

לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA Israel - Institute of Internal Auditors
הכנס המקצועי השנתי של הביקורת הפנימית 2025



ביקורת סייבר - להיות או לא להיות? ליאור סגל

עו"ד, רו"ח, MBA, CIA, CRMA, QAR, CISA, CISM,
CDPSE, CRISC

המבקר הפנימי בזק | דירקטור מזכיר וגזבר, IIA ישראל

23 בינואר, 2025

\$8

Trillion

Cost of cybercrime
in 2023



\$250K+

PER SECOND

\$9.5

Trillion

Cost of cybercrime
in 2024



\$300K+

PER SECOND

\$10.5

Trillion

Cost of cybercrime
in 2025



\$330K+

PER SECOND

מקור: נתונים שהציג נשיא הלשכה העולמית במחצית 2 2024

מתקפות סייבר נמצאות בכותרות כל הזמן, במיוחד במהלך המלחמה

אלפי ניסיונות תקיפה בכל יום: מלחמת הסייבר בין ישראל לאיראן וחיזבאללה

מתחילת המלחמה בוצעו 517 מתקפות סייבר נגד מוסדות להשכלה גבוהה בישראל

התרגיל נועד להעלות את המוכנות של המוסדות להשכלה גבוהה בישראל בארץ לנוכח האתגרים המתעצמים בתחום הסייבר.

סוג: חדשות • תאריך פרסום: 17.12.2024 • תאריך עדכון: 18.12.2024

חדשות • השירות החשאי

מפקדת ממר"ם הודתה לראשונה שהענן של צה"ל ספג מתקפות סייבר במלחמה

אל"מ רחלי דמבינסקי חשפה כי המערכות של צה"ל ספגו יותר משלושה מיליארד מתקפות סייבר מאז 7 באוקטובר. לדבריה, כלל המתקפות נהדפו, ובשום מקרה הן לא הובילו לקריסה של אחת המערכות

כלכלה טכנולוגיה

בעקבות המלחמה: התגברות משמעותית של תקיפות סייבר על ישראלים

מבקר המדינה מתריע על התגברות משמעותית של החשש מפני מתקפות סייבר על גופים ישראלים שונים. כמו כן, מתייחס המבקר למספר סקרי סיכונים שהרשויות נמנעו מלבצע

