



רכישת שירותי ענן במגזר הציבורי

מדריך - כולל דוגמת RFP עבור הסכם מסגרת לטכנולוגיית
ענן

גרסה 2: פברואר 2022

לתשומת לבכם

מסמך זה מסופק למטרות מידע בלבד. הוא לא פותח בהתאם לדרישות המשפטיות לתהליכי רכש ציבורי באזור מסוים. באחריות הלקוחות לבצע הערכה עצמאית משלהם של המידע במסמך זה וכל שימוש במוצרים או בשירותים של ספק הענן. מסמך זה לא מהווה כתב אחריות, מצגים, מחויבויות חוזיות, תנאים או הבטחות.

אין לפרש מסמכים ושפה לדוגמה כעצה, הדרכה או ייעוץ משפטיים. לקוחות ענן צריכים להתייעץ עם היועצים המשפטיים שלהם לגבי אחריותם לפי החוק החל במדינת הפעילות שלהם. CISPE מתנערת במפורש מכל חבות או אחריות או נזקים הקשורים או הנובעים ממידע המסופק במסמך זה.

מידע על CISPE

CISPE (<https://cispe.cloud>) Cloud Infrastructure Services Providers in Europe ספקי שירותי תשתיות ענן באירופה, היא קבוצת תעשייה עצמאית ללא מטרות רווח. אנחנו מייצגים ספקי שירותי תשתיות ענן באירופה, עובדים עם התעשייה וקובעי מדיניות כדי לספק הדרכה וחינוך על שירותי ענן ותפקידם בתעשייה, בחיים הציבוריים ובחברה בכלל.

מספר החברות ההולך וגדל שלנו כולל חברות הפועלות בכל מדינות האיחוד האירופי ויש לה מטות גלובליים ב-16 מדינות אירופיות. העמותה פתוחה לחברות בתנאי שהן מצהירות שלפחות אחד מהשירותים שלהן עומד בדרישות של קוד ההתנהגות להגנה על מידע של CISPE. אנחנו:

- דוגלים ביתרונות של מדיניות רכש ציבורי ראשון בענן בתוך האיחוד האירופי והמדינות החברות באיחוד האירופי
- יצירת מעורבות של מגזר תשתיות הענן כדי להגיע לניטרליות אקלימית עד 2030
- קידום דרישות אבטחה קוהרנטיות בכל האיחוד האירופי ותקנים טכניים
- תמיכה בדרישות פרטיות מקיפות עם קוד התנהגות להגנה על מידע
- פעילות לשמירה על שוק תשתיות הענן של האיחוד האירופי פתוח, תחרותי וללא נעילה
- מניעת חובות ניטור תוכן בלתי מוצדקות במסגרת החוקית של האיחוד האירופי

חברי הארגון שלנו מספקים ומתחזקים את "אבני הבניין" החיוניות ל-IT המאפשרות לממשלה, לרשויות ציבוריות ולעסקים לבנות מערכות משלהם ולספק שירותים חיוניים למיליארדי אזרחים. בתפקיד זה, אנחנו מסייעים לפיתוח טכנולוגיות ושירותים מובילים המשלבים בינה מלאכותית (AI), אובייקטים מחוברים, רכבים אוטונומיים ו-5G, ואת הדור הבא של טכנולוגיית קישוריות סלולרית.

קוד התנהגות עבור שירותי תשתיות ענן

קוד ההתנהגות להגנה על מידע של CISPE, שהושק לציבור בספטמבר 2016, קדם את האכיפה של תקנת הגנת המידע הכללית של האיחוד האירופי (GDPR). דבר זה מתיישב עם דרישות GDPR קפדניות כדי לעזור לספקי תשתיות ענן להפעיל תאימות להגנה על נתונים ולהציע מסגרת חזקה כדי לעזור ללקוחות לבחור ספקי ענן ולסמוך על השירותים שלהם. קוד ההתנהגות של CISPE [אפשר על ידי המועצה האירופית להגנת המידע](https://www.codeofconduct.cloud/) (EDPB) במאי 2021, [אפשר על ידי ה-CNIL](https://www.codeofconduct.cloud/) [הצרפתית](https://www.codeofconduct.cloud/) הפועלת כרשות המוסמכת. <https://www.codeofconduct.cloud/>

הסכם ניטרליות אקלימית של מרכזי נתונים

CISPE נכנסה להסכם עם הנציבות האירופית בסוף 2019 כדי לפתח מערך של מדדים ויוזמה של רגולציה עצמית ויוזמה ולהבטיח ניטרליות אקלימית של מרכזי נתונים עד 2030. יוזמה זו פותחה יחד עם איגוד מרכזי הנתונים האירופי (EUDCA) וכן איגודי סחר אחרים ושחקני שוק בתחום מרכזי נתונים - היוזמה הושקה בינואר 2021 כ"הסכם מרכז נתונים לניטרליות אקלימית" <https://www.climateneutraldatacentre.net/>

יוזמת תוכנה הוגנת

יחד עם איגוד ה-CIO הצרפתי CIGREF, ובתמיכתם של איגודי סחר אחרים של CIOs וספקים ברחבי אירופה, CISPE השיקה [10 עקרונות של רישוי תוכנה הוגן עבור לקוחות ענן](https://www.fairsoftware.cloud/), מערך של שיטות עבודה מומלצות לעסקים המחפשים את הענן לחדשנות צמיחה וגמישות, ומאתגרים את ספקי התוכנה שלהם להבטיח כי יש התייחסות למונחי רישוי הוגנים. <https://www.fairsoftware.cloud/>

GAIA-X

CISPE הייתה אחת מעשרים ושניים החברים המייסדים של GAIA-X - היוזמה האירופית שנועדה לספק אקוסיסטם דיגיטלי פתוח, שקוף ומאובטח. ככזאת CISPE הייתה מחויבת לחזון ולעקרונות של ארגון GAIA-X מלכתחילה והמזכיר הכללי שלה נבחר מחדש ביוני 2021 לכהן בדירקטוריון. ניתן להשתמש בחלק מהכלים המוזכרים במדריך כגון [קוד ההתנהגות של CISPE](https://www.gaia-x.eu) [להגנה על נתונים](https://www.gaia-x.eu) וקוד ההתנהגות של SWIPO IaaS כדי להדגים תאימות בעקרונות GAIA-X. <https://www.gaia-x.eu>

CISPE והמגזר הציבורי

CISPE תורמת לדיון על המדיניות הציבורית באירופה ופועלת להבטחת הבנה טובה יותר של התפקיד, התרומה והפוטנציאל של תעשיית תשתיות הענן באירופה.

בעוד שמודלים של רכישה ציבורית צריכים להתנות את תהליך האימוץ והשימוש במחשוב ענן, רכישת שירותי ענן שונה מרוב רכישות הטכנולוגיה המסורתיות המוכרות למגזר הציבורי. יש לחשוב מחדש על גישות רכש: CISPE מעודדת את קובעי המדיניות של האיחוד האירופי לפתח גישה שאפתנית יותר, שצופה את פני העתיד בקנה מידה של האיחוד האירופי המבוססת על יוזמות מדיניות של "ענן תחילה", עוזרת להניע את הצמיחה של שוק תשתיות הענן הבודד באירופה וביסוס יעדי הצמיחה של השוק היחיד הדיגיטלי (DSM).

מדריך זה נועד לספק הנחיות ותמיכה מועילות לרשויות ציבוריות בעת רכישת שירותי ענן.

מידע נוסף

חברי CISPE: <https://cispe.cloud/members>

מועצת המנהלים: <https://cispe.cloud/board-of-directors>

שירותי מחשוב ענן המוצהרים תחת קוד ההתנהגות של CISPE: <https://www.codeofconduct.cloud/public-register/>

תוכן העניינים

2	הודעות	
3	מידע על CISPE	
5	תוכן העניינים	
1	סיכום ומטרת מדריך זה	
3	1.0 סקירה כללית של הסכם מסגרת לטכנולוגיית ענן	
6	2.0 סקירת RFP לרכישת שירותי ענן	
6	2.1 הגדרת RFP לרכישת שירותי ענן	
6	2.1.1 מבוא ויעדים אסטרטגיים	
8	2.1.2 ציר זמן של תגובה ל-RFP	
9	2.1.3 הגדרות	
10	2.1.4 תיאור מפורט של מודל הקנייה והתחרות במסגרת הסכם המסגרת	
13	2.1.5 דרישות מינימום למשתתף במכרז - מנהלתי	
15	2.2 טכני	
15	2.2.1 דרישות מינימום	
18	2.2.2 השוואה בין ספקים	
19	2.2.3 התקשרות בחוזה	
20	2.3 אבטחה	
21	2.3.1 דרישות מינימום	
25	2.3.2 השוואה בין ספקים	
25	2.3.3 התקשרות בחוזה	
26	2.4 תמחור	
26	2.4.1 דרישות מינימום	
27	2.4.2 השוואה בין ספקים	
29	2.5 הגדרות ביצוע חוזה/תנאים והגבלות	
29	2.5.1 תנאים והתניות	
31	2.5.2 תנאים והגבלות של תוכנה	
32	2.5.3 איך לבחור בין זוכי מענקים לפי פרויקט	
33	2.5.4 הצטרפות ועזיבה	
34	3.0 שיטות עבודה מומלצות/לקחים שנלמדו	
34	3.1 משילות בענן	
34	3.2 תקצוב בענן	
36	3.3 הבנת המודל העסקי של שותפים	
36	3.4 מתווכי ענן	
36	3.5 איסוף מידע טרום-RFP/תחקיר שוק	
36	3.6 קיימות	
38	נספח א' - דרישות טכניות להשוואה בין משתתפים במכרז	
38	1. פרופיל ספק הענן	
38	2. תשתית גלובלית	
39	3. תשתית	
39	3.1 מחשוב	

42	3.2 עבודה ברשת
45	3.3 אחסון
49	4. אדמיניסטרציה
49	5. אבטחה
51	6. תאימות
55	7. העברות
57	8. חיוב
58	9. ניהול
59	10. תמיכה
61	נספח ב' - הערכה טכנית חיה
62	פלטפורמה - הערכה טכנית חיה לדוגמה
69	עומס עבודה: יישום אינטרנט - הערכה טכנית חיה לדוגמה

סיכום ומטרת מדריך זה

מטרת **מדריך זה לרכישת שירותי ענן** היא לספק הנחיות לאותם לקוחות ענן המעוניינים לרכוש שירותי ענן באמצעות תהליך רכש תחרותי (בקשה לקבלת הצעות (RFP) לרכישת שירותי ענן), אך חסרים את המומחיות לנסח הסכם מסגרת לטכנולוגיית ענן.

מסמך זה מסופק למטרות מידע בלבד. הוא לא פותח בהתאם לדרישות החוק לתהליכי רכש ציבורי באזור או מדינה מסוימים.

המדריך בוחן גם שפת קריטריוני בחירה נוספים עבור **חוזים מרוכזים** או **תחרויות זעירות** בעת רכישה מתוך הסכם מסגרת לטכנולוגיית ענן. כל סעיפיו של המדריך מאורגנים כך שהם מדמים RFP כללי של IT. נוסח כללי של RFP וקריטריונים לבחירה מלווה בפרשנות שתסייע להבין מדוע RFP ענן שונה מ-RFP מסורתי של IT.

לאחר פרסום אסטרטגיית הענן של נציבות האיחוד האירופי המנחה כיצד הסוכנויות והמוסדות האירופיים יהפכו את תשתיות ה-IT שלהם למודרניות באמצעות גישה של ענן תחילה, העבירה CISPE את המדריך לנציבות האיחוד האירופי ביולי 2019 במהלך האירוע 'כיצד לשנות ממשלות באמצעות מדיניות ענן חכמה'.



גרסה 2 של מדריך זה כוללת הנחיות חדשות לגבי; הגנת נתונים (סעיף 2.3.1.1), החלפת ספקי ענן והעברת נתונים (סעיף 2.3.1.2), תנאים והגבלות של התוכנה (סעיף 2.5.2), קיימות בענן (סעיף 3.6), ונספח ב' מחודש של הערכה טכנית חיה.

'שירותי ענן' מתייחס לכל טכנולוגיות הענן והשירותים הנלווים שמשתמש קצה עשוי להזדקק לגישה אליהם. זה כולל שירותי ייעוץ או שירותים מקצועיים/מנהלים לצורך תמיכה וביצוע העברה לענן ותמיכה בעומסי עבודה בענן, בנוסף לתשתית הענן עצמה, ושירותי פלטפורמת רכישת רישיונות ענן כגון מוצרי תוכנה כשירות (SaaS).

הופעתו של מחשוב ענן כברירת המחדל עבור IT במגזר הציבורי מהווה הזדמנות למודרניזציה של אסטרטגיות רכש קיימות. תהליכי רכישה ממוקדי ענן יכולים לאפשר לגופים במגזר הציבורי להפיק את מלוא היתרונות של הענן, כגון גישה לחדשנות מובילה, הגברת המהירות והזריזות, שיפור עמדת האבטחה וניהול התאימות - תוך מימוש היעילות וחסכון בעלויות.

שיטות רכש IT מסורתיות לקניית חומרה, תוכנה ומרכזי נתונים אינן מתורגמות לקניית שירותי ענן. גישות לתמחור, ניהול חוזים, תנאים והגבלות, אבטחה, דרישות טכניות, SLAs ועוד משתנות במודל ענן, ושימוש בשיטות רכש קיימות מפחית או מבטל בסופו של דבר את היתרונות שהענן מספק.

אחד האמצעים הטובים ביותר לרכישה אפקטיבית של שירותי ענן במגזר הציבורי הוא באמצעות **הסכם מסגרת לטכנולוגיית ענן** -מענק של תפריט עננים לאורגנים רבים, ממנו יכולים רוכשים זכאים המזוהים עם ארגון הרכישה לרכוש טכנולוגיות ענן ושירותים נלווים שעונים על צורכיהם ומתאימים להם. ככלי רכישה של חוזי ענן, הסכמי מסגרת כאלה מאפשרים רכישת שירותי ענן בצורה יעילה ואפקטיבית - מה שמביא לכך שארגוני רכש וגופי משתמשי קצה מקבלים גישה למגוון שלם של שירותי ענן, ובסופו של דבר קוטפים את מלוא היתרונות של הענן: זריזות וגמישות, תועלת מיתרונות מסיביים של סקייל, מדרגיות כדי להגיע לזמינות טובה יותר בעלות נמוכה יותר, רוחב הפונקציונליות, קצב החדשנות, קיבולת הרחבה לגאוגרפיות חדשות.

שימו לב שמאמר זה מתמקד בטכנולוגיות ענן לרכישת תשתית כשירות (IaaS) ופלטפורמה כשירות (PaaS), כפי שמסופקות על ידי ספק שירותי תשתיות ענן (CISP). ניתן לרכוש טכנולוגיות ענן כאלה ישירות מ-CISP, או דרך מפיץ CISP. שיקולי RFP נוספים יידרשו עבור מפיצים של שירותי פלטפורמת רכישת רישיונות ענן (SaaS ו-PaaS), ושירותי ייעוץ בענן.

שימו לב גם שמאמר זה אינו מכסה כל היבט של יצירת מסגרת רכש ענן מקצה לקצה. ישנם מסמכים רבים אחרים מהתעשייה ומאנליסטים המכסים נושאים כמו שיטות עבודה מומלצות לרכש בענן, כיצד לתקצב ענן, ניהול בענן וכו', ואנחנו ממליצים בחום לקחת בחשבון עצות ומאמרים כאלה בעת פיתוח אסטרטגיית רכש כוללת בענן.

טבלה 1 להלן מספקת מתווה של מדריך RFP לרכישת שירותי ענן, והיכן ממוקמת שפת RFP לדוגמה עבור כל רכיב RFP לרכישת שירותי ענן.

טבלה 1 - סיכום של סעיפי מדריך RFP לרכישת שירותי ענן

סעיף	סקירה כללית ודוגמה לשפת RFP
1.0 סקירה כללית של הסכם מסגרת לטכנולוגיית ענן	תצוגה ברמה גבוהה של מודל הסכם המסגרת לטכנולוגיית ענן (חלקות (LOT), כיצד להתחרות והתקשרות)
2.0 סקירת RFP לרכישת שירותי ענן	דוגמה לשפת RFP גנרית המכסה את הסעיפים שלהלן, יחד עם פרשנות המסבירה את הרציונל מאחורי מבנה ה-RFP לרכישת שירותי ענן והשפה שבה משתמשים
2.1 הגדרת RFP לרכישת שירותי ענן	2.1.1 מבוא ויעדים אסטרטגיים 2.1.2 ציר זמן של תגובה ל-RFP 2.1.3 הגדרות 2.1.4 תיאור מפורט של מודל הקנייה והתחרות במסגרת הסכם המסגרת 2.1.5 דרישות מינימום למשתתף במכרז - מנהלתי
2.2 טכני	2.2.1 דרישות מינימום 2.2.2 השוואה בין ספקים 2.2.3 התקשרות בחוזה
2.3 אבטחה	2.3.1 דרישות מינימום 2.3.1.1 הגנה על נתונים 2.3.1.2 החלפת ספקי ענן והעברת נתונים 2.3.2 השוואה בין ספקים 2.3.3 התקשרות בחוזה
2.4 תמחור	2.4.1 דרישות מינימום 2.4.2 השוואה בין ספקים
2.5 הגדרות ביצוע חוזה/תנאים והגבלות	2.5.1 תנאים והתניות 2.5.2 תנאים והגבלות של התוכנה 2.5.3 איך לבחור בין זוכי מענקים 2.5.4 הצטרפות ועזיבה
3.0 שיטות עבודה מומלצות/לקחים שנלמדו	3.1 ניהול בענן 3.2 תקצוב בענן 3.3 הבנת המודל העסקי של שותפים 3.4 מתווכי ענן 3.5 איסוף מידע טרום-RFP/תחקיר שוק 3.6 קיימות
נספח א' - דרישות טכניות להשוואה בין משתתפים במכרז	רשימה של דרישות טכנולוגיות ענן גנריות עבור חוזים מרוכזים או תחרויות זעירות
נספח ב' - הערכה טכנית חיה	סקריפט לדוגמה למוצר טכנולוגיית ענן המדגים ניקוד (הדגמות ענן כחלק מחוזה מרוכז או תחרות זעירה)

1.0 סקירה כללית של הסכם מסגרת לטכנולוגיית ענן

הסכם מסגרת לטכנולוגיית ענן מעוצב היטב יכול לאפשר רכישת שירותי ענן באופן שיועיל הן לארגוני המגזר הציבורי המשתתפים והן לספקי הענן. היתרונות של הסכם מסגרת מנוסח היטב לטכנולוגיית ענן כוללים:

• שיתוף פעולה בפועל:

- הכוונה היא לארגונים מרובים המתאגדים יחד כדי לבצע הזמנות עבור דרישות דומות ובכך מקבלים נוחות, יעילות, עלויות מופחתות, כמו גם תהליך הזמנה פשוט יותר. שיתוף הפעולה בפועל מבסס דרך יעילה לצבור ביקוש של מספר רב של ארגונים במגזר הציבורי לטכנולוגיות ענן נפוצות ולשירותי ענן נלווים כגון פתרונות מסוג Marketplace וייעוץ.

