטנציאל הסיכון
41	1	4-7
59	2	8-11
81	3	12-14
92	4	15-16

במקרה הזה יש להטמיע חבילת בקורות מספר 3

הנחיות למבחן :

- המבחן בנוי מ 25 שאלות אמריקאיות שלכל שאלה תשובה אחת נכונה בלבד. משקל כל שאלה 4 נקודות.
- המבחן יועבר בלינק לכולכם דרך הצי'אט אותו יש לפתוח באקספלורר (פתיחת הלינק בכרום קצת משבש ולכן מומלץ ועדיף לפתוח באקספלורר)
- המבחן עם מצלמות פתוחות ומיקרופונים סגורים, אין להתייעץ אחד עם השני בשעת המבחן, מותר להיעזר בכל חומר כתוב כולל מצגות ואינטרנט.
- לאורך כל המבחן ניתן לשאול שאלות בצי'ט ויוסי יענה.
- קבלת תעודות גמר – ישירות מהתאחדות התעשיינים למייל האישי שלכם עד כשבוע





שאלות ותשובות