כנדרש

RESEARCH

JULY 16, 2024

Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks

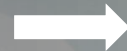


The Institute of
Internal Auditors

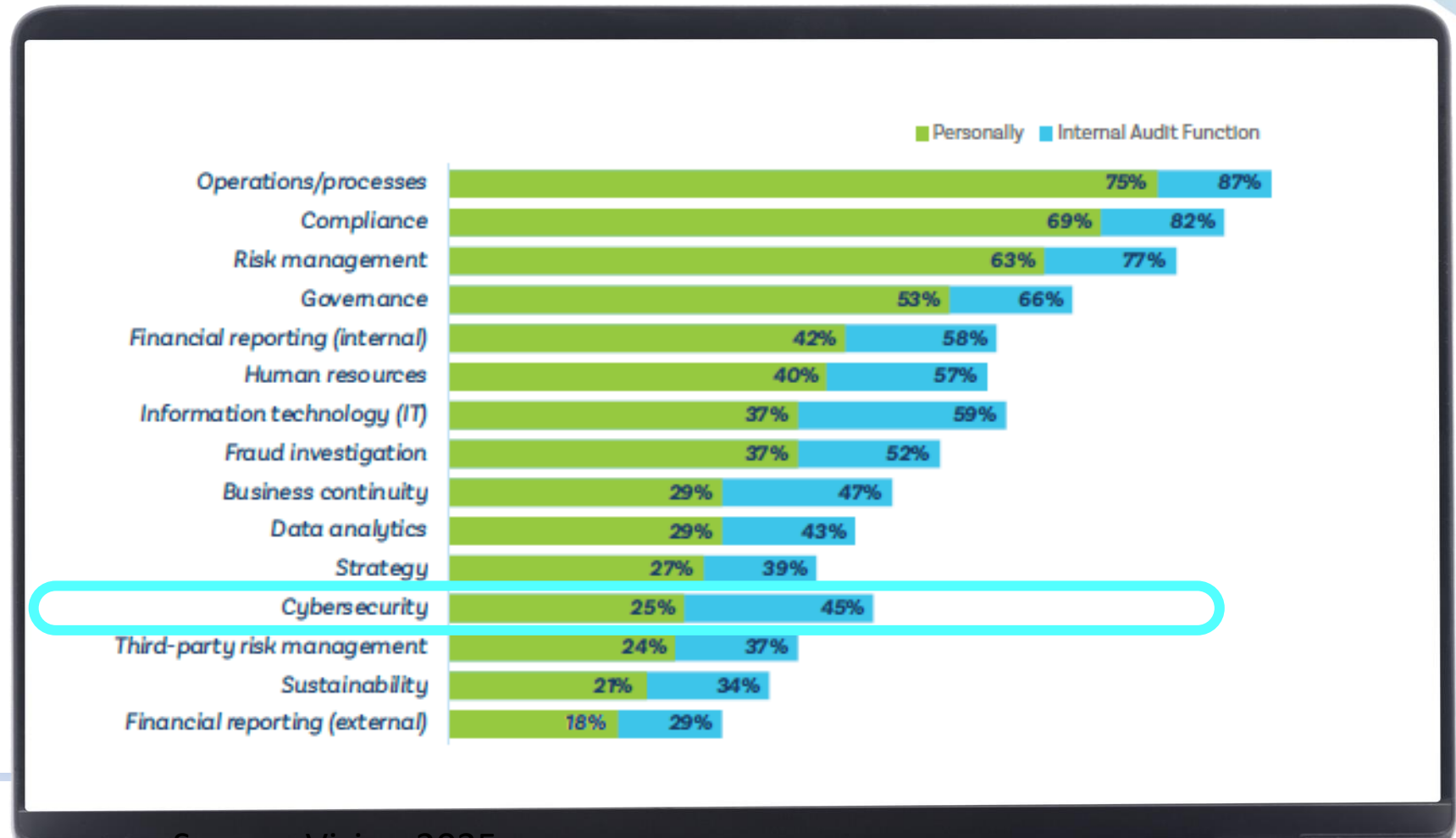
Elevating Impact

סקר מספר 1 - באיזו תדירות מבצעים ביחידת הביקורת שלכם ביקורת בנושא סייבר?

1. כל שנה
2. אחת לשלוש שנים
3. אנחנו לא מבצעים ביקורת סייבר
4. אני לא יודע/ת



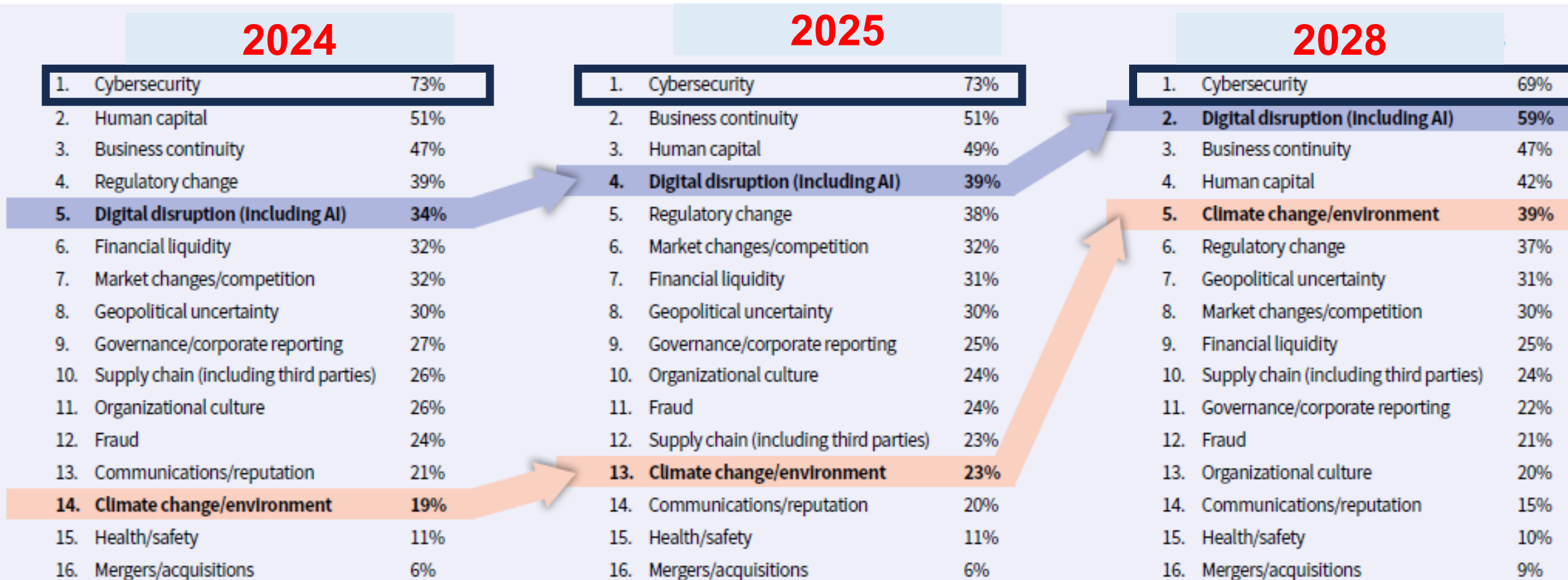
בסקר עולמי עלה לאחרונה כי רק כ-45% מיחידות הביקורת עורכות ביקורת סייבר