• מגוון מלא של שירותי ענן:

- אלה יכולים לכלול את כל שירותי הייעוץ, השירותים המקצועיים או השירותים המנוהלים הדרושים לתמיכה מלאה ולביצוע ההעברה לענן ואת עומסי העבודה התומכים בענן, בנוסף לטכנולוגיות ענן שסופקו על ידי CISP וכן שירותי Marketplace.
- ניתן לרכוש טכנולוגיות ענן כאלה ישירות מ-CISP, או דרך מפיץ מורשה.

• ניהול חוזים:

- מאחד ארגונים/רוכשים שונים סביב מערכת תנאים והגבלות משותפת ומענק חוזה אב יחיד, במקום חוזים שונים עבור כל ארגון.
- ניהול חוזים גם מועיל לספקים מכיוון שהוא מספק תהליך רכישה סטנדרטי, תנאים והגבלות, ומנגנון הזמנה לניווט במקום תהליכים שונים לכל ארגון במגזר הציבורי.
- הוא מספק גמישות. יצירה, אישור והרצה של חוזה ענן יעיל במסגרת מדיניות/תקנות ממשלתיות קיימות דורשות ניסוי ויכולת התאמה מהירה. מועיל יותר ליצור הסכם מסגרת המאפשר למגזר הציבורי ולספקי הענן לעבוד יחד כדי לשפר את החוזה - מבחינה חוזית, מכנית ויעילות. חוזה רב שנתי שאינו עובד ואינו ניתן להתאמה מוביל לחוויה גרועה עבור משתמשי קצה במגזר הציבורי, ארגוני רכש וספקי ענן

• בחירה:

- מאפשרת לרוכשים לבחור בין מספר CISPs מוסמכים, ומציבה רף גבוה לכל שירותי הענן והשירותים הנלווים כגון פלטפורמת רכישת רישיונות בענן כגון PaaS/SaaS וכן ייעוץ בענן.
- היא מאפשרת שליטה על מספר הספקים במסגרת באמצעות הבטחה שהסטנדרט של כל זוכה במענק נבדק כראוי.

הסכם מסגרת לרכישת שירותי ענן עובד בצורה הטובה ביותר כאשר הוא כולל טכנולוגיות ליבה של IaaS/PaaS המסופקות על ידי CISP, יחד עם Marketplace מסוג PaaS/SaaS, ושירותי הייעוץ שמשתמשי הקצה במגזר הציבורי יכולים לגשת אליהם, בעת הצורך, כדי לעזור להם לתכנן, להעביר, לנצל ולתחזק עומס עבודה הפועל בענן. לפיכך, אנחנו מציעים ל-RFP לרכישת שירותי ענן להגדיר הסכם מסגרת לטכנולוגיית ענן שיחולק ל-3 חלקות כמפורט להלן:

• חלקה 1 - טכנולוגיות ענן

רכישת טכנולוגיות ענן כאלה ישירות מ-CISP, או דרך מפיץ CISP מורשה.

• חלקה 2 – MARKETPLACE

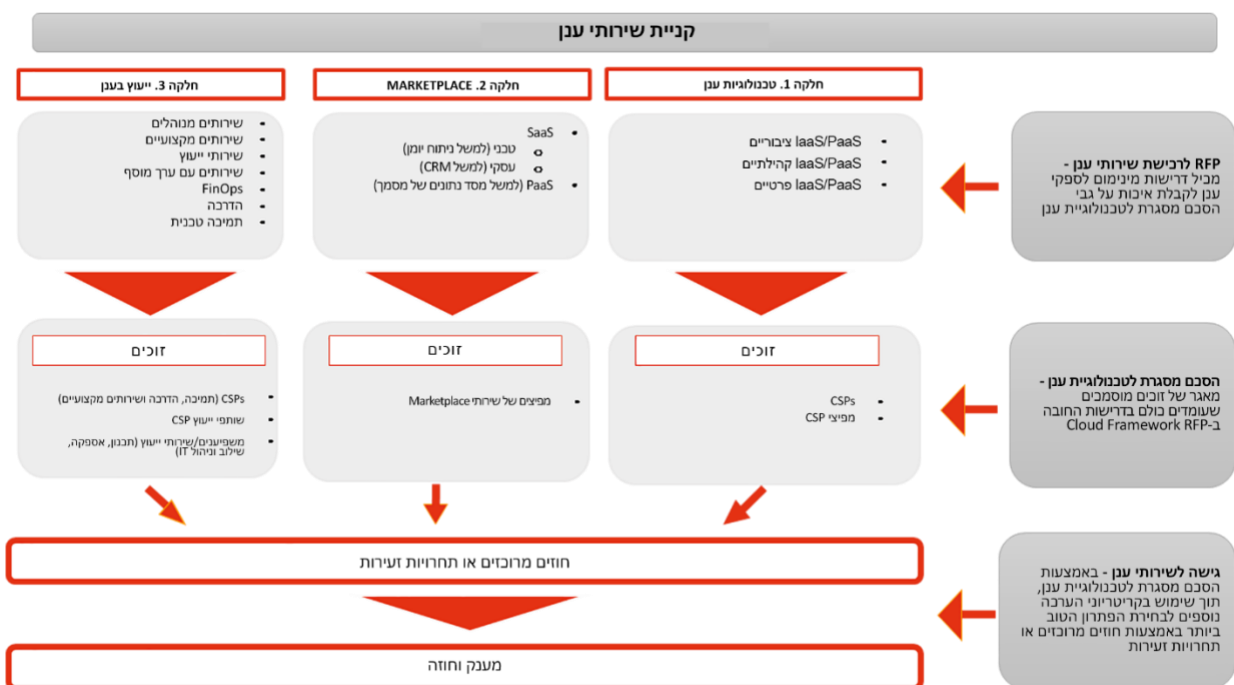
גישה ל-Marketplace של שירותי PaaS ו-SaaS.

• חלקה 3 - ייעוץ בענן

שירותי ייעוץ בנושא ענן (הדרכה, שירותים מקצועיים, שירותים מנוהלים ועוד) ותמיכה טכנית.

כפי שצוין קודם לכן, מאמר זה מתמקד ברכישת טכנולוגיות ענן IaaS ו-PaaS (חלקה 1) כפי שסופקו על ידי CISP (נרכשו ישירות מ-CISP, או דרך מפיץ CISP). דרישות הסמכה נפרדות של ספקים יהיו נחוצות עבור ספקים בחלקות 2 ו-3 של RFP לרכישת שירותי ענן.

איור 1 להלן מסופקת תצוגה ברמה גבוהה של האופן שבו RFP לרכישת שירותי ענן מובנה היטב, המחולק לשלוש החלקות הללו, יכול להוביל להסכם מסגרת לטכנולוגיית ענן המספק זריזות וגמישות לגופים במגזר הציבורי (מבחינה טכנית וחוזית), נראות ושליטה של הוצאות ושימוש בענן, יחד עם היכולת לקבל את כל שירותי הענן הדרושים כדי לבנות ולתחזק את הפתרונות שהם צריכים.



איור 1 - RFP לרכישת שירותי ענן מוצלחים מופרד ל-3 חלקות. כל חלקה מכילה קטגוריות או 'סוגי הצעה' תחת החלקה המתאימה, כדי להבטיח התאמה טכנית וחוזית המיועדת לעמוד בדרישות משתמש הקצה בעת רכישה מחוץ להסכם המסגרת לטכנולוגיית ענן.

לתשומת לבך:

- כל חלקה מוענקת למספר ספקים.
- ניתן להעניק את חלקה 3 באמצעות RFP אחר, או אולי באמצעות חוזה קיים לשירותי ייעוץ.

חלקה 1 קטגוריות

הסכמי מסגרת לטכנולוגיית ענן מוצלחים מבקשים מ-CSPs לתאר את מודל הענן שהם מציעים, מופרדים לקטגוריות מתחת לכל חלקה. אנחנו ממליצים להשתמש בתקן התעשייה עבור מחשוב ענן ([המכון הלאומי לתקנים וטכנולוגיה](#) [\(\(NIST\) Essential Cloud Characteristics](#)) - לקביעת ההגדרות של ענן **ציבורי**, ענן **קהילתי** וענן **פרטי**. בניית הסכם מסגרת לטכנולוגיית ענן בדרך זו מאפשרת לסוכנות הרכש ולגופים הציבוריים המשתמשים במסגרת לבחור מתוך מגוון דגמי ענן שיתאימו לצורכיהם.

ניתן לעיין בסעיף 2.1.3 הגדרות להגדרת ה-NIST של כל מודל ענן תחת חלקה 1 (Public IaaS/PaaS, Private IaaS/PaaS ו-Community IaaS/PaaS).

איך להתחרות - חוזים מרוכזים או תחרויות זעירות?

קריטריוני ההסמכה עבור RFP לרכישת שירותי ענן צריכים לכסות אלמנטים קריטיים ותקני מינימום ואינם יכולים לכלול תקנים של "טוב שיש". הוספת תקנים נוספים מעל קו הבסיס עבור ספקים המתאימים למסגרת יכולה להוביל לכך שספקים מסוימים לא יוכלו להשתתף במכרזים, ובסופו של דבר תינתן פחות בחירה לרוכשים.

בעקבות ה-RFP וההגדרה שלאחר מכן של הסכם מסגרת לטכנולוגיית הענן, גופים במגזר הציבורי שהם צד למסגרת יכולים להזמין או 'לערוך חוזה מרוכז' לשירותי הענן הדרושים להם בעת הצורך. הצבת חוזה מרוכז במסגרת הסכם מסגרת מאפשרת ללקוחות לחדד דרישות עם מפרט פונקציונלי נוסף לחוזים מרוכזים, תוך שמירה על ההטבות המוצעות במסגרת הסכם המסגרת.

במידת הצורך, ניתן לקיים תחרות זעירה לאיתור הספק הטוב ביותר עבור עומס עבודה או פרויקט מסוים. תחרות זעירה היא המקום שבו לקוח הולך לתחרות נוספת במסגרת הסכם המסגרת, על ידי הזמנת כל הספקים בתוך החלקה להיענות למערכת של דרישות. הלקוח יזמין את כל הספקים המתאימים בתוך החלקה להשתתף במכרז, ומכאן החשיבות של דרישות המינימום למקבלי מענקים על RFP לרכישת שירותי ענן - מכיוון שהן מבטיחות סטנדרט גבוה של אפשרויות בכל חלקה.

יש לשים לב שחשוב שיהיו **סטים נפרדים של תנאים והגבלות** של חוזה עבור כל אחת מהחלקות, כפי שמופיע באיור 1 לעיל. עבור כל החלקות - "גישת מידה אחת מתאימה לכולם" להתקשרות תוביל לבעיות סביב היתכנות טכנית ותאימות.

2.0 סקירת RFP לרכישת שירותי ענן

סעיף זה מתאר את המודל וההיקף של RFP לרכישת שירותי ענן, כולל: יעדים אסטרטגיים, משתתפים, הגדרות, ציר זמן ודרישות מינימום ניהוליות. שוב, נציין שהמוקד של מדריך זה הוא **חלקה 1 - טכנולוגיות ענן**.

2.1 הגדרת RFP לרכישת שירותי ענן

אנחנו ממליצים בחום לגופים במגזר הציבורי להיות ברורים לגבי היעדים והדרישות הגבוהות שלהם במבוא של RFP לרכישת שירותי ענן.

2.1.1 מבוא ויעדים אסטרטגיים

במבוא של RFP לרכישת שירותי ענן, אם רוצים לשרטט באופן ברור יעדים אסטרטגיים, שיטת העבודה המיטבית היא; (1) להגדיר מהם היעדים העסקיים והתועלת שהארגון מבקש להשיג באמצעות שימוש בענן; (2) להגדיר את מבנה הסכם המסגרת – מי קונה, מי מפעיל, מי מתקצב וכו'; (3) להבין באופן ברור את מודל האחריות המשותפת בין המגזר הציבורי לספקי הענן, שמהווה את הליבה של רכישה ושימוש מוצלחים בענן, ו-(4) להגדיר את סוג הקשר שנוצר בין ספקי שירותי ענן (CISPs), מפיצים של שירותי פלטפורמה לרכישת רישיונות דיגיטלית, שותפי ייעוץ, סוכנויות רכש/סוכנויות קבלניות לבין משתמשי קצה ממשלתיים. ניסוח ארבע הנקודות הללו מסייע לארגונים לפתח RFP העונה בצורה הטובה ביותר לצורכיהם, ובנוסף להבטיח שהלקוחות והספקים יהיו ברורים לגבי תוצרי ה-RFP.

RFP בענן שונה בכונה מה-RFP המסורתית של IT. טכנולוגיית הענן אינה רק תחליף דומה לשיטות מחשוב מסורתיות - היא מציגה דרך חדשה לחלוטין לצרוך טכנולוגיה. RFPs לרכישת שירותי ענן שמעוצבים היטב יכולים לעזור לגופים במגזר הציבורי לנוע במהירות כדי לנצל את היתרון של הענן.

הבנה ברורה של מודל האחריות המשותפת היא אולי נקודת ההתחלה הטובה ביותר מכל ההיבטים של רכישת ענן שאנחנו מציינים כשיטת עבודה מיטבית. משתמשים במודל האחריות המשותפת¹ בעיקר כאשר דנים באבטחה ותאימות בענן, אך מתווה זה של תחומי אחריות חל על כל ההיבטים של טכנולוגיות הענן. כל מה שבמסגרת התפקיד של ה-CISP בסביבת ענן וכל מה שיישאר במסגרת אחריות לקוח צריך להיות ברור ומוגדר ב-RFP לרכישת שירותי ענן. לדוגמה, CISP מספק יכולות לניטור משאבים ויישומים הפועלים בענן, אך באחריות הלקוח להשתמש בפועל ביכולות האלה שסופקו על ידי ה-CISP – זאת מכיוון ש-CISP הפועל בסקייל מסיבי לא תוכנן לבצע זאת עבור מיליוני לקוחות.

יתרה מכך, לקוחות ענן צריכים להבין כיצד רשת השותפים של CISP עוזרת ללקוחות להשתמש בענן ולנהל את תחומי האחריות שלהם. לדוגמה, ספק שירות מנוהל בענן (MSP) יכול לעזור ללקוח להגדיר ולהשתמש ביכולות ניטור שסופקו על ידי CISP כדי לעמוד בדרישות התאימות והביקורת הייחודיות שלו.

במילים פשוטות, תחומי האחריות במודל הענן הם:

CISP מספק טכנולוגיית ענן

לקוח משתמש בטכנולוגיית ענן

חברות ייעוץ (אם רלוונטי) עוזרות ללקוח לגשת ולנצל את טכנולוגיית הענן

¹ יש לעיין בסעיף 5 של קוד ההתנהגות לספקי תשתית שירותי ענן של CISPE:

https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

'חברות ייעוץ' הן חברות ייעוץ ושירותים מנוהלים/מקצועיים המסייעות ללקוחות לעצב, לתכנן אדריכלית, לבנות, להעביר ולנהל את עומסי העבודה והיישומים שלהם בענן. חברות כאלה כוללות משלבי מערכות, חברות ייעוץ אסטרטגי, סוכנויות, ספקי שירותים מנוהלים ומפיצים בעלי ערך מוסף.

אם חושבים למשל על "קניות" של שירותי ענן כאנלוגיות לקניות בחנות לחומרי בניין. קיים מגוון עצום של חומרים וכלים לבנייה בחנות לחומרי בניין. ניתן לבנות ארון או בריכת שחייה, או בית שלם, הבחירה בידך. כשקונים את החומרים והכלים, הצוות בחנות לחומרי הבניין יכול לספק הדרכה ומומחיות, אבל הם לא באים אליך ובונים עבורך. לכן, יש לך כמה אפשרויות:

1. לרכוש בעצמך את החומרים והכלים ולבנות משהו בעצמך.
2. לרכוש את החומרים והכלים בעצמך, ולשכור מישהו לבנות ו/או לתפעל משהו עבורך.
3. לשכור מישהו לבנות/לתפעל משהו עבורך, ושהוא ירכוש את החומרים והכלים כחלק מהצעה כוללת.

אם לארגון יש אנשים עם הכישורים המתאימים לבנות ולנהל את סביבת הענן והפתרונות של הארגון בעצמם, כל מה שנשאר הוא לקבל גישה מה-CISP לטכנולוגיות ולכלי הענן המתקדמים (שירות עם CISP, או דרך מפיץ CISP - יש לעיין בחלקה 1). תוכנות SaaS ו-PaaS הדרושות צריכות להיות זמינות בפלטפורמת רכישת הרישיונות הדיגיטלית בענן (חלקה 2). אם יש צורך בסיוע נוסף בייעוץ, העברה, הטמעה ו/או ניהול, כאן נכנסת לתמונה רשת שותפים של CISP (חלקה 3).

שפת RFP לדוגמה: מבוא ויעדים אסטרטגיים

מחשוב ענן מספק לארגונים במגזר הציבורי גישה מהירה למגוון רחב של משאבי IT גמישים ובעלות נמוכה, כשהתשלום הוא לפי שימוש. ארגונים יכולים להקצות את הסוג והגודל הנכונים של המשאבים הדרושים להם כדי להפעיל את הרעיונות המצוינים החדשים ביותר שלהם או כדי להפעיל את מחלקות ה-IT שלהם, ובכך לבטל את הצורך בהשקעות גדולות בחומרה ו/או בחוזי רישוי תוכנה לטווח ארוך.

דרישה אחת של ה-**ארגון** היא לקבל גישה לסוגים אלה של טכנולוגיות ענן זמינות מסחרית כדי לענות על הצרכים העסקיים שלו על פני קשת רחבה של ארגונים קשורים.