Source: Vision 2035

ובסקר אחר הצביעו מבקרים על כך כי זה הסיכון שמדורג

במקום הראשון



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



אז מה חדש בקשר בין
סייבר והביקורת הפנימית?

הכנס המקצועי השנתי של הביקורת הפנימית 2025

מאמצים את השינוי ומציבים סטנדרטים חדשים

יום חמישי, 23 בינואר 2025 | LAGO, ראשון לציון

ראשית, התקנים החדשים כבר כאן



תקן 9.4 תוכנית עבודת הביקורת הפנימית

דרישות

המבקר הפנימי הראשי חייב ליצור תוכנית עבודה של הביקורת הפנימית אשר תומכת בהשגת יעדי הארגון.

המבקר הפנימי הראשי חייב לבסס את תוכנית עבודת הביקורת הפנימית על הערכה מתועדת של האסטרטגיות, היעדים והסיכונים של הארגון. הערכה זו חייבת להיות מבוססת על משוב/מידע ממועצת המנהלים ומהנהלה הבכירה, וכן על הבנתו של המבקר הפנימי הראשי לגבי הממשל התאגידי, ניהול הסיכונים ותהליכי הבקרה (GRC) של הארגון. ההערכה חייבת להתבצע לפחות מדי שנה.

תוכנית עבודת הביקורת הפנימית חייבת:

- לשקול את מנדט הביקורת הפנימית ואת כל מגוון שירותי הביקורת הפנימית המוסכמים.
 - לציין שירותי ביקורת פנימית אשר תומכים בהערכה ושיפור של הממשל התאגידי, ניהול הסיכונים ותהליכי הבקרה (GRC) של הארגון.
 - לשקול כיסוי של ממשל טכנולוגיות מידע, סיכון למעילות והונאות, האפקטיביות של תוכניות הציות והאתיקה של הארגון, ותחומים אחרים בסיכון גבוה.
 - לזהות את משאבי האנוש, המשאבים הפיננסיים, והמשאבים הטכנולוגיים הנדרשים למימוש התוכנית.
 - להיות דינמית ומעודכנת במועד בתגובה לשינויים בעסקי הארגון, בסיכונים, בפעילות, בתוכניות, במערכות, בבקורות, ובתרבות הארגונית.
- המבקר הפנימי הראשי חייב לסקור ולשנות את תוכנית עבודת הביקורת הפנימית ככל הנדרש, ולתקשר (לדווח) במועד למועצת המנהלים ולהנהלה הבכירה על:
- השפעתן של מגבלות כלשהן במשאבים על כיסוי הביקורת הפנימית.
 - הרציונל בגינו תוכנית העבודה אינה כוללת מטלת הבטחה בתחום או בפעילות בסיכון גבוה.
 - דרישות סותרות לשירותים בין מחזיקי עניין מרכזיים, כגון בקשות בעדיפות גבוהה על-בסיס סיכונים פורצים ובקשות להחליף מטלות הבטחה מתוכננות במטלות ייעוץ.
 - מגבלות על היקף או הגבלות על גישה למידע.