המטרה העיקרית של RFP זה היא להעניק **הסכם מסגרת** מקביל לא בלעדי עם עד **3** ספקים המייצגים טכנולוגיות ענן שונות ושירותים הקשורים לענן.

1. **חלקה 1.** ספקי שירותי ענן (CISPs) או מפיצי CISP לרכישת טכנולוגיות ענן
2. **חלקה 2.** ספקים של שירותי פלטפורמה דיגיטלית לרכישת רישיונות
3. **חלקה 3.** ספקי שירותי ייעוץ שנועדו לספק מומחיות נוספת לצורך מעבר אל הצעות ה-CISP האלו והשימוש בהן

בהתייחס **לחלקה 1**, ארגונים המשתתפים במכרזים (CISPs או מפיצי CISP) חייבים להדגים כיצד ההצעה שלהם תעמוד ביעדים הבאים:

- **זריזות** - הפיכת משאבי IT לזמינים למשתמשי הקצה תוך דקות במקום לוחות הזמנים המסורתיים של שבועות וחודשים.
- **חדשנות** - גישה מיידית לטכנולוגיה החדשה והחדשנית ביותר בשוק.
- **עלות** - הוצאות הון סחר עבור הוצאה משתנה (למשל: CapEx ל-OpEx). משלמים רק על מה שנצרך.
- **תקצוב** - הצגת מידע על חיוב ושימוש הן ברמת פירוט והן ברמת סיכום, הדמיית דפוסי הוצאות לאורך זמן, בנוסף לחיזוי הוצאות עתידיות.
- **אלסטיות** - השגת עלויות משתנות נמוכות יותר הודות ליתרונות הגודל הכבירים שמספק הענן.
- **קיבולת** - ביטול הצורך בניחושים בכל הנוגע לצורכי קיבולת תשתית.

- **הפסקת ההסתמכות על מרכזי נתונים** - התמקדות בעסק של האזרחים שלנו, במקום להסתמך על העבודה הקשה של סידור במדפים, הערמה והפעלה של שרתים.
- **אבטחה** - הפיכת עיצוב החשבון לרשמי עם יכולות נראות וביקורת גבוהות יותר של משאבים, וביטול עלות ההגנה על מתקנים וחומרה פיזית.
- **אחריות משותפת** - הפחתת עומס תפעולי כאשר ה-CISP פועל, מנהל ושולט ברכיבים ממערכת ההפעלה המארכת ומשכבת הווירטואליזציה ועד לאבטחה הפיזית של המתקנים שבהם השירות פועל.
- **אוטומציה** - אוטומציה מובנית בארכיטקטורת הענן נועדה לשפר את היכולת לבצע סקיל בצורה מאובטחת במהירות רבה יותר ותוך חיסכון בעלויות.
- **ניהול בענן** - (1) יש להתחיל עם מלאי מלא של כל נכסי ה-IT, (2) לנהל את כל הנכסים הללו באופן מרכזי; וכן (3) ליצור התראות לגבי שימוש/חיוב/אבטחה/וכו'. - והכל יחד עם יכולות למעקב אחר נכסים, ניהול מלאי, ניהול שינויים, ניהול וניתוח יומנים, וכן נראות כללית וניהול בענן.
- **שליטה** - השגת נראות מלאה של האופן שבו שירותי IT נצרכים, והיכן ניתן לכוון אותם לצורך אבטחה, אמינות, ביצועים ועלות.
- **תהליך הפוך** - כלים ושירותי נידות שסייעו במעבר אל תשתית ה-CISP וממנה, תוך מזעור נעילה של ספקים וכיבוד כללי ההתנהלות של התעשייה.
- **הגנה על נתונים** - יכולת להוכיח תאימות עם האסדרה הכללית להגנה על מידע (GDPR), באמצעות קוד התנהגות ייעודי בתעשייה עבור שירותי תשתית ענן: קוד ההתנהגות של CISPE להגנה על נתונים.
- **שקיפות** - לקוחות צריכים להיות זכאים לדעת את מיקומן של תשתיות המשמשות לעיבוד ואחסון הנתונים שלהם (אזור העיר).
- **ניטרליות אקלימית** - לקוחות צריכים לתקשר עם CISP הנוקטים צעדים מוכחים וספציפיים כדי לעמוד ביעדי ניטרליות אקלימית עד 2030, וחתומים על הסכם מרכז הנתונים לניטרליות אקלימית. זה יעזור ללקוחות לעמוד ביעדי הניטרליות האקלימית שלהם.

2.1.2 ציר זמן של תגובה ל-RFP

שיטת עבודה מיטבית היא לספק למשתתפים במכרז ציר זמן של פעילות מכרזים צפויה בעת יצירת הסכם מסגרת ענן, ואת ה-RFP לרכישת שירותי ענן הקשור. ככל שתהיה יותר מעורבות עם התעשייה כך ייטב, שכן זה יעזור להבטיח שקיימת הבנה ברורה של כל הצדדים לגבי דרישות ה-RFP, וכמובן גם לגבי האופן שבו כל שירותי הספק משתלבים במודל שירותי הענן.

יש לשים לב שציר הזמן של RFP כפוף לחוקים המקומיים ולמחויבויות המשפטיות, והרשימה המופיעה להלן נועדה לשמש כמדריך לשיטות עבודה מומלצות, בניגוד לרשימה מנחה של פעילויות ומסגרות זמן.

שפת RFP לדוגמה: ציר זמן לתגובה

יש לעיין בציר הזמן של RFP שלהלן עבור RFP לרכישת שירותי ענן:

ציר הזמן של RFP לרכישת שירותי ענן	
•	היתר בקשה למידע (RFI):
•	תגובת RFI:
•	היתר טיוטת בקשה להצעה (RFP):
•	מועד הגשת טיוטה של תגובת RFP:
•	שלב הייעוץ בתעשייה: <ציר זמן>
•	היתר RFP לקדם-הסמכה:
•	תגובת RFP לקדם-הסמכה:
•	היתר RFP:

- סיבוב 1 מועד לשאלות:
- סיבוב 1 תשובות:
- סיבוב 2 מועד לשאלות:
- סיבוב 2 תשובות:
- מועד לתגובת RFP:
- תקופת בירור ההצעה:
- תקופת המו"מ:
- תאריך להענקת:
- מענק חוזה:
- משך החוזה (אפשרויות להארכה):

יש לשים לב שציר הזמן של RFP כפוף לחוקים המקומיים ולמחויבויות המשפטיות, והרשימה המופיעה להלן נועדה לשמש כמדריך לשיטות עבודה מומלצות, בניגוד לרשימה מנחה של פעילויות ומסגרות זמן.

2.1.3 הגדרות

RFP לרכישת שירותי ענן צריך לכלול רשימה מפורטת של הגדרות. רשימה זו כוללת תפקידי ספקים (למשל, ספק שירותי ענן, מפיץ ענן, שותף ספק), מושגים טכנולוגיים כלליים (מחשוב, אחסון, SaaS, PaaS, IaaS) וחלקי מפתח אחרים בהסכם. להלן רשימת הגדרות לדוגמה:

שפת RFP לדוגמה: הגדרות

ההגדרות שלהלן הן הגדרות מחשוב ענן של המכון הלאומי לתקנים וטכנולוגיה (NIST).²

- **תשתית כשירות (IaaS).** היכולת המסופקת לצרכן היא להקצות עיבוד, אחסון, רשתות ומשאבי מחשוב בסיסיים אחרים שבהם הצרכן מסוגל לפרוס ולהריץ תוכנות שרירותיות, שיכולות לכלול מערכות הפעלה ויישומים. הצרכן אינו מנהל את תשתית הענן הבסיסית או שולט בה, אך יש לו שליטה על מערכות ההפעלה, האחסון והיישומים הפרוסים; ואולי שליטה מוגבלת ברכיבי רשת נבחרים (למשל, חומות אש של מארח).
- **פלטפורמה כשירות (PaaS).** היכולת הניתנת לצרכן היא לפרוס על תשתית הענן יישומים שנוצרו או נרכשו על ידי הצרכן. יישומים שנוצרו באמצעות שפות תכנות, ספריות, שירותים וכלים הנתמכים על ידי הספק. הצרכן אינו מנהל את תשתית הענן הבסיסית או שולט בה, לרבות רשת, שרתים, מערכות הפעלה או אחסון, אך יש לו שליטה על היישומים הפרוסים ואולי על הגדרות התצורה של סביבת אירוח היישומים.
- **תוכנה כשירות (SaaS).** היכולת הניתנת לצרכן היא להשתמש ביישומי הספק הפועלים על תשתית ענן. היישומים נגישים ממכשירי לקוח שונים באמצעות ממשק לקוח דק, כגון דפדפן אינטרנט (למשל, דואר אלקטרוני מבוסס אינטרנט), או ממשק תוכנית. הצרכן אינו מנהל את תשתית הענן הבסיסית או שולט בה, לרבות רשת, שרתים, מערכות הפעלה, אחסון, או אפילו יכולות יישום בודדות, למעט הגדרות מוגבלות של הגדרות יישום ספציפיות למשתמש.
- **ענן ציבורי.** תשתית הענן מוקצית לשימוש פתוח על ידי הציבור הרחב. הענן יכול להיות בבעלות ארגון עסקי, אקדמי או ממשלתי, או שילוב כלשהו שלהם, ומנוהל ומופעל על ידם. והוא קיים בשטחו של ספק הענן.
- **ענן קהילתי.** תשתית הענן מוקצית לשימוש בלעדי על ידי קהילה ספציפית של צרכנים מארגונים שיש להם חששות משותפים (למשל, שיקולי משימה, דרישות אבטחה, מדיניות ותאימות). הוא עשוי להיות בבעלות אחד או יותר מהארגונים בקהילה, צד שלישי, או שילוב כלשהו שלהם ומנוהל ומופעל על ידם, והוא עשוי להתקיים בשטח או מחוצה לו.

² <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- **ענן היברידי.** תשתית הענן היא הרכב של שתי תשתיות ענן נפרדות או יותר (פרטיות, קהילתיות או ציבוריות) שנשארות כגופים ייחודיים, אך קשורות זו לזו על ידי טכנולוגיה סטנדרטית או קניינית המאפשרת ניידות נתונים ויישומים (למשל, שירותי עזר לענן לאיזון עומסים בין עננים).
- **ענן פרטי.** תשתית הענן מוקצית לשימוש בלעדי על ידי ארגון יחיד הכולל מספר צרכנים (למשל, יחידות עסקיות). הוא עשוי להיות בבעלות הארגון, צד שלישי, או שילוב כלשהו שלהם ומנוהל ומופעל על ידם, והוא עשוי להתקיים בשטח או מחוצה לו.

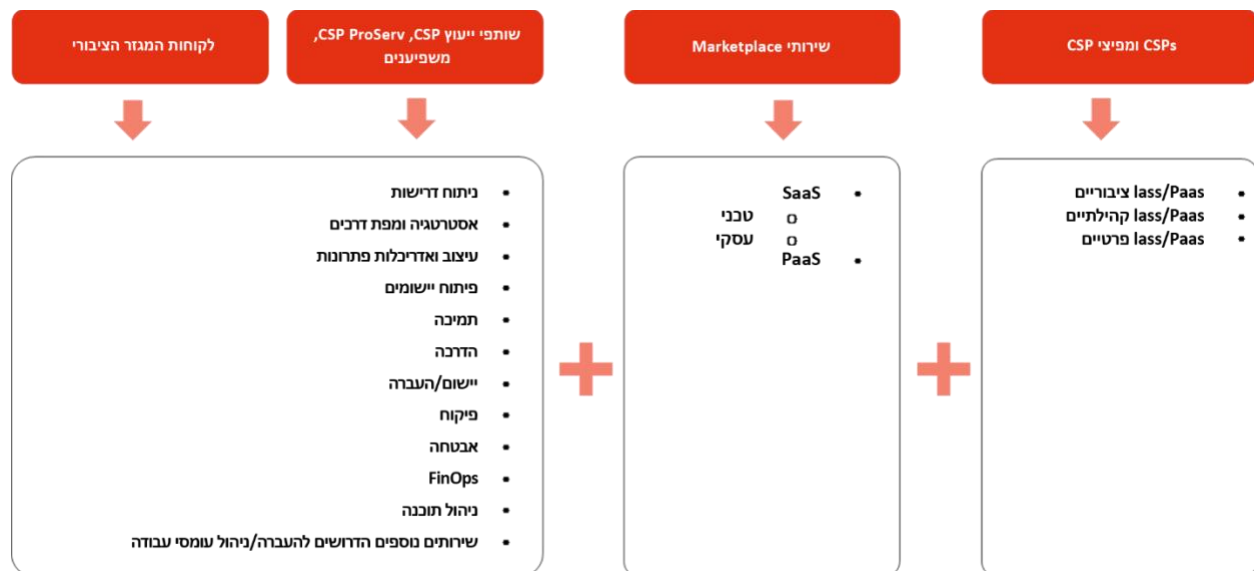
2.1.4 תיאור מפורט של מודל הקנייה והתחרות במסגרת הסכם המסגרת

כפי שצוין לעיל, ארגונים במגזר הציבורי צריכים לזהות את המודל לאופן שבו הסכם מסגרת יפעל כמנגנון קנייה של טכנולוגיות ענן, ושירותי הטמעה וניהול נלווים. יש להבהיר זאת ב-RFP לרכישת שירותי ענן כך שספקי טכנולוגיות ענן, ארגוני שירותי ייעוץ קשורים, מפיצי שוק וגופי רכישה יבינו את התפקידים שלהם.

בכל הנוגע להיקף הסכם המסגרת, ובעקבות חוזים מרוכזים או תחרויות זעירות, ארגונים צריכים לשקול:

- מי יהיה אחראי על אינטגרציה ושירותים מנוהלים הכרוכים בשימוש בטכנולוגיות הענן במסגרת החוזה.
- האם יש דרישה ממפיץ/שותף של CISP לספק שירותים בעלי ערך מוסף מלבד שמירה על מערכת יחסים חוזית עם ה-CISP, מתן שירותי חיוב מאוחדים וגישה ישירה ובזמן לנתוני שימוש וחיוב הקשורים לשימוש בשירותי ספק הענן?
- האם יש דרישה למפיץ עם ערך מוסף בשירות מלא, למשל מערכות או לספק שירותים מנוהלים, או לכל צורה של שירותי עבודה ב-IT?

חשוב לציין ש-CISP אינו משלב מערכות (SI) או ספק שירות מנוהל (MSP). לקוחות רבים מהמגזר הציבורי יצטרכו CISP עבור ה-IaaS/PaaS שלהם, ויבצעו מיקור חוץ של ייעוץ ו"עבודות מקלדת" הקשורות לתכנון, העברה וניהול למשל מערכות (SI) או לספק שירותים מנוהלים (MSP). תיאור של תיחום התפקידים והאחריות במודל שירותי ענן נמצא להלן **באיור 2**.



איור 2 - RFP לרכישת שירותי ענן צריך לספק למשתמשי הקצה תפריט של כל שירותי הענן שהם צריכים. לקוחות במגזר הציבורי ידרשו CISP עבור טכנולוגיות ענן, אם יש צורך בפלטפורמה לרכישת רישיונות למוצרי SaaS ו-PaaS. לאחר מכן הלקוח יוכל לקבוע את גודל התפקיד שהוא רוצה לקחת על עצמו באספקת שירותי ענן וכמה ברצונו להעביר למיקור חוץ כגון חברת ייעוץ/משלב מערכות/ספק שירותים מנוהלים/וכו'.

השפה לדוגמה שלהלן מעוצבת לפי התפקידים ותחומי האחריות, כפי שמוצג באיור 2 לעיל. על הסכם מסגרת לטכנולוגיית ענן RFP-ו לרכישת שירותי ענן קשורים להבטיח שהלקוחות יישארו עם היכולת להעריך כראוי את ההצעות של כל ספק, מה שיאפשר להם לבחור בין השירותים הדרושים לעומס העבודה/לפרויקט. הצורה הטובה ביותר לבצע זאת היא על ידי הפרדת שירותים לחלקות כפי שכבר הוסבר, ועל ידי כך שיהיה ברור כיצד מתנהלים חוזים מרוכזים ותחרויות זעירות במסגרת הסכם המסגרת.

שפת RFP לדוגמה: מודל רכישה

חוזת זה יישמש ככלי לרכישת **מסגרת**. הסכם מסגרת זה לטכנולוגיית ענן יכלול מספר **חלקות** כפי שהוגדרו על ידי **ארגון**, הן ישמשו עבור טכנולוגיות ענן ושירותים/מוצרים קשורים של הפלטפורמה הדיגיטלית לרכישת רישיונות, שירותי ייעוץ, שירות מקצועי/שילוב מערכות/שירותים מנוהלים/שירותי העברה מקצועיים, הדרכה ותמיכה כפי שהוגדרו על ידי **ארגון**, וישמשו קונים זכאים מרובים המזוהים עם **ארגון**. זה יפשט את תהליך הרכש תוך מיטוב החיסכון של הסקיייל.

לאחר הקמת הסכם המסגרת הוא מאפשר לארגון לרכוש את טכנולוגיות הענן הספציפיות ואת השירותים הקשורים לענן שהוא זקוק להם, כאשר הוא זקוק להם - בניגוד לביצוע רכישות נפרדות. גישה כזו מפחיתה את הדרישות הניהוליות ומפחיתה משמעותית את מורכבות הרכש וזמן המחזור.

משך הסכם המסגרת יהיה **<X>** שנים לכל היותר, כולל חידושים כלשהם. משך הזמן המרבי של חוזת מסגרת מרוכב הוא בדרך כלל **<X>** חודשים; ניתן להאריך אותו ב-**<X>** חודשים ולאחר מכן ב-**<X>** חודשים נוספים, עם האישורים הפנימיים המתאימים הנדרשים להארכת חוזה. זה יצוין בכל **חוזה מרוכב** ספציפי.

המסגרת מחולקת ל-3 (שלוש) חלקות.

1. **חלקה 1: טכנולוגיות ענן** - היקף מלא של טכנולוגיות ספקי ענן (שירות מ-CISP, מהמפיץ או מהמפיץ עם שירותים/תמיכה בעלי ערך מוסף):

i. **שירותי IaaS ו-PaaS** - תפריט של טכנולוגיות ענן, למשל. מחשוב, אחסון, רשתות, מסד נתונים, ניתוח, שירותי יישומים, פריסה, ניהול, מפתח, האינטרנט של הדברים (IoT) וכו'. כולל פתרונות טכנולוגיית ענן ארוזים כמו DR/COOP, Archive, Big Data & Analytics, DevOps וכו'.