המבקר הפנימי הראשי חייב לדון, עם מועצת המנהלים והנהלה הבכירה, בתוכנית עבודת הביקורת הפנימית, לרבות שינויי ביניים משמעותיים. תוכנית העבודה ושינויים משמעותיים בתוכנית עבודת הביקורת הפנימית חייבים להיות מאושרים על ידי מועצת המנהלים.

על נושא הסייבר להילקח בחשבון במסגרת גיבוש בתוכנית העבודה



וקיימות בתקנים דרישות רבות

תקן 3.1 יכולת

דרישות

מבקרים פנימיים חייבים להחזיק או להשיג את היכולות הנדרשות כדי למלא את תחומי האחריות שלהם בהצלחה. היכולות הנדרשות כוללות את הידע, המיומנויות והכישורים המתאימים לתפקיד ולתחומי האחריות המתאימים לרמת הניסיון שלהם. מבקרים פנימיים חייבים להחזיק או לפתח ידע בתקנים הגלובאליים של הביקורת הפנימית של ה- IIA.

מבקרים פנימיים חייבים לעסוק אך ורק באותם שירותים עבורם הם מחזיקים או יכולים להשיג את היכולות הנדרשות.

כל מבקר פנימי אחראי לפיתוח מתמשך וליישום היכולות הנדרשות על מנת לבצע את תחומי האחריות המקצועיים שלו. בנוסף, המבקר הפנימי הראשי חייב לוודא שפונקציית הביקורת הפנימית, בכללותה, מחזיקה ביכולות הנדרשות כדי לבצע את שירותי הביקורת הפנימית המתוארים בכתב האמנה של הביקורת הפנימית (צ'רטר), או חייב להשיג את היכולות הנדרשות כאמור (ר' גם תקן 7.2 המבקר הפנימי הראשי - כישורים מקצועיים, ותקן 10.2 ניהול משאבי אנוש).

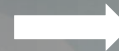
חשיבות גם למיומנות האישית

סקר מספר 2 - מה לדעתכם צריכה הביקורת הפנימית לדעת על סייבר?

1. הבנה בסיסית

2. הבנת עומק

3. לא צריכים כל הבנה בנושא



מה צריכים כל המבקרים הפנימיים לדעת על אבטחת סייבר?

כיצד יכולים להגן על עצמם מפני איומי סייבר?

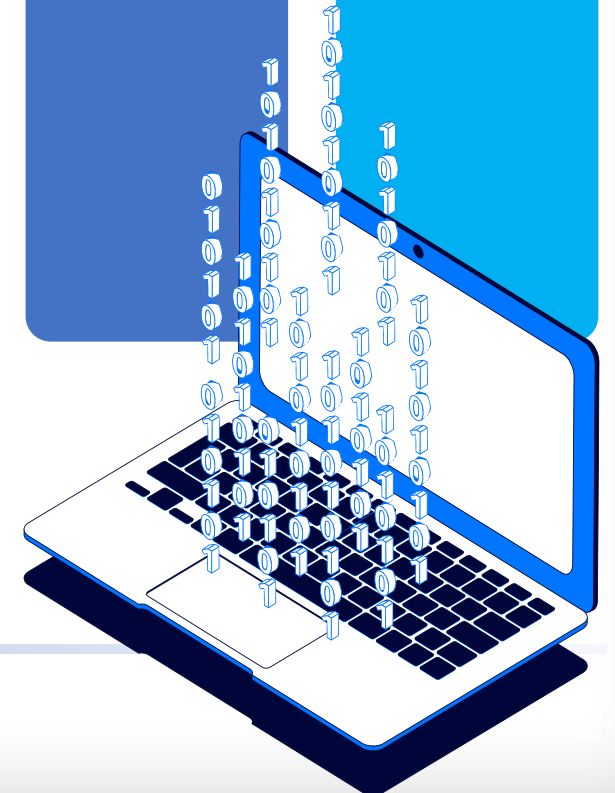
מהי ההשפעה של איומים אלו?

מה תורם להתפתחות המהירה של איומי סייבר?

מה בכוונת ההתקפות להשיג?

מי מבצע התקפות סייבר?

מהם איומי סייבר (קיימים ועתידיים)?



חידוש משמעותי- חובת יישום דרישות נושאיות

הדרישות הנושאיות
(Topical requirements)



Topical Requirement



מהן הדרישות הנושאיות?