2. **חלקה 2: MARKETPLACE** - היקף מלא של שירותי/מוצרי PaaS ו-SaaS כגון הנהלת חשבונות, CRM, עיצוב, משאבי אנוש, GIS ומיפוי, BI, HPC, ניהול תוכן, ניתוח יומנים וכו'.

3. **חלקה 3: ייעוץ בענן** - היקף מלא של שירותי ייעוץ (שירותים מנוהלים, שירותים מקצועיים, שירותי ייעוץ, שירותים עם ערך מוסף, FinOps, תמיכה טכנית) הקשורים להעברה לענן ולשימוש בו. שירותים אלו יכולים לכלול: תכנון, עיצוב, העברה, ניהול, תמיכה, QA, אבטחה, הדרכה וכו'.

ספקים יכולים להגיש את ההצעות שלהם לכמה חלקות.

הספקים יגישו את ההצעות שלהם ואת התמחור הקשור בפורמט הרצוי שלהם.

תחרות בתוך המסגרת והענקת חוזים

חוזים מרוכזים

גופים במגזר הציבורי השותפים להסכם המסגרת יכולים להזמין או להגיש 'חוזה מרוכב' לשירותים הדרושים להם בעת הצורך. הצבת חוזה מרוכב במסגרת הסכם המסגרת מאפשרת ללקוחות לחדד דרישות עם מפרט פונקציונלי נוסף לחוזה מרוכב, תוך שמירה על ההטבות המוצעות במסגרת הסכם המסגרת.

חוזים שיוענקו במסגרת הסכם המסגרת יוכלו להציג נתיב ביקורת ברור מבחינת הדרישות המשמשות לבחירת הספק בתוך כל חלקה. רוכשי קצה ישמרו תיעוד של התקשרות עם הספקים, כולל כל מעורבות מוקדמת בשוק, שאלות הבהרה, אימיילים ושיחות פנים אל פנים שביצעו.

1. כתיבת דרישות חוזה מרוכז ובקשת אישור פנימי לקנייה

כל רוכשי הקצה הזכאים להשתמש בהסכם המסגרת ייצרו צוותים משותפים של משתמשי קצה עסקיים, מומחי רכישה ומומחים טכניים כדי להבין רשימה של 'חייב שיהיה' ו'רצונות'. דרישות אלו יסייעו להחליט אילו חלקות ישימות, ואיזה ספק הכי מתאים לעמוד בדרישות. בעת ניסוח הדרישות הרוכשים ישקלו את:

- הכספים הזמינים לשימוש בשירות
- דרישות הרכש והדרישות הטכניות של הפרויקט
- הקריטריונים שעליהם תתבסס הבחירה

2. חיפוש שירות

רוכשים במסגרת הסכם המסגרת ישתמשו בקטלוג מסגרת מקוון (פורטל שבו יופיעו מקבלי מענק הסכם מסגרת מוסמכים ושירותיהם) כדי למצוא מוצרים/שירותים העונים על הצרכים המזוהים שלהם. הם יבחרו את החלקות המתאימות, ולאחר מכן יחפשו שירותים.

3. סקירה והערכה של שירותים

הרוכשים בהסכם המסגרת יסקרו את תיאורי השירות כדי למצוא את השירותים המתאימים ביותר לצרכים בהתבסס על הדרישות והתקציב. כל תיאור שירות יכול:

- מסמך הגדרת שירות או קישורים להגדרות שירות
- מסמך תנאים והגבלות
- מסמך תמחור (קישורים לתמחור ציבורי מקובלים בהנחה שמחירון מלא/מסמך תמחור זמין לפי בקשה)

המחיר יהיה עלות התצורה הנפוצה ביותר של השירות. עם זאת, התמחור בדרך כלל מבוסס על נפח, ולכן הרוכשים צריכים תמיד להסתכל במסמך התמחור של הספק או בתמחור הציבורי ובכלי מחשבון המחירים כדי לחשב את המחיר האמיתי של מה שנרכש, ואת הערך הכולל שניתן לרוכש (לדוגמה, שירותי אופטימיזציה והפחתת עלויות כתוצאה מכך).

רוכשים במסגרת הסכם המסגרת רשאים לדבר עם ספקים כדי לבקש מהם להסביר את תיאור השירות, התנאים וההגבלות, התמחור או מסמכי/מודל הגדרת השירות שלהם. יישמר תיעוד של כל שיחה עם ספקים.

4. בחירת שירות והענקת חוזה**ספק יחיד**

אם רק ספק אחד עומד בדרישות, ניתן להעניק לו חוזה.

ספקים רבים

אם יש מספר שירותים ברשימה קצרה, הרוכש יבחר בשירות עם המכרז המשתלם ביותר כלכלית (MEAT). יש לעיין בקריטריונים בטבלה הבאה לקבלת הערכה מבוססת MEAT. הרוכשים יכולים להחליט באילו מאפיינים מפורטים להשתמש וכיצד לשקלל אותם.

שימו לב שיתכן והרוכש יצטרך:

- לבדוק שילובים של ספקים שונים
- לקבל מידע ספציפי על הנחות לפי נפח או ארגוניות, ושירותי ייעול עלויות ספקים

הערכה של ספקים צריכה להיות תמיד הוגנת ושקופה. הבחירה תתבסס על ההתאמה הטובה ביותר, וספקים/שירותים לא יוחרגו מבלי לחזור לדרישות הפרויקט.

טבלה 2 - הערכה מבוססת MEAT
קריטריונים למענק
עלות חיים שלמים: עלות אפקטיבית, מחיר ועלויות שוטפות
כישורן טכני והתאמה פונקציונלית: כיסוי, קיבולת רשת וביצועים במפורט ברמות השירות הרלוונטיות
ניהול שירות לאחר המכירה: מוקד עזרה, תיעוד, פונקציית ניהול חשבונית והבטחת אספקת מגוון שירותים
מאפיינים לא פונקציונליים

תחרויות זעירות

במידת הצורך, ניתן לקיים תחרות זעירה לאיתור הספק הטוב ביותר עבור עומס עבודה או פרויקט מסוימים. תחרות זעירה היא המקום שבו לקוח הולך לתחרות נוספת במסגרת הסכם המסגרת, על ידי הזמנת כל הספקים בתוך החלקה להיענות למערכת של דרישות. הלקוח יזמין את כל הספקים המתאימים בתוך החלקה להשתתף במכרז. יש לעיין במידע ההשוואה הנוסף בסעיפים שלהלן לגבי מפרטים טכניים, אבטחה ותמחור/ערך.

חוזת

הלקוח והספק יחתמו שניהם על עותק של החוזה לפני שניתן יהיה להשתמש בשירות. משך הזמן המרבי של חוזה מסגרת הוא בדרך כלל <X> חודשים; ניתן להאריך זאת ב-<X> חודשים ולאחר מכן ב-<X> חודשים נוספים, עם האישורים הפנימיים המתאימים הנדרשים להארכת חוזה.

עותק של החוזה חייב להיות חתום על ידי כל בעלי העניין (הלקוח והספק) לפני שניתן יהיה להשתמש בשירות.

2.1.5 דרישות מינימום למשתתף במכרז - מנהלתי

שפה פשוטה וברורה לקביעת קריטריונים להסמכה של הסכם מסגרת תסייע להבטיח שלא יהיו הגשות ממרכזי נתונים מסורתיים או ספקי חומרה המארחים פתרון מסורתי כ'ענן'. משתתפי RFP צריכים להדגים כיצד הם עומדים בדרישות המינימליות המנהלתיות של המשתתף במכרז.

שוב שימו לב שהמאמר הזה מתמקד בחלקה 1 - טכנולוגיות ענן. עם זאת, הוספנו מידע נוסף על חלקה 2 - MARKETPLACE וחלקה 3 - ייעוץ בענן כשזה עוזר לספק הקשר כללי בכל הנוגע לדרישות ולהיקף ה-RFP. לדוגמה, חשוב לכלול קריטריוני הסמכה מינימליים למפיץ CISP/MSP/SI/חברת ייעוץ/וכו', וזה עוזר להבטיח שהם (1) קשורים ישירות ל-CISP כמפיץ או כשותף ערוץ, (2) מוסמכים על ידי CISP למכור מחדש גישה ישירה להצעות CISP לגופי צד שלישי, ו-(3) יש להם אישורים מאותם CISPs המציעים את היכולות והמומחיות שלהם

שפת RFP לדוגמה: דרישות מינימום למשתתף במכרז - מנהלתי

הסכם מסגרת זה יעניק חוזים לספקים מרובים בקטגוריות הבאות. הספקים חייבים להיות CISP מסחרי, מפיצי צד שלישי של CISP, מפיץ של שירותי Marketplace ו/או ספק שירותים לשימוש ב-CISP (לדוגמה: ייעוץ, שירותי העברה, שירותים מנהלים, FinOps וכו'). יש לזהות את התפקידים שאתם מציעים במכרז:

חלקה 1

_____ - ספק ישיר (CISP) של שירות ענן ציבורי (PaaS-IaaS)

_____ - ספק ישיר (CISP) של שירות ענן קהילתי (PaaS-IaaS)

_____ - ספק ישיר (CISP) של שירות ענן פרטי (PaaS-IaaS)

_____ - מפיץ צד שלישי של CISP (יכולת לספק גישה ישירה להצעות ענן מקוונות של CISPs).

○ יש לזהות את הצעת ה-CISP שניתן להפיץ גישה ישירה לשירות שלהם: _____

○ יש לספק מכתב מה-CISP שאומר כי אתם מפיצים מורשים של ההצעות שלהם: _____

חלקה 2

_____ ספק ישיר של שירותי Marketplace הפועלים ב-CISP (PaaS ו/או SaaS)

_____ מפיץ של שירותי Marketplace הפועלים ב-CISP (PaaS ו/או SaaS)

חלקה 3

_____ CISP - המספק שירותים מקצועיים

_____ ספק תמיכה טכנית של CISP

_____ שותף CISP המספק שירותים לשימוש או הפעלה ב-CISP

_____ משפיען/חברת ייעוץ המספקים שירותים לשימוש או הפעלה ב-CISP

זיהוי סוג ההצעה:

- שירותים מנוהלים של עומסי עבודה ב-CISP (כן/לא): _____
 - זיהוי התמחויות אם רלוונטי: _____
- שירותים מקצועיים (כן/לא): _____
- ייעוץ – הדרכה (כן/לא): _____
- ייעוץ – אסטרטגיה (כן/לא): _____
- ייעוץ – העברה (כן/לא): _____
- ייעוץ – משילות בענן (כן/לא): _____
- ייעוץ – FinOps (כן/לא): _____
- ייעוץ – אחר (יש לפרט): _____

יש לזהות CISP/CISPs שאתם מספקים שירותים עבורם: _____
 יש לספק מכתב מה-CISP המאשר את ייעוד השותף שלך לפי מודל ה-CISPs: _____

חלקה 1 דרישות מנהלתיות מינימליות

ספקי שירותי ענן (CISPs)

על מנת להיות מוסמכים ב-CISP, עליהם לספק התאמה לדרישות שלהלן.

קריטריוני דרישה מוצעים עבור CISP	סיבה
פרטים ארגוניים כגון שם, מבנה משפטי, מספר רישום/DUNS, מע"מ וכו'.	
גודל החברה, מצבה הכלכלי והפיננסי ³	הלקוח יכול לקבוע שה-CISP יוכל לבצע את החוזה.
עילות להדרה עשויות להיות פעילות פלילית/הונאה וכו'.	
תיאורי מקרה/הפניות ללקוח (יש לציין מספר/סוג דרישה נדרשים)	ללקוח יש את היכולת למדוד ניסיון ב-CISP כדי לספק את השירותים הנדרשים.
תחומי אחריות חברתית של התאגיד	אלה צריכים להיות גרסאות נגישות לציבור שה-CISP מספק.
התחייבויות ושיטות עבודה בנושא קיימות הזמינות לציבור.	הלקוח יכול לראות שה-CISP מחויב לנהל את העסק שלו בצורה הכי ידידותית לסביבה שיש

³ יש לשים לב כי RFP לרכישת שירותי ענן בודק מידע חברה ברמה גבוהה, בניגוד למספר העובדים בחברה ומבנה צוות העובדים הפנימי. עם טכנולוגיית ענן אין מתאם בין הבטחה לביצועי השירות, לבין מספר העובדים. במקום זאת, RFPs של ענן בודקים שגודל החברה הכולל עומד בדרישות (סקייל מתאים) ושיש ניסיון/ביצועים מוכחים.

ה-CISP חייב לספק רקורד מוכח בחדשנות והפצה של שירותים ותכונות שימושיים חדשים במהלך 5 השנים האחרונות, במיוחד בתחום של PAAS, למידת מכוּנה וניתוח, Big Data, שירותים מנהלים ותכונות אופטימיזציה של שימוש בענן. ניתן להשתמש ביומני שינויים נגשים לציבור או בעדכונים כדי להוכיח את הנקודה.	מוכיח שה-CISP פועל כדי להעביר מוצרים חדשים לידי הלקוחות במהירות, ולאחר מכן חוזר ומשפר במהירות את המוצרים. הדבר עוזר ללקוחות לשמור על תשתית IT חדישה ללא צורך בהשקעות הזרמת הון
--	--

קשר מפניץ/שותף עם CISP

ארגון דורש שהקבלן הראשי יהיה מזוהה ישירות עם ה-CISP כמפניץ או כשותף ערוץ, מוסמך על ידי CISP להפיץ גישה ישירה להצעות CISP לגופי צד שלישי, עם אישורים של אותם CISP המעידים על יכולותיהם ומומחיותם. זה מבטל את הדרישה מה**ארגון** לעיין במונחים והשירותים הקשורים לשכבה נוספת של קבלנות משנה בין הקבלן הראשי של **הסכם המסגרת** לבין ה-CISP. דרישה זו גם מפחיתה את המורכבות שמייצרות שכבות מפיצים נוספות כאשר (1) **הארגון** מבצע את בדיקת הנאותות שלו כדי להבטיח הקצאה ברורה של תחומי אחריות בנוגע לשירותים שיוספקו, וכן (2) **הארגון** מבצע מדי יום ביומו פעילויות הכרוכות בצריכת שירותי הענן

2.2 טכני

RFP לרכישת שירותי ענן צריך להעלות את הרף עבור CISP בדרישה שהם יספקו את טכנולוגיות הענן הסטנדרטיות הדרושות ללקוח כדי לבנות את הפתרון המותאם שלהם. כפי שצוין קודם לכן, ההבדל הזה בין מה שמתקבן לבין מה שמוצאם אישית הוא חשוב מאוד כאשר נגשים ל-RFP לרכישת שירותי ענן. CISP מציעים שירותים סטנדרטיים למיליוני לקוחות, כך שהתאמות אישיות ב-RFP לרכישת שירותי ענן מתמקדות בפתרונות ובתוצאות הטובים ביותר במערם, בניגוד לשיטות, לתשתית או לחומרה המשמשות כבסיס להצעת שירותי הענן המנוצלים להשגת תוצאות המהוות פתרון.

2.2.1 דרישות מינימום

רכישות IT מסורתיות מסתמכות לרוב על דרישות עסקיות שפותחו באמצעות סדרה של הפעלות עבודה המתעדות את האופן שבו הארגון מנהל את עסקיו כיום. קבלת דרישות אלה בצורה נכונה לחלוטין היא תהליך קשה בנסיבות הטובות ביותר. אם יצליח, הפעלות התייעוד הללו מתעדות את התהליך העסקי ההיסטורי שעשוי, כשלעצמו, להיות מיושן ולא יעיל. אם הדרישות הללו הופכות לחלק מה-RFP שישוּבפל על ידי ה-CISP, הפתרון היחיד עשוי להיות פתרון בהתאמה אישית. מודל זה אינו תואם לרכישות בענן.

ארגונים במגזר הציבורי צריכים להבין את היעדים העסקיים ואת צורכי הביצועים שלהם, אך לא צריכים להיות הקווים המנחים ב-RFP ובכך להכתיב את עיצוב המערכת ואת הפונקציונליות. במקום זאת, הארגון צריך לחפש את ההתאמה העסקית הטובה ביותר. במקום להעריך הצעות על מאות או אפילו אלפי דרישות מנחות שאולי לא יובילו לשירותים מוצלחים, ארגונים צריכים לכלול קריטריונים להערכה המבוססים על מידת ההתאמה של הטכנולוגיה והשירותים הנלווים או כאלה שישפרו יעדים עסקיים, בין אם הם משיגים את צורכי הביצועים שלהם, ואת היכולת לכוון כללים עסקיים באמצעות קביעת תצורה.

RFPs בענן צריכים לשאול את השאלות הנכונות כדי לקבל את הפתרונות הטובים ביותר. בהתחשב בכך שבמודל ענן לא נרכשים נכסים פיזיים, מכאן נובע שדרישות רבות של רכישת מרכזי נתונים מסורתיים אינן ישימות. **מחזור שאלות במרכז הנתונים יוביל בהכרח לתשובות במרכז הנתונים**, מה שגורם לכך ש-CISP לא יוכלו להשתתף במכרזים, או יובילו לחוזים מעוצבים בצורה גרועה שמונעים מלקוחות במגזר הציבורי לחלץ את מלוא היכולות והיתרונות של הענן.

RFP לרכישת שירותי ענן מתמקד בדרישות המפתח הנדרשות מ-CISP ומשירותי ענן, ומבטיח שספקים שמתאימים לחלקה 1 עומדים ברף גבוה. הדרישות צריכות גם להימנע מלהיות מנחות מדי, כדי שלא להגביל את הגישה למגזר הציבורי למגוון רחב של CISP מוסמכים.

שפת RFP לדוגמה: יכולות של ספק ענן

יש לעיין גם בדרישות המנהלתיות המינימליות של CISP המצוינות לעיל עבור חלקה 1

קריטריוני דרישה מוצעים עבור CISP	סיבה
תשתית	
תשתית CISP צריכה להציע לפחות 2 אשכולות של מרכזי נתונים. כל אשכול חייב להיות מורכב מ-2 מרכזי נתונים לפחות המחוברים בקישור עם השהיה נמוכה כדי לאפשר פריסות והטמעות זמינות במיוחד מסוג Active-Active של תרחישי DR-BC. מרכזי הנתונים המרכיבים כל אשכול חייבים להיות מבודדים פיזית ונפרדים מבחינת זה מזה.	ה-CISP צריך להיות מסוגל להציע תשתית המתאימה לבניית יישומים זמינים במיוחד, שבהם ניתן להימנע מנקודות כשל בודדות.
CISP צריך לספק אזורי מבודדים מבחינה לוגית וגאוגרפית. אין לשכפל נתוני לקוחות מחוץ לאזורים אלה על ידי ה-CISP.	דרישות תושבות הנתונים מחייבות שהלקוח יהיה בשליטה מלאה לגבי המיקום של הנתונים שלו.
ה-CISP חייב להיות בעל יכולת לספק קישוריות ישירה, יעודית ופרטית בין מרכזי הנתונים של ה-CISP.	קישוריות פרטית היא דרישה בסיסית שלפיה ניתן יהיה לבנות תשתית היברידית ומאובטחת.
CISP צריך לספק מנגנונים מספקים, הכוללים הצפנה עבור נתונים במעבר.	הלקוח יכול לדרוש שתהיה יכולת שלפיה אף נתון לא יוכל לעבור ללא הצפנה.
אישור CISP מינימלי	
ה-CISP חייב להיות בעל הסמכת ISO 27001.	ביקורת, אישור והסמכה של צד שלישי מבטיחים שלקוחות יכולים לבצע השוואת שירותים (ובפרט את הפלטפורמה) לאיכות, בטיחות ואמינות. חובה לעמוד במינימום אישורים.
ה-CISP חייב לציית לקוד ההתנהגות להגנה על המידע של CISP, כדי לספק תכונות ושירותים שניתן להשתמש בהם בתאימות ל-GDPR, דבר המאפשר ללקוחות לבנות יישומים תואמי GDPR.	הלקוח חייב להיות מסוגל לבנות או להריץ יישומים בתאימות עם GDPR.
ה-CISP חייב להעמיד דוחות ביקורת של צד שלישי, כגון דוחות SOC 1 ו-2 (המכסים את המיקומים והשירותים שבהם משתמשים לקוחות קצה) כדי לאפשר שקיפות ביחס לבקורות ולנהלים של ה-CISP.	ה-CISP צריך להיות שקוף לגבי אופן ההפעלה והניהול של היישום. דוחות SOC מסייעים להבטיח אומון ושקיפות.
ה-CISP חייב להיות מחובר להסכם מרכז הנתונים לניטרליות אקלימית.	הסכם מרכז הנתונים לניטרליות אקלימית מחייב את ה-CISP להגיע לניטרליות אקלימית עד 2030, ולכן מאפשר למשתמש לתמוך ביעדי הקיימות שלו. מבקרי צד שלישי הם חובה לספקים < 250 FTE (לא SMEs).
ה-CISP חייב לציית לקוד ההתנהגות הקשור לניידות של SWIPO IaaS.	קוד ההתנהגות הקשור לניידות של SWIPO IaaS מבטיח שהשירותים עומדים בדרישות סעיף 6 "ניוד נתונים" של תקנת הזרימה החופשית של נתונים לא אישיים.
מאפייני שירות	
תשתית ה-CISP חייבת להיות נגישה באמצעות ממשקים תכנותיים (API) ומסוף ניהול מבוסס אינטרנט.	גישה לשירות עצמי וממשקים תכנותיים הם סטנדרט נדרש של ספקי CISP כדי לבטל ככל האפשר את גישת המשתמש ואת הספק עצמו.
ה-CISP חייב להציע מערכת יסוד של שירותים הכוללים: אחסון אובייקטים, מסד נתונים קשור מנוהל, מסד נתונים לא קשור מנוהל, מאזני עומסים מנוהלים, ניטור ו-Autoscaling משולב.	עצם ההצעה של מכונות וירטואליות אינה מספיקה כדי להכשיר ספק כספק ענן. ספקי ענן צריכים להציע מערך של שירותי PAAS ו-IAAS כדי להאיץ ולשפר את היישומים של הלקוח.

ה-CISP חייב לאפשר ללקוח לשנות באופן חופשי את השימוש וקביעת התצורה של השירותים שלו, או להעביר נתונים בתוך ומחוץ ל-CISP (הצעת שירות עצמי).	גישה בשירות עצמי לשירותים ונתונים היא דרישה קשה המאפשרת ללקוח להיות עצמאי לחלוטין.
ה-CISP חייב לאפשר חיוב "תשלום לפי שימוש" של השירותים שלו.	תשלום לפי שימוש מאפשר ללקוח לייעל את עומסי העבודה שלו מבחינת עלות, למזער סיכונים ולמנף את ה-CISP עבור יישומים ו-PoCs קצרי מועד.
אבטחת נתונים ומערכות	
ה-CISP חייב לאפשר ללקוח לשמור על שליטה מלאה בנתונים שלו, לתת ללקוח חופש לבחור היכן מאוחסנים הנתונים (אזור עירוני של העיר), ולהבטיח שלא יועברו נתוני לקוח אלא אם כן הלקוח יזום מהלך כזה בעצמו.	ללקוח חייבת להיות שליטה על המקום שבו מאוחסנים הנתונים, כיצד לנהל את הגישה לתוכן, וגישה של משתמשים לשירותים ומשאבים
מאפייני ה-CISP חייבים לתת ללקוח שליטה מלאה במדיניות האבטחה שלו, כולל סודיות, שלמות נתוני הלקוח והמערכות זמינותם.	הלקוח חייב להיות מסוגל להגדיר וליישם את תקני האבטחה שלו על פני עומסי העבודה שלו. לסמוך על הספק ש"יעשה את הדבר הנכון" עם הנתונים של הלקוח אינו מספיק.
בקרת עלויות	
ה-CISP חייב להיות בעל מנגנונים וכלים שיאפשרו ללקוח לפקח על ההוצאות לאורך זמן. הכלים חייבים לאפשר פילוח בסיסי של עלות בהתבסס על עומס עבודה, שירות וחשבון.	
ה-CISP חייב להציע כלים שיתריעו בפני הלקוח בכל פעם שנחצה סף עלות.	
ה-CISP חייב לספק חשבונות מפורטים ללקוח. חייבת להיות אפשרות לבנות את החשבון כך שיפריד בין עלות לפי עומס עבודה, סביבה וחשבון.	

CISP צריך גם לספק תשובות לשאלות בנוגע לדרישות הטכניות שלהלן.

פתרונות

CISP צריך להדגים כיצד הוא יכול לספק תבניות מובנות מראש ופתרונות תוכנה שמתארחים ב-CISP או משתלבים בו, עבור הפתרונות הבאים:

- אחסון
- DevOps
- אבטחה/תאימות
- Big Data/ניתוח
- יישומים עסקיים
- טלקומוניקציה ורישיות עסקי
- גאו-מרחבי
- IoT
- [אחר]

מספק סקירה כללית של אופן השימוש ב-CISP לעומסי העבודה הבאים:

- התאוששות מאסונות
- פיתוח ובדיקה
- ארכיב נתונים
- גיבוי ושחזור
- Big Data
- מחשוב בעל ביצועים גבוהים (HPC)
- האינטרנט של הדברים (IoT)
- אתרי אינטרנט

- מחשוב עם שירות מנוהל
- DevOps
- אספקת תוכן
- [אחר]

2.2.2 השוואה בין ספקים

בנוסף לדרישות המינימום ב-RFP לרכישת שירותי ענן, חשוב לספק קריטריונים לפיהם ניתן להשוות טכנולוגיות CISP במהלך הערכה תחרותית.

RFPs לרכישת שירותי ענן צריכים לבקש את יכולות הענן שארגון צריך, מתוך הבנה שהלקוח מחזיק בשימוש ביכולות כאלה כדי לבנות את הפתרון שלו. פונקציונליות מעבר לסטנדרט ש-CISP יכול לספק (כגון פתרונות מובנים מראש באמצעות ה-CISP, או תכונות אוטומציה) - יכולה לשמש לניתוח משמעותי יותר של "אפשרויות עם ערך מוסף" או "התמורה הטובה ביותר" ב-RFP לרכישת שירותי ענן.

המגזר הציבורי דורש לעיתים קרובות תחרות בין משתתפים במרכז תוך שימוש בקריטריונים להערכה כמו התמורה הטובה ביותר, המכרז המשתלם ביותר כלכלית (MEAT), או המחיר הנמוך ביותר. כאשר גופים במגזר הציבורי מתכננים את החלק הזה של RFP לרכישת שירותי ענן, חשוב לבנות גישה שלוקחת בחשבון את התכונות הייחודיות של הענן. לדוגמה, הבנה שרק השוואת פריטים בין הצעות של ספקי ענן (למשל: מחשוב או אחסון) אינה דרך יעילה להשוואת הצעות. במקום זאת, אנחנו ממליצים בחום להתמקד בפתרונות ברמה גבוהה יותר, כגון אלו המפורטים למעלה בסעיף 2.2.1. לאחר מכן, גופים במגזר הציבורי יכולים להסתכל על דרישות ספציפיות לענן, כגון אלו המפורטות ב-נספח א' - דרישות טכניות להשוואה בין משתתפים במכרז.

RFPs צריכים לציין את מאפייני הענן החיוניים הדרושים לבניית פתרון הענן שלהם. לשם כך, ארגונים במגזר הציבורי יכולים למנף את מאפייני הענן החיוניים של המכון הלאומי לתקנים וטכנולוגיה (NIST), בנוסף לשימוש בדוחות מאנליסטים של צד שלישי כדי להבטיח של-CISP יש את הצעת ה"ענן האמיתי" המתאימה ביותר, הפועלת בסקייל מסיבי.

שפת RFP לדוגמה - השוואה בין ספקים

CISP צריכים גם לספק תשובות לכל שאלות הדרישות הטכניות בנספח א'.

על המשיבים להיות בעלי המאפיינים הבאים ועליהם לתאר כיצד ההצעות שלהם לשירותי ענן עונות לחמשת המאפיינים החיוניים למחשוב ענן⁴.

(1) **שירות עצמי לפי דרישה:** על המשיב לספק את היכולת להקצות באופן חד צדדי יכולות מחשוב, כגון זמן שרת ואחסון רשת, לפי דרישה ובאופן אוטומטי ללא צורך באינטראקציה אנושית עם כל אחד מספקי השירות. המשיב יספק את היכולת לביצוע פעולות ההזמנה כדי להקצות שירותים באופן חד צדדי (כלומר, ללא בדיקת ספק או אישור). יש להסביר כיצד זה עובד עם ההצעה שלך או עם ההצעה המיוצגת שלך.

(2) **גישה לרשת בכל מקום:** על המשיב לספק אפשרויות חיבור מרחבות לרשת, אחת מהן חייבת להיות מבוססת אינטרנט. יש להסביר כיצד זה עובד עם ההצעה שלך או עם ההצעה המיוצגת שלך.

(3) **מאגר משאבים:** ה-CISP של המשיב חייב לספק משאבי מחשוב מאוחדים המשרתים צרכנים מרובים באמצעות מודל ריבוי דיירים עם משאבים וירטואליים שונים המוקצים ומוקצים מחדש באופן דינמי בהתאם לדרישת הצרכנים. המשתמש יכול לציין מיקום ברמת הפשטה גבוהה יותר (למשל: מדינה, אזור או מיקום מרכז נתונים). המשיב יתמוך בסקיילינג של משאבים אלה תוך דקות או שעות לאחר בקשת הקצאה. יש להסביר כיצד זה עובד עם ההצעה שלך או עם ההצעה המיוצגת שלך.

(4) **גמישות מהירה:** ה-CISP של המשיב יתמוך ביכולות אספקת שירות וביטולה (סקייל למעלה ולמטה), ולהפוך את השירות לזמין בתוך מספר השעות המינימלי שנקבע (מקסימום 'x' שעות) מבקשת ההקצאה. המשיב יתמוך בהתאמות חיוב הנובעות מבקשות ההקצאה הללו על בסיס יומי או על בסיס שעתי או יומי.

⁴ <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

5) **שירות מדוד:** המשיב יציע נראות לגבי השימוש בשירות באמצעות לוח בקרה מקוון או אמצעי אלקטרוני דומה.

בנוסף, ה-CISP חייב:

- להיות מנהיג מוכר באספקת שירותי ענן כפי שהודגם ברביע הקסם של Gartner עבור IaaS⁵
- לספק דוחות מאגליסטים של צד שלישי המוכרים בתעשייה, שמדגימים את היכולות והאמינות של ה-CISPs.

לבסוף, תיערך השוואה בין ה-CISPs באמצעות התרחישים המפורטים בנספח ב'.

2.2.2.1 הסכמי רמת שירות (SLA)

CISPs מספקים SLA מסחריים מתוקננים למיליוני לקוחות, ולכן אינם מסוגלים להציע SLA מותאמים אישית, כפי שקורה במודל מרכז נתונים בשטח. עם זאת, לקוחות CISP (לעיתים קרובות בסיוע CISP Partners) יכולים לתכנן אדריכלית את השימוש בענן כדי למנף את ה-SLAs המסחריים של CISP כדי לעמוד בדרישות הספציפיות ללקוח ובשירותי SLA ייחודיים ואף לעבור אותם.

RFPs לרכישת שירותי ענן צריכים להבטיח שה-CISPs מציעים את היכולות וההדרכה הדרושים למינוף השירותים וה-SLA המסחריים שלהם, כך שמשמשי קצה בודדים יוכלו לעמוד בדרישות הביצועים והזמינות.

שפת RFP לדוגמה: הסכמי רמת שירות

לספק מידע על גישת CISPs להסכמי רמת שירות (SLA) וקישורים אליה.

הארגון ישמור על מודעות להסכמי רמת השירות (SLA) של ה-CISP ויפרסם עומסי עבודה ויישומים חשובים בצורה כזאת שהוא ימשיך לפעול גם במקרה שלא יעמוד ב-SLA.

הארגון יהיה אחראי לתחזוקת SLA מתאימה הקשורה לכל ציוד שבבעלות **הארגון** או לשירותים המופעלים על **הארגון** ומשמשות אותו עם ה-CISP.

ה-CISP צריך לספק ל**הארגון** את היכולות לקבל נראות ודיווח מתמשכים של ביצועי ה-SLA התפעוליים, ושיטות עבודה מומלצות מתועדות למינוף תשתית CISP לשירותי ארכיטקטורה לביצועים, עמידות ואמינות.

2.2.3 התקשרות בחוזה

התנאים וההגבלות של CISP מתוכננים לשקף את אופן פעולתו של מודל שירותי ענן (נכסים פיזיים אינם נרכשים ו-CISPs פועלים בסקייל מסיבי ומציעים שירותים מתוקננים); לפיכך, זה קריטי שהתנאים וההגבלות של ה-CISP יהיו משולבים וינוצלו במידה המרבית האפשרית. יש לעיין בסעיף 2.5 שלהלן לקבלת מידע נוסף על תנאים והגבלות והתקשרות.

2.2.3.1 שירותים חדשים ומשתנים

CISPs מספקים ביצועים באמצעות שירות. בניגוד לפתרונות בשטח מסורתיים הדורשים שדרוגים וחוזי תחזוקת שירות שפג תוקפם, ספקי ענן פשוט מספקים את השירות המתוקנן. כדי שמודל הענן ישיג חיסכון של הסקייל, השדרוגים והשינויים בתשתית הבסיסית מופעלים לכולם, לא למשתמשים בודדים, ואז הלקוחות בוחרים בקפידה את השירותים שבהם הם משתמשים. השירות חלק יותר ממערכות בשטח שהשתמשו בהן בעבר, וספקי ענן מוסיפים כל הזמן שירותים חדשים ומשופרים עבור הלקוחות לשימוש כרצונם.

אם לא ניתן להוסיף שירותי CISP חדשים או משופרים לאחר המועד האחרון להגשת RFP, ארגונים במגזר הציבורי מגבילים את עצמם וכך לא יכולים להיעזר בשירותים החדשים ובתכונות המשופרות עד לשחרור האיתרציה הבאה של הסכם מסגרת. לכן אנחנו ממליצים בחום כי הקצאת השירותים המתוארים במסגרת הסכם המסגרת תהיה רחבה ותאפשר הוספה של שירותי CISP חדשים לאחר המועד האחרון להגשה. חוק הרכש של האיחוד האירופי עשוי להגביל את ההצגה של שירותי

⁵ <https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb>

CISP חדשים ושונים באופן מהותי שיתווספו להסכם המסגרת, אך ניתן להוסיף עדכונים וגרסאות חדשות של שירותים שאינם נחשבים לשינויים מהותיים ללא אתגר רכש.

שפת RFP לדוגמה: שירותים חדשים ומשתנים

ה-CISP יספק פתרון חסכוני המשתמש בטכנולוגיות וירטואליזציה מוכחות ויציבות ובטכנולוגיות חדשניות המתרענות כל הזמן. ה-**ארגון** מאשר ומסכים שטכנולוגיות הענן עשויות להיות מסופקות על בסיס שירות משותף ל-**ארגון** וללקוחות אחרים של ה-CISP מבסיס קוד משותף ו/או סביבה משותפת וה-CISP עשוי מעת לעת: לשנות, להוסיף או למחוק את הפונקציות, התכונות, הביצועים או מאפיינים אחרים של שירותי הענן, ואם יבוצעו שינוי, הוספה או מחיקה כאמור, המפרטים של שירות הענן יתוקנו בהתאם.

היקף הזמנת האספקה הזו כולל את כל שירותי ה-CISP הקיימים כעת ושירותי CISP חדשים או משופרים **בתוך הסכם המסגרת**. שירותי ענן שסיפקו CISP הזמינים ללקוחות מסחריים יהיו זמינים ל-**ארגון**.

2.2.3.2 נעילת ספק/הפיכות

טכנולוגיית הענן מפחיתה את נעילת הספקים מכיוון שלא נרכשים נכסים פיזיים, ולקוחות יכולים להעביר את הנתונים שלהם מספק ענן אחד לאחר בכל עת.

עם זאת, מידה מסוימת של נעילת ספקים היא בלתי נמנעת בעת רכישת שירותי ענן - מכיוון שלא כל העננים שווים, ולכן CISP אחד עשוי להציע שירותים ויכולות שהאחר פשוט אינו יכול לספק - ולכן מפחית את היכולת להשתמש בשירותים כאלה עם ספק אחר. גישה נבונה היא לדרוש מ-CISPs לספק את התכונות והשירותים הנדרשים כדי לצאת מהענן שלהם, כאשר תיעוד לגבי אופן השימוש בשירותים אלה משמש כ'אסטרטגיית יציאה' סבירה - בהתחשב בכך שלא ייתכן ש-CISP יידע את התצורה הייחודית של שימוש הלקוח בשירותים המתקננים שלו, וככזה לספק תוכנית יציאה מותאמת אישית.