דרישות נושאיות (Topical Requirements) - מרכיב חובה שעל כל מבקר פנימי ליישם אותו, כאשר מבוצעת ביקורת בנושא שבו עוסקת הדרישה הנושאית (הסבר בהמשך)

כן ולא בנוגע לדרישות הנושאים



נדרש לציית לדרישות אלה כאשר מבצעים ביקורת בנושא
כאשר פועלים לא בהתאם לקבוע בהן - יש לתעד זאת
מהוות נקודת בסיס כאשר הנושא מבוקר
כוללות את ההיבטים הדרושים בנושאי ממשל תאגידי,
ניהול סיכונים ובקרה
ייבדקו במסגרת הערכת איכות חיצונית

אינן מטילות חובה לבצע ביקורת בנושא
אינן מהוות תוכנית ביקורת מקיפה
לא נועדו לטפל בנושאים פורצים
אינן תחליף להערכת סיכונים או לשיקול דעת מקצועי
אינן מחליפות דרישות החלות מכח רגולציה ספציפית



מדוע נוצר הצורך בדרישות נושאים?

חיזוק הרלבנטיות המתמשכת של התקנים הבינלאומיים ככלי להתמודדות עם סיכונים מתפתחים

להבטיח אחידות ואיכות בעת ביצוע מטלת ביקורת בנושאים אלו

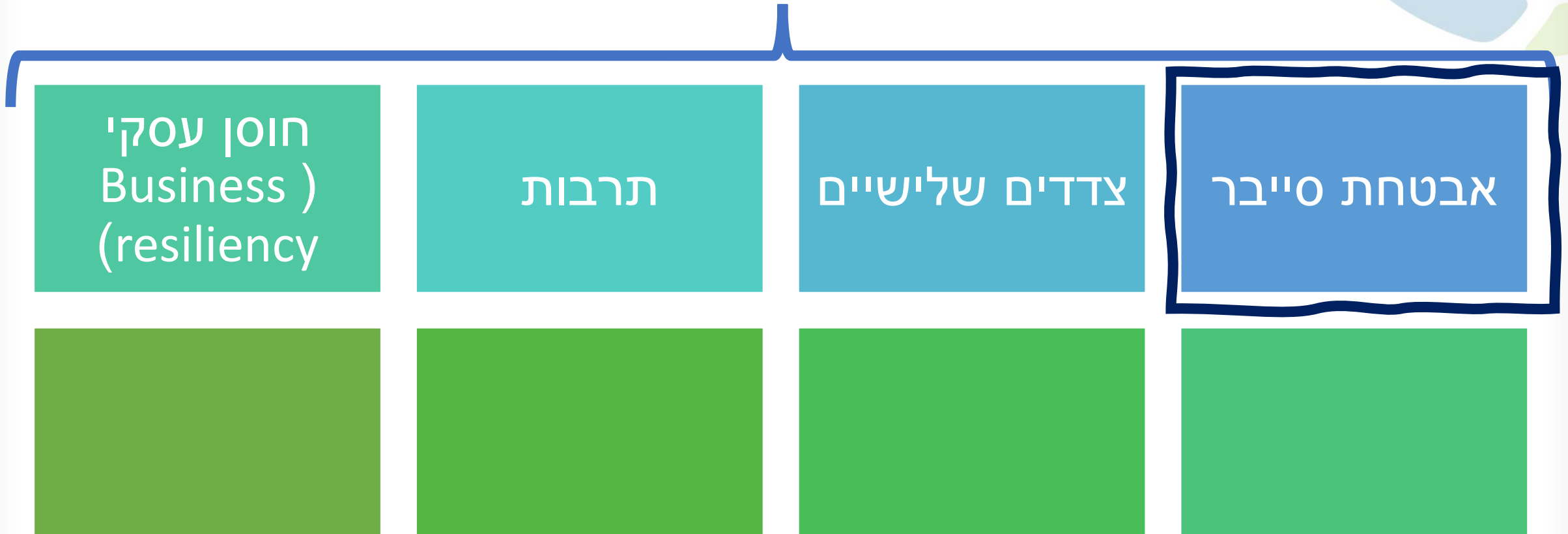
להגביר את המודעות לצורך בייחוד משאבים לביצוע ביקורות בנושאים בעלי חשיבות



קיימות שורה של דרישות נושאיות ב"תנור", נדבר

על אבטחת סייבר

צפוי להישלח לתגובות/ להתפרסם ב-2025



A hand on the right side of the image points towards a glowing blue shield. The shield is semi-transparent and contains a keyhole cutout. The shield is covered in binary code (0s and 1s). The background is dark blue with glowing network lines and binary digits.