יש לעיין בסעיף 2.3.1.2 למידע על קודים התנהגותיים של התעשייה לטיפול ב"ניוד נתונים" ו"החלפת ספקי ענן" כדי לעמוד בדרישות סעיף 6 של האיחוד האירופי "תקנת הזרימה החופשית של מידע לא אישי".

שפת RFP לדוגמה: הצטרפות ועזיבה

ה-**ארגון** מחפש הצעות המספקות אסטרטגיית יציאה סבירה למניעת נעילה. ה-**ארגון** אינו קונה נכסים פיזיים, וה-CISP יספק את היכולת להתקדם במערום ה-IT ולרדת שוב למטה. ה-CISP יספק כלי ניידות ושירותים שיסייעו במעבר אל פלטפורמת CISP וממנה, תוך מזעור הנעילה. תיעוד מפורט לגבי אופן השימוש בכלי ניידות ושירותים המסופקים על ידי CISP ישמש כתוכנית יציאה סבירה.

ה-CISP לא צריך **לדרוש** התחייבויות מינימום או **לדרוש** חוזים ארוכי טווח.

הלקוח יכול לייצא נתונים השמורים אצל ספק שירות בכל עת. ה-CISP יאפשר ל-**ארגון** להעביר נתונים לפי הצורך מהאחסון ולאחסון של CISP. ה-CISP יאפשר גם הורדת תמונות של מחשבים וירטואליים והעברתן לספק ענן חדש. ה-**ארגון** יכול לייצא את תמונות המכונה שלו ולהשתמש בהן בשטח או אצל ספק אחר (בכפוף להגבלות רישוי תוכנה).

2.3 אבטחה

אחריות אבטחה ותאימות מחולקת בין CISP ללקוחות ענן. במודל זה, לקוחות ענן שולטים כיצד הם מעצבים מבחינת ארכיטקטורה ומאבטחים את היישומים והנתונים שלהם על התשתית, בעוד ש-CISPs אחראים לספק שירותים בפלטפורמה מאובטחת ומבוקרת במיוחד, ולספק מגוון רחב של תכונות אבטחה נוספות. רמת האחריות של CISP ואחריות הלקוח במודל זה תלויה במודל פריסת הענן (IaaS/PaaS/SaaS) והלקוחות צריכים להיות ברורים לגבי האחריות שלהם בכל מודל.

הבנת מודל אחריות משותפת זה חיונית לתכנון RFP לרכישת שירותי ענן מוצלח. ארגונים במגזר הציבורי צריכים להבטיח שהם יודעים על מה אחראי CISP, על מה הם עצמם אחראים, והיכן שותפי ייעוץ/ISV והפתרונות שלהם משתלבים כדי לעזור.

2.3.1 דרישות מינימום

מילת המפתח בכל הנוגע לאבטחה בענן היא **יכולת**. ארגונים במגזר הציבורי צריכים להציב דרישות ל-CISPs, ולבקש מהם לספק את יכולות האבטחה הדרושות כדי להבטיח שלקוחות יוכלו לעמוד בתחומי האחריות שלהם במודל האחריות המשותפת. כפי שניתן לראות מרשימת הדרישות המייצגת להלן, ה-CISP מתבקש לספק יכולת מתוקנת, כך שהלקוח יוכל לנצל אותה כדי להפוך את סביבת הענן הייחודית שלו למאובטחת.

- **לספק חומות אש ויכולות חומת אש** של יישומי אינטרנט כדי ליצור רשתות פרטיות ולשלול בגישה למופעי שרת ויישומים.
- **לספק אפשרויות לקישוריות** המאפשרות חיבורים פרטיים או ייעודיים מהמשרד או מהאתר שלך.
- **לספק את היכולת** ליישם אסטרטגיית הגנה עמוקה ולסכל התקפות DDoS.
- **יכולות הצפנת נתונים** זמינות בשירותי אחסון ומסד נתונים.
- **לספק אפשרויות גמישות לניהול מפתחות**, המאפשרות לך לבחור אם לתת ל-CISP לנהל את מפתחות ההצפנה או לאפשר ללקוח לשמור על שליטה מלאה על המפתחות.
- **לספק API** עבור לקוחות לשילוב הצפנה והגנה על נתונים עם כל אחד מהשירותים שפותרו או נפרסו בסביבת ה-CISP.
- **לספק כלי פריסה לניהול היצירה וההשבתה** של משאבי CISP על פי תקני הארגון.
- **לספק כלי ניהול מלאי ותצורה המזהים משאבי CISP** ולאחר מכן עוקבים אחר שינויים במשאבים אלו לאורך זמן ומנהלים אותם.
- **לספק כלים ותכונות** המאפשרים ללקוחות לראות בדיוק מה קורה בסביבת ה-CISP שלהם.
- **לאפשר נראות** עמוקה לקריאות API - כולל מי, מה, מתי ומאיפה בוצעו שיחות.
- **לספק אפשרויות צבירת תיעוד**, ייעול חקירות ודיווח תאימות.
- **לספק יכולת להגדיר הודעות התראה** כאשר מתרחשים אירועים ספציפיים או חריגה מספים.
- **לספק יכולות להגדיר**, לאכוף ולנהל מדיניות גישת משתמשים בכל שירותי CISP.
- **לספק את היכולת** להגדיר חשבונות משתמש בודדים עם הרשאות על פני משאבי CISP.
- **לספק את היכולת** לשלב ולאחד עם ספריות ארגוניות כדי להפחית את התקורה הניהולית ולשפר את חוויית משתמש הקצה.

עוד מהדרישות הללו נמצאות ב-נספח א' - דרישות טכניות להשוואה בין משתתפים במכרז.

ניתן להשתמש בפונקציונליות מעבר לסטנדרט המינימלי לאבטחה לניתוח משמעותי יותר של "אפשרויות עם ערך מוסף" או "הערך הטוב ביותר" ב-RFP. וככל שיש יותר פונקציונליות מובנית או אוטומטית בכל הנוגע לאבטחה, כך ייטב. שוב, ראו את נספח א' - דרישות טכניות להשוואה בין משתתפים במכרז לדרישות להשוואה בין מציעים.

ארגונים במגזר הציבורי צריכים להסתכל על אישורי הסמכה בענן והערכות כדי להבטיח שבקורות האבטחה הנדרשות של CISP קיימות. לדוגמה: יש לשקול CISP שאומת ואושר על ידי מבקר בלתי תלוי כדי לאשר התאמה לתקן ההסמכה ISO 27001. ISO 27001 נספח A, תחום 14 צולל לעומק הבקורות הספציפיות ש-CISP מתנהל לפיהן, בהתאם לדרישות ISO סביב רכישה, פיתוח ותחזוקה של מערכת. סביר להניח שהבקורות הללו מכסות את רוב, אם לא את כל הבקורות סביב רכישה מערכות, פיתוח ותחזוקה של רוב ארגון ב-RFP הקשור ל-IT יבקש. לכן, סביר שארגון פשוט ידרוש ש-CISP יהיה מוסמך ISO 27001, במקום לשכפל את המאמצים ולפרט את דרישות הבקרה סביב רכישה, פיתוח ותחזוקה של מערכת ב-RFP לרכישת שירותי ענן.

ניתן ליישם גישה זו של מינוף דוחות תאימות של צד שלישי על רוב בקורות האבטחה והתאימות, למשל: קוד ההתנהגות של CISPE, ISO, SOC וכו'.

שפת RFP לדוגמה: אבטחה

ה-CISP יחשוף בפני ה<ארגון> את תהליכי האבטחה הלא קנייניים שלו ואת המגבלות הטכניות שלו כך שניתן יהיה להשיג הגנה וגמישות נאותים בין ה<ארגון> לבין ספק השירות.

ה-CISP יציין את תפקידיו ותחומי אחריותו בכל הנוגע לאבטחה ותאימות:

- בהצעה המוצעת יש לתאר את התפקידים ותחומי האחריות הקשורים לאבטחה של ה-CISP וה-**ארגון**. כדאי לכתוב באופן ברור לגבי תיחום תחומי האחריות, ולציין אילו שירותי CISP יכולים לסייע ל-**ארגון** בבנייה ובאוטומציה של פונקציות אבטחה בסביבת הענן שלו.
- יש לספק תשובות למפרט הטכני **בנספח א'** הקשור לדרישות האבטחה של ה-**ארגון**.

בעלות ושליטה על התוכן של **ארגון**

יש לתאר כיצד יכולות CISP עשויות להגן על פרטיות הנתונים של ה-**ארגון**. כדאי לכלול את הבקורות הקיימות כדי לטפל בהגנה על התוכן של ה-**ארגון**. CISP חייב לספק בידוד אזורי חזק, כך שאובייקטים המאוחסנים באזור לעולם לא יעזבו את האזור אלא אם ה-**ארגון** מעביר אותם במפורש לאזור אחר

- ה-**ארגון** ינהל את הגישה לתוכן, לשירותים ולמשאבים שלו. ה-CISP צריך לספק ערכה מתקדמת של תכונות גישה, הצפנה ורישום כדי לעזור ל-**ארגון** לעשות זאת ביעילות. ה-CISP לא ייגש לתכנים של ה-**ארגון** או ישתמש בהם לכל מטרה שאינה נדרשת על פי חוק ורק לצורך שמירה על שירותי ה-CISP ואספקתם ל-**ארגון** ולמשתמשי הקצה שלו.
- ה-**ארגון** יבחר את האזור/ים שבהם התוכן שלו יאוחסן. CISP לא יעביר או ישכפל את התוכן של ה-**ארגון** מחוץ לאזור/ים שנבחרו, למעט כנדרש על פי חוק וכנחוץ כדי לתחזק את שירותי ה-CISP ולספק אותם ל-**ארגון** ולמשתמשי הקצה שלו.
- ה-**ארגון** יבחר כיצד התוכן שלו יאובטח. CISP חייב לספק הצפנה חזקה עבור תוכן במעבר או במצב מנוחה של ה-**ארגון**, ולספק ל-**ארגון** את האפשרות לנהל בעצמו את מפתחות ההצפנה שלו.
- ל-CISP חייבת להיות תוכנית להבטחת האבטחה שמשתמשת בשיטות עבודה מומלצות לשמירה על פרטיות וההגנה על הנתונים כדי שה-**ארגון** יקים, יפעיל וימנף את סביבת בקרת האבטחה של ה-CISP. הגנות אבטחה ותהליכי בקרה חייבים להיות מאומתים באופן עצמאי על ידי הערכות בלתי תלויות מרובות של צד שלישי.

אישורי הסמכה והערכות בענן מספקים לארגונים במגזר הציבורי הבטחה של CISPs יש בקורות אבטחה פיזיות ולוגיות יעילות. כאשר נעשה מינוף של ההסמכות האלה ב-RFPs, הדבר מייצל את תהליך הרכישה, ועוזר למנוע תהליכים כפולים ומכבידים מדי או זרמי עבודה של אישור, שאולי אינם נדרשים בסביבת ענן.

RFPs של ענן צריכים לספק ל-CISPs הזדמנות להוכיח שהם עולים בקנה אחד עם הסמכות והערכות תאימות. כפי שצוין לעיל, קיימת חפיפה ניכרת בתרחישי סיכונים ובשיטות עבודה לניהול סיכונים בכל תוכניות ההסמכה הללו, וככל שהבקורות והדרישות משולבות יחד בהסמכות מסוג זה, הדרישה שה-CISPs יעמדו בהסמכות היא דרך מהירה יותר לטפל בתאימות ב-RFP מאשר לשכפל את המאמץ ברישום בקורות בודדות שכאלו (שרבות מהן עשויות להילקח מ-RFPs קודמים שנמצאים ישירות במרכזי הנתונים באתר, וככאלו עשויות שלא לחול על מחשוב ענן).

הערה: חשוב מאוד גם להבין כיצד ניתן לגשת לדוחות המפורטים להלן. לדוגמה, דוחות SOC 1 ו-SOC 2 הם בדרך כלל מסמכים רגישים. יש להבין את ההסכמים הדרושים כדי לגשת אליהם (למשל, הסכם סודיות - NDA) ואין לבקש להגיש את המסמכים האלה כחלק מתגובת ה-RFP (מסמכים אלה יכולים להתפרסם באמצעות פעולות Open Records או חקיקה דומה המסכנת את אבטחת הענן).

שפת RFP לדוגמה: תאימות

השימוש בתקני אבטחה, תאימות ותפעול מוכרים, הנגזרים משיטות עבודה מומלצות בתפעול שירותי ענן - לרבות טיפול בנתונים, אבטחת נתונים, סודיות, זמינות וכו' - הופך את רכישת טכנולוגיית הענן לחלקה.

ה-**ארגון** יעריך הצעות ייחודיות מול תקני אבטחה, תאימות ותפעול מקובלים כמפורט להלן **ובנספח א'**. על סמך אישור התאימות של הספק מול כל תקן, ה-**ארגון** יכול להשתמש בתאימות מינימלית מול התקן בתור הבסיס להערכת ההצעה.

דרישה מה-CISP להמשיך לעמוד בתקן המינימלי לאורך חיי החוזה מעניקה יתרון בשמירה על תאימות השירות עדכנית.

ה-CISP שלגביו משתתפים במכרז (באופן ישיר או באמצעות מפיץ) אמור להיות מסוגל להוכיח את יכולתו לעמוד בהסמכות, בדוחות ובאישורים של גורמי הצד השלישי העצמאיים הבאים (הערה - אם חלק מההסמכות, הדוחות והאישורים הללו נמצאים תחת מגבלות גילוי בשל נושאי אבטחה, ה-**ארגון** יעבוד עם ה-CISP כדי לקבל גישה מוסכמת משותפת):

אישורים \ הסמכות	חוקים, תקנות ופרטיות	התאמות \ מסגרות
CS (גרמניה) ☐		CDSA ☐
☐ קוד התנהגות להגנה על המידע של CISPE (GDPR)		
☐ CNDPCP (הסכם ניטרליות אקלימית של מרכזי נתונים)		
DIACAP ☐	☐ צו הגנת מידע של האיחוד האירופי	CIS ☐
DoD SRG רמות 2 ו-4 ☐	☐ סעיפים במודל האיחוד האירופי	☐ מידע על משפט פלילי שירות (CJIS)
HDS (צרפת, שירותי בריאות) ☐		
FedRAMP ☐	FERPA ☐	CSA ☐
FIPS 140-2 ☐	GDPR ☐	☐ מגן הפרטיות של האיחוד האירופי-ארה"ב
ISO 9001 ☐	GLBA ☐	☐ נמל מבטחים של האיחוד האירופי
ISO 27001 ☐	HIPAA ☐	FISC ☐
ISO 27017 ☐	HITECH ☐	FISMA ☐
ISO 27018 ☐	IRS 1075 ☐	G-Cloud [בריטניה] ☐
IRAP [אוסטרליה] ☐	ITAR ☐	GxP (FDA CFR 21 חלק 11) ☐
MTCS שכבה 3 [סינגפור] ☐	PDPA – 2010 [מלזיה] ☐	ICREA ☐
PCI DSS רמה 1 ☐	PDPA – 2012 [סינגפור] ☐	IT Grundschatz [גרמניה] ☐
SEC כלל (f) 17-a-4 ☐	PIPEDA [קנדה] ☐	MARS – E ☐
SecNumCloud (צרפת) ☐		
SOC1 / ISAE 3402 ☐	☐ חוק הפרטיות [אוסטרליה]	MITA 3.0 ☐
SOC2 / SOC3 ☐	☐ חוק הפרטיות [ניו זילנד]	MPAA ☐
SWIPO IaaS ☐		
	☐ הרשות הספרדית DPA	NIST ☐
	☐ בריטניה DPA - 1988	Uptime Institute Tiers ☐
	☐ VPAT/חלק 508	☐ עקרונות אבטחת ענן בבריטניה

הרשימה שלהלן סופקה למטרות המחשה בלבד ואין לראות בה כממצה את האישורים והתקנים שיכולים לחול על שירותי ענן.

2.3.1.1 הגנה על נתונים

שיקול מרכזי בעת שימוש בשירותי ענן הוא שהעיבוד של נתונים אישיים מתבצע בהתאם לחוק הגנת המידע החל באיחוד האירופי, לרבות תקנת הגנת המידע הכללית (GDPR). GDPR היא תקנה המבוססת על עקרונות ולכן אינה מספקת הנחיות ספציפיות למגזר כדי לסייע בהבטחת תאימות. עם זאת, GDPR מעודדת אימוץ של כלי תאימות כגון קודים של התנהגות כדי לספק הנחיות כאלה. CISPE, בעבודה עם הרשות הצרפתית להגנת מידע (CNIL) פיתחה קוד התנהגות להגנה על מידע (CISPE Code⁶) שאושר על ידי המועצה האירופית להגנת מידע עם ישימות כללית באירופה. מטרת הקוד היא לסייע ל-CISPs לציית ל-GDPR ולהנחות לקוחות בזמן ההערכה האם CISPs מתאימים לעיבוד נתונים אישיים שהלקוח מעוניין לבצע.

- הקוד מתמקד אך ורק במגזר IaaS ומתייחס לתפקידים ולתחומי האחריות הספציפיים של ספקי IaaS.
- הקוד עוזר להבהיר את ההיבטים של עיבוד הוגן ושקוף ואת אמצעי האבטחה המתאימים בהקשר של שירותי תשתית ענן (GDPR, סעיף 40 [2]).
- בנוסף הוא עוזר ללקוחות להבין איך הם יכולים לשמור את הריבונות על הנתונים שלהם תוך הבטחה שהם נשארים בתוך האיחוד האירופי.
- הוא מקדם שיטות עבודה מומלצות להגנה על נתונים התומכות ביוזמת GAIA-X של האיחוד האירופי לפיתוח שירותי נתוני ענן אירופיים.

תאימות של CISP לקודי התנהגות להגנה על נתונים כגון קוד CISPE מספקים הבטחה שהנתונים האישיים יעובדו תוך תאימות קפדנית ל-GDPR.

שפת RFP לדוגמה: הגנת נתונים

ה-CISP שמוצע למכרז (שירות או באמצעות מפיץ) אמור להיות מסוגל להוכיח את יכולתו לציית לקוד התנהגות להגנה על נתונים כגון קוד CISPE. קוד הגנת הנתונים חייב להתאים לדרישות שנקבעו במסגרת ה-GDPR. הקוד צריך לכלול לכל הפחות: (1) הגדרה ברורה של התפקידים ותחומי האחריות של ה-CISP, (2) הדרישה שה-CISP לא ישתמש בנתוני לקוחות למטרות שיווק או פרסום, וכן (3) את היכולת של הלקוחות לבחור בשירותי CISP המאפשרים עיבוד נתונים בתוך האזור הכלכלי האירופי כולו. תאימות בקוד חייבת להיות מאומתת על ידי מבקרים חיצוניים בלתי תלויים (גופי פיקוח) המוסמכים על ידי מבקרים חיצוניים בלתי תלויים שהוסמכו על ידי הרשות האירופית להגנת מידע.

2.3.1.2 החלפת ספקי ענן והעברת נתונים

הלקוחות צריכים את החופש לבחור בשירותי הענן שהם רוצים להשתמש בהם, ולא להיות 'נעולים' על ידי ספק CISP או PaaS/SaaS.

שירותי הענן המסופקים על ידי CISP הם מתוקננים ומוצעים על בסיס "אחד לרבים", כאשר השירותים מוגדרים, מוקצים ונשלטים על ידי הלקוח. היתרון של מחשוב ענן הוא שללקוחות יש את היכולת לבחור את השירותים המתוקננים שהם צריכים כדי לפתח את היישומים והפתרונות הייחודיים להם. הטבה זו כוללת גם את היכולת לעבור לשירותים חדשים או שונים המתאימים בצורה הטובה ביותר לצורכי הלקוח בכל זמן.

כמו בהגנה על נתונים, קודי התנהגות יכולים לעזור לספק ללקוחות הבטחה וביטחון בכל הנוגע למעבר לענן מתשתית בשטח, או בעת מעבר בין CISPs. יחד עם EuroCIO (האיגוד האירופי של CISPE, CIOs) כיהנה כיו"ר משותף בפיתוח קוד ההתנהגות לניידות נתונים ומעבר לשירותי ענן מסוג IaaS (קוד SWIPO IaaS⁷). הגרסה הראשונה של הקוד פותחה בהתאם לתקנת הזרימה החופשית של האיחוד האירופי, שנמסרה לנציבות האירופית בנובמבר 2019 במסגרת נשיאות האיחוד האירופי הפינית ופורסמה על ידי עמותת SWIPO AISBL במאי 2020. באפריל 2021, הוכרזו השירותים הראשונים שמצייתים לקוד של SWIPO AISBL, ובמאי 2021 הוכרזו שירותי החברים הראשונים ב-CISPE שמצייתים לקוד.

⁶ <https://cispe.cloud/code-of-conduct/>

⁷ <https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security>

⁸ <https://swipo.eu/>

שפת RFP לדוגמה: החלפת ספקי ענן והעברת נתונים

ה-CISP שמוצע למכרז (שירות או באמצעות מפיץ) אמור להיות מסוגל להוכיח את יכולתו לציית לקוד ההתנהגות 'החלפה והעברת נתונים' כגון קוד SWIPO IaaS. הקוד חייב לפרט כיצד CISP מציע ללקוחות העברה בטוחה של נתונים עסקיים, אם יחליטו לעבור מ-CISP.

2.3.2 השוואה בין ספקים

בדומה לקריטריונים הטכניים בסעיפים לעיל, בנוסף לדרישות האבטחה המינימליות ב-RFP לרכישת שירותי ענן, חשוב לספק קריטריונים לפיהם ניתן להשוות את יכולות האבטחה והשירותים של CISP במהלך הערכה תחרותית.

מומלץ לעיין בנספח א' - דרישות טכניות להשוואה בין משתתפים במכרז דרישות אבטחה לדוגמה של CISP. אנחנו ממליצים בחום שהיכולות שלהלן יהיו שיקולי אבטחה מרכזיים עבור גופים במגזר הציבורי המעריכים CISOs:

שפת RFP לדוגמה: שיקולי אבטחה מרכזיים

- הבנת CISP של מודל האחריות המשותפת, ותיעוד שיעזור ללקוחות להבין את תחום אחריות האבטחה עבור תכונות ושירותי CISP (לדוגמה, בהקשר של GDPR)
- היסטוריה מוכחת של אבטחת תשתית CISP, עם תיעוד זמין לציבור שאינו קנייני של מצב אבטחת CISP ובקורות פיזיות/לוגיות
- תמיכת CISP ספציפית לאבטחת ענן
- שירותים המאפשרים ללקוחות להפוך את עיצוב החשבון לרשמי, להפוך בקורות אבטחה ומשילות בענן לאוטומטיות ולהפוך את הביקורת לחלקה
- היכולת ליצור, להקצות ולנהל אוסף של משאבים בצורה דמוית תבנית (כולל תבניות אבטחה בנויות בתקן זהב של CISP/CISP-Partner)
- היכולת לבסס תפעול אמין של בקורות ושניתן לחזור עליו
- תכונות לביקורת רציפה ובזמן אמת
- היכולת לבנות סקריפט טכני של מדיניות משילות בענן
- היכולת ליצור פונקציות כפייה שמשתמשים שאינם מורשים לשנות את הפונקציות האלה לא יכולים לעקוף
- היכולת לבצע הטמעה אמינה של מה שנכתב בעבר בקווי המדיניות, בתקנים ובתקנות, יחד עם יצירת אבטחה ותאימות ניתנים לאכיפה, אשר בתורם יוצרים מודל משילות בענן אמין ופונקציונלי עבור סביבות IT
- שירותים להגנה מפני התקפות מניעת שירותי מבוזרות (DDoS) ושכבת תחבורה הנפוצות, השכיחות ביותר ברשת, יחד עם היכולת לכתוב כללים מותאמים אישית כדי למתן את התקפות שכבת היישומים המתוחכמות
- שירות זיהוי איומים מנוהל

2.3.3 התקשרות בחוזה

כפי שצוין לעיל, התנאים וההגבלות של CISP נועדו לשקף את אופן פעולתו של מודל שירותי ענן (נכסים פיזיים אינם נרכשים, ו-CISOs פועלים בסקיל מסויבי ומציעים שירותים מתוקננים); לפיכך, זה קריטי שהתנאים וההגבלות של ה-CISP יהיו משולבים ויונצלו במידה המרבית האפשרית. יש לעיין בסעיף 2.5 שלהלן לקבלת מידע נוסף על תנאים והגבלות והתקשרות.

בכל הנוגע לאבטחה, אנחנו שוב ממליצים בחום לאפשר ל-CISOs לעדכן כל הזמן הצעות, או שספקים יורשו להוסיף מוצרים לאחר מועד ההגשה, כל עוד הם תואמים לפרמטרים המקוריים של ה-RFP. העדכון הזה משקף את העובדה שתכונות ושירותי אבטחה מתפתחים במהירות, ו-CISOs משחררים שירותים ממוקדי אבטחה לעתים קרובות, כך שבמקרים רבים ניתן להשתמש בהם בחינם. יש לשים לב כי חשוב שתהיה רמת אבטחה בסיסית (יש לעיין בדרישות המינימום שלעיל) כדי להבטיח שהשינויים בהצעות האבטחה לא יהיו מזיקים.

מודל האחריות המשותפת נמצא כמובן בליבת האבטחה ב-RFP לרכישת שירותי ענן. כל צד צריך להיות ברור לגבי תחומי אחריות האבטחה שלו, ויש לדרוש מ-CISOs לתעד את תחומי אחריות האבטחה של CISP/לקוח עבור טכנולוגיות ענן המסופקות על ידי CISP, יחד עם תיעוד שיעזור ללקוחות לשלב שיטות אבטחה מומלצות ולהפוך אותן לאוטומטיות.

הסכם מסגרת לטכנולוגיית ענן צריך לספק גמישות להסרת ספק אם הוא לא יעמוד עוד בדרישות האבטחה והתאימות המינימליות כפי שנקבעו ב-RFP לרכישת שירותי ענן.

2.4 תמחור

כדי לקבל חוזה עבור טכנולוגיית ענן בצורה שתתחשב בביקוש משתנה, ארגונים במגזר הציבורי זקוקים לחוזה המאפשר להם לשלם עבור שירותים תוך כדי צריכתם - עם המשילות והנראות של הענן הנדרשות בשל השימוש וההוצאות.

חשוב לציין, RFPs לרכישת שירותי ענן צריכים להסתכל על הערך ועלות הבעלות הכוללת (TCO), בניגוד להשוואה פשוטה בין תפוחים לתפוחים של מחירי יחידות. שיטת עבודה מסורתית זו של הסתכלות על מחיר היחידה הנמוך ביותר אינה מתורגמת למודל הענן, וככזאת אינה נוטה להוביל למכרז החסכוני ביותר, או למחיר הנמוך ביותר.

כדי לסייע בהערכת תמחור CISP, כדאי קודם כל לקבל הסמכה מוקדמת של CISP או רשימה קצרה, עם **דרישות מינימום הקשורות לתמחור**, כך ש-CISPs עם יכולות דומות יהיו זכאים להסכם המסגרת. תהליך ההערכה לחוזים מרוכזים ותחרויות זעירות יכול לחפש מבחר ארכיטקטורות ענן טיפוסיות לדוגמה **ותרחיש תמחור** התואמים מספר עומסי עבודה טיפוסיים של המגזר הציבורי ולאפשר ל-CISPs לתמחר אותם. הבדיקות על מערכות אמיתיות מומלצות גם כדי לאפשר השוואת ביצועים ואלסטיות של שירותי טכנולוגיות ענן הניתנות על ידי CISPs. יש לעיין בנספח ב' לסקריפט בדיקה לדוגמה עבור טכנולוגיות ענן.

2.4.1 דרישות מינימום

סעיף התמחור ב-RFP לרכישת שירותי ענן כולל ארבעה מרכיבי מפתח:

1. **תמחור שירותים:** לקוחות ענן משלבים מודל שירות של תשלום לפי שימוש, שבו בסוף כל חודש הם פשוט משלמים על השימוש שלהם, והדבר אופטימלי עבור מדדי ניצול ומשאבים.
2. **תמחור שקוף:** תמחור CISP צריך להיות זמין ציבורית ושקוף.
3. **תמחור דינמי:** יש לכלול את הגמישות כדי לאפשר למחירי הענן להשתנות בהתאם לתמחור בשוק. גישה זו מנצלת את האופי הדינמי והתחרותי של תמחור בענן, ותומכת בחדשנות ובהורדות מחירים.
4. **הוצאה מבוקרת:** CISPs צריכים לספק כלי דיווח, ניטור וחיזוי המאפשרים ללקוחות (1) לנטר את השימוש וההוצאה הן ברמה הכללית והן ברמה פרטנית, (2) לקבל התראות כאשר השימוש וההוצאות מגיעים לספים מותאמים אישית, ו-(3) להעריך את השימוש וההוצאות על מנת לתכנן תקציבי ענן עתידיים.

שפת RFP לדוגמה: תמחור

«ארגון» מבקש שה-CISPs המגיבים יכללו את מודל השיטה המוצעת והתמחור שלהם לאספקת כל אחד מהשירותים שלהם למשתמשי קצה ביכולת ענן מסחרית.

ה-CISP יספק:

- מסמך הגדרת שירות או קישורים להגדרות שירות
- מסמך תנאים והגבלות
- מסמך תמחור (קישורים לתמחור ציבורי מקובלים בהנחה שמחירון מלא/מסמך תמחור זמין לפי בקשה)

המחיר יהיה עלות התצורה הנפוצה ביותר של השירות. CISPs צריכים לספק אפשרויות להנחות מבוססות נפח, וכלים לחישוב מחירים כדי לחשב את המחיר האמיתי של מה שנרכש, ואת הערך הכולל הניתן ללקוח (לדוגמה, שירותי אופטימיזציה והפחתת עלויות כתוצאה מכך).

רוכשים במסגרת הסכם המסגרת רשאים לדבר עם ספקים כדי לבקש מהם להסביר את תיאור השירות, התנאים וההגבלות, התמחור או מסמכי/מודל הגדרת השירות שלהם. יישמר תיעוד של כל שיחה עם ספקים.

דרישות תמחור נוספות

- לספק טכנולוגיות ענן עם מודל תמחור דינמי המעניק גמישות עסקית מרבית ומאפשר מדרגיות וצמיחה.
- מאפייני התמחור חייבים לכלול את הדברים הבאים:
 - האם התמחור מסופק בשירותי שלום לפי שימוש בפועל, בסגנון שירות? יש להסביר את מודל התמחור שלך.
 - האם ניתן להשיג הנחות נוספות כאשר מתחייבים לשימוש ו/או קנייה בכמויות? יש לספק פרטים כיצד לעשות זאת.
 - האם התמחור זמין ציבורית ושקוף? יש לכלול קישורים לתמחור הזמין ציבורית.
 - האם תמחור דינמי ומגיב במהירות ויעילות לתחרות בשוק?
 - האם מסופקות שיטות עבודה מומלצות ומשאבים לעקוב אחר הוצאות?
 - האם מסופקות שיטות עבודה מומלצות ומשאבים לאופטימיזציה של עלות?

תמחור שקוף

בשל מגמת הירידה המתמדת בטכנולוגיות ענן מסחריות המונעות על ידי חדשנות ותחרות, עלות יחידת השירות המדודה של CISP המשולמת על ידי **ארגון** תחת הסכם המסגרת, לעולם לא תחרוג מתמחור יחידות ספק הענן המתפרסם באתר האינטרנט של ספק הענן והוא בתוקף באותו הזמן שיחידת השירות נצרכת על ידי הלקוח.

התראות/דוחות תקצוב וחיוב

כדי להדגים אספקה של טכנולוגיות ענן ושימוש בהן, CISP צריכים לספק ל**ארגון** את הכלים להפקת דוחות חיוב מפורטים המפרטים את העלויות לפי שעה, יום או חודש; לפי כל חשבון בארגון; לפי מוצר או משאב מוצר; או על ידי תגים המוגדרים על ידי הלקוח. **ארגון** מכיר בכך שבחלק ממודל האחריות המשותפת בענן, ה**ארגון** יהיה אחראי לשימוש בתכונות ובכלים של תקציב וחיוב שסופקו על ידי CISP כדי לעמוד בדרישות הייחודיות לתחזיות ודיווח.

- יש לספק מידע לגבי האופן שבו **ארגון** יכול להציג מידע חיוב הן ברמת פירוט והן ברמת סיכום, תוך הצגת דפוסי הוצאות על משאבי CISP לאורך זמן, בנוסף לחיזוי הוצאות עתידיות.
- יש לספק מידע לגבי האופן שבו **ארגון** יכול לסנן תצוגת שימוש/חיוב לפי שירות, לפי חשבון מקושר או לפי תגים מותאמים אישית המוחלים על משאבים, וליצור התראות חיוב ששולחות הודעות כאשר השימוש בשירותים מתקרב לספים/לתקציבים המוגדרים של ה**ארגון** או חורג ממנו.
- יש לספק מידע לגבי האופן שבו **ארגון** יכול לחזות בכמה שירותי ענן הוא משתמש במהלך תקופת זמן חזויה מוגדרת, בהתבסס על השימוש בעבר. CISP צריך להציע **הערכה** של כמה יצא חיוב CISP של **ארגון**, ולאפשר ל**ארגון** להשתמש בהתראות ובתקציבים לסכומים שהם צפויים להשתמש בהם, כדי לקבל משילות רבה יותר על העלויות וההוצאות.

2.4.2 השוואה בין ספקים

ארגונים במגזר הציבורי דורשים לעתים קרובות תחרות בין משתתפים במרכז תוך שימוש בקריטריונים להערכה כמו התמורה הטובה ביותר, המכרז המשתלם ביותר כלכלית (MEAT), או המחיר הנמוך ביותר. כאשר מתכננים תמחור של חוזים מרוכזים או תחרויות זעירות בהסכם מסגרת, חשוב לבנות גישה שלוקחת בחשבון את התכונות הייחודיות של הענן. לדוגמה, ההבנה שרק השוואה של פריטי קו בין הצעות של ספקי ענן (למשל: מחשוב או אחסון) אינה דרך יעילה להשוואה, מאחר שהיא לא לוקחת בחשבון תכונות כגון ביצועים, אופטימיזציות עלויות באמצעות שירותים מותאמים לסביבת ענן וכלי ניטור CISP, או שירותים מבדילים שהם CISP עשויים להציע בחינם. בנוסף, המחיר הקטלוגי של CISP יכול להיות עשרות אלפי פריטים, דגמי התמחור שונים משירות אחד למשנהו ומספק אחד למשנהו.

ניתוח TCO

אנחנו ממליצים להתמקד בעלות כוללת (TCO) של מקרי שימוש מוגדרים, אשר לוקחים בחשבון את כל ההיבטים של פתרונות ענן (כולל שירותי שותפים, הנחות CISP מתוקננות, תכונות טכניות שיכולות להגביר את הביצועים ולהפחית/לייעל עלויות, וכו').

השוואה לפי תרחישים

תהליך ההערכה יכול לשקול גם את התרחישים האופייניים המתאימים למערכות או יישומים נפוצים. תרחישים כאלה (דברים כמו אירוח אתרים, או הטמעה של מערכת משאבי אנוש עם מספר x של משתמשים וכו') יכולים לכלול משתני זמן כמו מהירות והיקף המשאבים, ביצועי היישום או הפתרון, זמני גישה לאחסון, נתונים מורכבים בנפח נמוך בהשוואה למשימות

מחשוב פשוטות עם נפח גבוה וכו'. ליישומים או למערכות יכולים להיות גם תרחישים אופייניים כגון עיבוד של נפח גבוה בעת החזר המס, הודעות חירום כגון אזהרות הצפה. התרחישים צריכים להיות מקיפים כדי לכלול את היקף הטכנולוגיה והשירותים שבהם הלקוח עשוי להשתמש במהלך הפרויקט. כך, הלקוח יכול להשוות את העלות הכוללת המשוערת של הפרויקט.

השוואת תרחישים מבחינה פיננסית וטכנית

חשוב גם לקחת בחשבון יתרונות טכניים בעת השוואת תמחור בין הצעות CISP. לדוגמה, CISP אחד עשוי לאפשר ללקוחות לבנות טופולוגיה מסוג פעיל-פעיל (Active-Active) של התאוששות מאסונות (DR) הודות למודל שלו של מרכזי נתונים באשכולות בתוך אזור גאוגרפי. CISP שאין לו סוג כזה של יתירות ותצורת מרכז נתונים עשוי להיות יקר ב-X% בהתחשב בעלות של שילוב צורכי התאוששות מאסונות. כדוגמה מדוע גישה הוליסטית לתמחור הכוללת תכונות טכניות נוספות היא חיונית להערכת CISP, יש לשקול את האלטרנטיבה למטה של השוואה ישירה - תפוחים לתפוחים.