LET'S TALK CYBERSECURITY!

הדרישה הנושאת הראשונה הנה בנושא אבטחת סייבר*

אבטחת סייבר
דרישה נושאת

- מהי הדרישה הנושאת, עיתוי הביקורת בנושא
- הגדרה סייבר
- תיאור דרישות חובה בנושא ממשל תאגידי, ניהול סיכונים ובקרה

אבטחת סייבר
דרישה נושאת
מדריך למשתמש

- נושאים שלהם השפעה על בדיקת הנושא
- שיקולים ליישום - ממשל תאגידי, ניהול סיכונים ובקרה
- נספחים



אז מה כוללות דרישות החובה בנושא אבטחת סייבר?



אבטחת סייבר
דרישה נושאית

הסבר- מתי הדרישה הנושאת בקשר לסייבר עשויה להיות רלבנטית?

מתבקשת
ביקורת לאבטחת
סייבר מעבר
לתוכנית
הביקורת
הפנימית
המקורית

נושא/סוגיית
אבטחת סייבר
עולה בעת מטלת
ביקורת אחרת

מטלת ביקורת
אבטחת סייבר
נכללת בתכנית
העבודה השנתית
של הביקורת
הפנימית



דרישות החובה בנושא אבטחת סייבר הם בשלושה מישורים

על המבקר הפנימי לבצע את ביקורתו בנושא במיקודים אלו

ניהול סיכונים

ממשל תאגידי

בקרה

דרישות החובה - ממשל תאגידי

1
אסטרטגיה ויעדים
נקבעים ומתעדכנים

2
מדיניות ונהלים נקבעים
ומתעדכנים

3
נקבעים תפקידים
ואחריות; תהליך
להערכת ידע והכישורים

4
מחזיקי עניין מעורבים
בהחלטות לטיפול
בחשיפות

דרישות החובה- ניהול סיכונים



ניהול הסיכונים מתנהל
ברחבי הארגון

2

ניהול סיכונים כולל זיהוי,
ניתוח, הפחתת וניטור
איומי סייבר

1

תהליך תגובה והתאוששות
לאירועי אבטחת סייבר

4

קיום תהליך להסלמה
מהירה של הסיכון

3

דרישות החובה- בקרה

1

הבטחת קיום בקרות, להגנה על הסודיות, היושרה וזמינות מערכות ונתונים

2

ניהול כישרונות

3

ניטור ולדיווח באופן רציף על איומים ופגיעויות באבטחת סייבר

4

אבטחת סייבר נכללת בניהול מחזור החיים של כל נכסי מערכות המידע

ומה במדריך למשתמש?

אבטחת סייבר
דרישה נושאת
מדריך למשתמש



נושאים מרכזיים הכלולים במדריך למשתמש (גוף המסמך)

פירוט תוכן הדרישות, מודל שלושת הקווים

ישימות, סיכון ושיקול דעת מקצועי בעת היישום, ראיות דרושות

אופן העמידה בדרישה הנושאית

שיקולים ליישום (considerations)

נושאים מרכזיים הכלולים במדריך למשתמש (נספחים)

פירוט המצבים שבהם יידרש ליישם את הדרישה הנושאת

מיפוי בין מסגרות מקובלות ובין הוראות החובה בדרישות
הנושאות

כלי אפשרי לבחינת העמידה בהוראות הדרישה הנושאת

לסיכום...

מתקפות הסייבר נמצאות במגמת גידול משמעותית בשנים האחרונות, ובייחוד בישראל, מאז פרצה מלחמת "חרבות ברזל" עלינו, כמבקרים פנימיים, להבין היטב את סיכוני הסייבר והיבטים הקשורים בנושא זה

השקת הדרישה הנושאת בנושא אבטחת סייבר, מחייבת כל אחד מאתנו להכיר את הדרישה, ולבחון את יישום הדרישות הכלולות בה, כאשר מבוצעת ביקורת בנושא



תודה רבה!

אשמח אם תשמרו על קשר



לפרטים נוספים:

ליאור סגל

טלפון: 050-6773706

מייל: lior.segal@gmail.com

<https://www.linkedin.com/in/liorsegal>