דוגמה: לקוח רוצה להשוות את המחיר של אחסון אובייקטים המסופק על ידי CISP מוסמכים על הסכם מסגרת. המחיר של הפרויקט 'יחידת אחסון' מ-1 CISP הוא € 0.023 GB. המחיר של אותה 'יחידה' מ-2 CISP הוא € 0.01 GB. בהשוואה פשוטה של יחידה ליחידה, הלקוח לא ישאל שאלות קריטיות כמו:

1. כמה עותקים מיותרים של האובייקט זמינים במקרה של כשל? בדוגמה לעיל, 1 CISP מתוכנן לשמור על אובדן ב-זמנית של נתונים בשני מתקנים שונים ושומר על מספר עותקים של נתונים. במקרה של 2 CISP, לא נוצרים עותקים מיותרים.
2. מהי רמת הקיימות של חפצים מאוחסנים? 1 CISP הוא 99.999999999% CISP 2 הוא 99%.
3. יש לקחת בחשבון את העלות לאורך חיי הבעלות על הפרויקט או עומס העבודה הכולל, וכיצד תכונות של אופטימיזציות עלויות יכולות להפחית עלויות בכל הנוגע לאופן האחסון והשימוש בנתונים (לדוגמה, הגדלת השימוש בפונקציות לא מנוהלות של CISP יכולה להפחית עלויות ב-X%).

אלו הם רק חלק משיקולים טכניים רבים אחרים המשפיעים על התמחור, במיוחד הקשורים לאבטחה ותאימות.

שיקולים לתרחישי תמחור כוללים

תעריפי בסיס - אלה הם בעצם מחירים ציבוריים של CISP. CISP צריכים לספק מחירים אלה בפומבי; עם זאת, כפי שצוין לעיל, כדי להשוות ביעילות בין CISP, לקוחות יכולים לבקש אולי 3-5 תרחישים ספציפיים (או מספר תרחישים הגיוני עבור הלקוח) שיתומחרו על ידי כל הספקים. תרחישים צריכים להיות מקיפים כדי לכלול את רוחב השירותים והטכנולוגיות שהלקוח עשוי להשתמש בהם במהלך הפרויקט. כך, הלקוח יכול להשוות את העלות הכוללת המשוערת של הפרויקט. השוואות ברמת פריט קו/מק"ט נטות להיות בעייתיות יותר מאשר מועילות ללקוחות ולספקים (הלקוחות יצטרכו להשוות בין עשרות אלפי פריטים בין כל ה-CISP, והספקים יצטרכו לספק רמת פירוט זו ולנהל אותה. כאשר המחיר בפועל נקבע רק על סמך צריכת השירות).

הערכת מערך היכולות הכולל של CISP היא הכרח עבור לקוחות ענן המעוניינים לקבל את התמורה הטובה ביותר. לדוגמה, ל-CISP עשויים להיות מספר שירותים שהם חיוניים או כמעט חיוניים, והערכת תמחור צריכה לקחת בחשבון שירותים כאלה, ו-CISP אחרים עשויים לגבות תשלום עבור פונקציונליות דומה.

קריטריוני הערכה יכולים להיכתב בצורה כזו שתאפשר ל-CISP להשבית את התכונות "הכלולות x ברירת המחדל" שלהם, וכיצד יש לשירותים כאלה השפעה על העלות הכוללת. קריטריוני הערכה יכולים גם להסתכל על תמחור מבוסס נפח/שכבות של CISP והנחות זמינות מסחרית כגון מופעי שרת שמורים/מופעי שרת נקודתיים. לדוגמה:

- חיסכון של x% אם לקוחות רוכשים קיבולת מחשוב שנשמרה (שנה, 3 שנים וכו')
- הנחה של x% על תמחור בשכבות/נפח
- חיסכון של x% מבוסס על סקירות ארכיטקטורה ואופטימיזציה של תשתית כגון מעבר לאפשרות המחשוב שבהתאמה טובה יותר
- כפי שצוין לעיל, יש לקחת בחשבון את עלות החיים השלמה, וכיצד תכונות אופטימיזציה של עלויות יכולות להפחית את העלות

תרחיש תמחור

על המשתתפים במכרז לספק תמחור עבור התרחיש שלהלן רק למטרות הערכה. המחיר בפועל יתבסס על צריכת שירותים לפי מודל של תשלום לפי שימוש בפועל.

להלן דרישות ייצוגיות לצורך גילוי מחירים והן ניתנות מתוך הבנה מפורשת כי במהלך תקופת ההתקשרות הדרישות הנומיליות הללו ישתנו. יש לספק תמחור עבור 12 ו-36 חודשים תשלום לפי שימוש בפועל וגם עבור קיבולת שנשמרה של 12 ו-36 חודשים.

יש לספק את:

- שם הפתרון המוצע (או הפתרונות המוצעים):
- התמחור הטוב ביותר של המשתתף במכרז:
- שעות השירות: 24X7X365
- זמינות השירות: 99.95%

תרחישי תמחור יכולים לכלול גם דוגמאות מלקוחות קיימים עם עומסי עבודה דומים, שמיטבו את ההוצאה שלהם במשך 1/2/3 שנים - באמצעות שימוש בכלי ניטור ואופטימיזציה של CISP, אימוץ פתרונות מקוריים בענן ממוטבים, ודרך הפחתת מחירי CISP.

2.5 הגדרות ביצוע חוזה/תנאים והגבלות

CISP שסופק עם טכנולוגיות ותפעול בענן הוא במהותו מתוקנן, ולכן גם התנאים החוזיים מתוקננים. עם זאת, ישנה יכולת לבחון באופן שולי את החוזים הללו כדי שיתאימו להקשרים חקיקתיים ורגולטוריים מקומיים.

לעתים קרובות שיטות רכש IT מסורתיות כוללות כללים נוקשים המחייבים את הפונים לעמוד בדרישות רבות או בכל הדרישות של הרכש או שהם יידחו. או שאולי הם כוללים תת-מערך קפדני של דרישות חובה. מחלקות הרכש נוטות להיכשל בעת שימוש בשיטת מיקור מסוג זה עם טכנולוגיות ענן, שהן באמת מערך של רכיבים וכלים מתוקננים שעוזרים לך לתכנן פתרון מותאם אישית.

2.5.1 תנאים והתניות

הצעד הראשון בכל הנוגע להתקשרות ב-RFP לרכישת שירותי ענן הוא לסקור ולהבין מונחים מסחריים קיימים של CISP אשר, במקרים רבים, ניתן למצוא בפומבי באתרי CISP. לגופים במגזר הציבורי נוח יותר ויותר לקבל מונחים מסחריים מ-CISPs. חלק מהמאמץ הזה להבין מונחים הוא להיפגש עם CISPs ושותפיהם כדי להבין לעומק את הגישות שלהם. שאלת המפתח שיש לשאול היא 'מדוע' CISPs פועלים עם מונחים ספציפיים. חלק מהמונחים הללו עשויים להיראות שונים ממונחי IT מסורתיים, אבל יש סיבות מאוד ספציפיות 'למה' הם חלק מחוזה ענן. אם המונחים הזמינים לציבור אינם מקובלים, ל-CISPs יש לעתים קרובות הסכמים הניתנים לשינוי קל עבור לקוחות ארגוניים שניתן לחקור לגביהם.

יחד עם סקירת התנאים וההגבלות של ה-CISP, חשוב להבין את המדיניות, התקנות ו/או החוקים הקיימים (למשל: אלה הכוללים טכנולוגיה, סיווג נתונים, פרטיות, כוח אדם וכו'). לעיתים קרובות ישנן מדיניות/תקנות/חוקים קיימים המיועדים לקנייה ושימוש בהצעות IT מסורתיות, והם יכולים להיות מנוגדים למודל של CISP. לדוגמה, מתן אפשרות רק לשימוש בטכנולוגיות ענן שנכללו בהצעת הסכם המסגרת המקורית באמצעות RFP לרכישת שירותי ענן. CISPs מוסיפים כל הזמן שירותים חדשים וכן תכונות חדשות. אין היגיון עבור לקוח הקצה לחנוק את הגישה לשירותים החדשים האלה רק כי עוקבים אחר גישת רענון מוצרי IT מסורתית. אם זה המקרה, חשוב לקיים דיונים מעמיקים עם CISPs הכוללים התבוננות במדיניות/תקנות ו/או חוקים אלו.

כדאי לנצל את היתרונות של דיונים לפני RFP

כפי שצוין לעיל, לפני ניסוח RFP, כדאי להקדיש זמן לפגישה עם CISPs והספקים הקשורים כדי להבין את התנאים וההגבלות שלהם וללמד אותם על הגישה, המדיניות, התקנות והחוקים של הישות שלך. החלק החשוב ביותר בדיונים הללו הוא ששני הצדדים ילמדו 'מדוע' המונחים הרלוונטיים עובדים כפי שהם עובדים. לדוגמה, התנאים וההגבלות בענן שונים מאלו של מרכז נתונים מסורתי, שירות מנוהל, חומרה, תוכנה מהניילון ומונחי שילוב מערכות. מכיוון שהם מודלים בודדים וברוכים בחדשנות מתמדת, המודלים העסקיים שלהם דורשים שתהליך ה-RFP יהיה גמיש מספיק כדי לאפשר משא ומתן או דיונים כדי לקבל הבהרה.

על ידי הכללת היכולת להבהיר תנאים והגבלות לאורך דיונים או משא ומתן, ארגונים במגזר הציבורי משיגים הבנה רבה יותר של מודלים בענן ונמנעים מהבעיה של דחיית ספקים שבאמת עשויים לענות על צרכי הארגון. תהליך טיפוס אחד הוא שהארגון יזהה מראש מונחים מסוימים שהוא מוכן לדון בהם ולנהל משא ומתן לפני מתן המענק. על ידי משא ומתן על מונחים מקובלים עם המציעים מראש, הארגון מבטיח שהוא מקבל את ההתאמה הטובה ביותר למענק ופותר מחלוקות שאחרת עלולות לגרום לדחיית הצעה יעילה. גופים במגזר הציבורי יכולים גם לסקור את המדיניות, התקנות והחוקים שלהם, ושני הצדדים יכולים להבין כיצד השימוש בענן ישתלב במודלים אלה. פעמים רבות, יש דרכים לעבוד עם הסעיפים הקיימים. עם זאת, אם יש תחום בעייתי, שני הצדדים יכולים לעבוד יחד כדי למצוא פתרון (עדיף לקיים את הדיונים הללו הרבה לפני כל RFP ומשא ומתן חוזי שבהמשך).

גמישות במשא ומתן

כדי להיות מסוגלים לחתום על חוזים תוך תאימות לחקיקה המקומית ותוך הסתמכות על מונחים חוזיים מתוקננים על ידי CISP, מומלץ (1) לבקש מהפונים את החוזה האחיד שלהם, (2) לא לחקוק תנאים חוזיים לא מתאימים בעת הקמת הסכם המסגרת ל-RFP לרכישת שירותי ענן, ו-(3) לספק אפשרות למשא ומתן על כל הוראות הייעוץ וההצעות שיביאו להסכם המסגרת (למעט, כמובן, סעיפי החובה המחייבים בחוק).

הערה: היקף האחריות המשותפת טבוע במודל הענן וצריך לבוא לידי ביטוי במונחי החוזה (למשל, ה-CISP מאשר שהלקוחות הם הבעלים של הנתונים שלהם, של המיקום שלהם, ומספק כלים להבטיח שהבחירה במיקומי הנתונים היא מוגבלת - אבל - באחריות הלקוח או השותף להשתמש בכלים אלו).

יש לשים לב שחשוב שיהיו **מערכים נפרדים של תנאים והגבלות** של חוזה עבור כל אחת מהחלקות בהסכם מסגרת לטכנולוגיית ענן. "גישת מידה אחת מתאימה לכולם" להתקשרות בכל החלקות תוביל לבעיות סביב היתכנות טכנית ותאימות.

כפי שכבר צוין, הצעות מחיר הכוללות מונחים מחייבים שאינם ניתנים למשא ומתן הם בעצם הצעת "לקבל הכל או לדחות הכל" (take it or leave it) לספקים שעלולים לגרום לדחיית הצעה שאחרת הייתה מתקבלת. ארגונים במגזר הציבורי צריכים לשקול היטב את ההשלכות של שימוש במונחים מחייבים **אלא אם כן מדובר בדרישת חוק**. ארגונים צריכים להיות בטוחים לגבי הצורך בדרישה או תנאי מחייבים, כיוון שמשא ומתן עתידי מסוכל מראש על ידי סיווגם כחובה. יש לצמצם את השימוש בדרישות או במונחים מחייבים למינימום מוחלט, כדי לספק לארגון את הגמישות הדרושה לרכישת הטכנולוגיה והפתרון הטובים ביותר.

כדאי לזכור כי טכנולוגיות הענן של CISP הן מתוקננות לחלוטין ומסופקות באופן אוטומטי לחלוטין. לכן, CISP אינו מסוגל לבצע כל סוג של שינוי בתנאים וההגבלות שיצריך כל התאמה אישית של השירות הבסיסי. יתר על כן, המחירים של השירותים הם בדרך כלל ציבוריים ומתוקננים עבור כל המשתמשים, מה שאומר ש-CISP לא יכול להתאים את התמחור על מנת לספוג יותר סיכונים בשם לקוח מסוים.

רכישות עקיפות

אפשרות חלופית לרכישת טכנולוגיות ענן ישירות מ-CISP היא לרכוש אותן ממפיץ CISP במקום זאת. מידע נוסף על מפיצי CISP נמצא בחלק 2.1.3 לעיל.

שפת RFP לדוגמה: תנאים והגבלות

CISPs או ספקים מייצגים חייבים לספק את התנאים וההגבלות הזמינים לציבור ולספק משוב על התנאים וההגבלות העיקריים שסופקו על ידי הארגון.

בכוונת הארגון להתקשר בחוזה בכתב עם המשתתף במכרז הזוכה בהתבסס על המונחים החוזיים של המשתתף במכרז. על המשתתף במכרז לספק מערך של מונחים חוזיים המוצעים לעיון הארגון, ומייצגים את ההצעה המסחרית והמשפטית הטובה ביותר שלו. מציעים והארגון יכולים לדון בשני מערכי התנאים וההגבלות במהלך שלב הדיון/משא ומתן.

מונחי מסגרת מובילים ברמה גבוהה יהיו מורכבים לכל היותר מהרכיבים הבאים:	
○	משך המסגרת
○	ניהול המסגרת
○	ביצועי המסגרת
○	סיום המסגרת
○	היקף המסגרת
○	הליך ההזמנה
○	הוראות הקשורות לחיסיון
○	IP ומידע ספציפיים לקטגוריה
○	דרישות טכניות מינימליות שעל ה-CISPs לעמוד בהן - למשל, תקני איכות, הסמכה, אבטחה והגנה על נתונים
יהיו תנאים שונים עבור כל אחת מחלקות הסכם המסגרת	
ניתן לשקול את הפרטים של שירות CISP והם יטופלו בעת החוזה המרכזי	
יש לאפשר שינויים בחוזה - התנאים אינם אמורים להגביל לקוחות וספקים להסכים לשינויים בחוזה או להוסיף שירותים או שיפורים חדשים. האופי המתפתח של שירותי הענן הוא כזה ששיפורי השירות יהיו זמינים על בסיס מתמשך ובכך כל אלה יכולים לעזור לספק יעילות ללקוחות	
אין צורך שהלקוח יציין הסכמי רמת שירות (SLA). מונחי הלקוח אינם אמורים להגדיר SLA מותאמים אישית עם עמלה ספציפית, השונים ממודלים סטנדרטיים של אספקת שירותים של CISPs. כשמאפשרים הסכמי רמת שירות (SLA) סטנדרטיים של CISPs, הם יכולו לשמור על עלויות נמוכות ולהעביר אותן ללקוחות תוך מתן אפשרות ללקוחות להיות בטוחים שה-CISP יכול לעמוד ב-SLA.	
תקורות אחריות צריכות להיות מידתיות. האחריות צריכה להיות פרופורציונלית לשירותים הנרכשים ולא אמורות להיות תקורות אחריות גבוהות באופן לא פרופורציונלי. אם התקורות גבוהות באופן לא פרופורציונלי, זה ירתיע CISPs מלקבל פרויקטים בעלי ערך נמוך. פרויקטים אלה משמשים לעתים קרובות כמבוא שימושי וכמקרה "מבחן" עבור לקוחות כדי לקבוע אם פתרונות ענן מסוימים יעילים עבור הארגון שלהם.	
לקוחות צריכים להיות הבעלים של הנתונים שלהם. לקוחות צריכים לשלוט בנתונים שלהם ולהיות בעלי היכולת לקבוע את המיקום הגאוגרפי שבו הנתונים מוחזקים. דבר זה יאפשר ללקוחות להימנע מגעילת ספקים ולהעביר נתונים לספקים חדשים בחופשיות.	

2.5.2 תנאים והגבלות של תוכנה

למרות שמדריך זה מתמקד ברכישת טכנולוגיות ענן PaaS ו-IaaS כפי שמסופקות על ידי CISP, חשוב להדגיש את התנאים וההגבלות של התוכנה כדי שארגוני המגזר הציבורי יוכלו לשקול אותם בעת רכישת תוכנה מספקים. יש לעיין באיור 1 (עמוד 5) כדי לסקור כיצד תוכנה נרכשת כחלק מ-RFP לרכישת שירותי ענן מובנה היטב.

תוכנה משחקת תפקיד קריטי כמעט בכל עסק, כולל במגזר הציבורי. הכללת התחייבויות כגון תנאים והגבלות של רישוי תוכנה ב-RFP לרכישת שירותי ענן עוזרת להבטיח שגופים במגזר הציבורי יקבלו את התמורה הטובה ביותר ושיש להם חופש לבחור ספקים בעת רכישת תוכנה.

יש לעיין בעשרת העקרונות של רישוי תוכנה הוגן עבור לקוחות ענן⁹ למידע נוסף. העקרונות פותחו על ידי Cigref¹⁰, איגוד של חברות צרפתיות גדולות ומנהלים ציבוריים המייצגים את המשתמשים בטכנולוגיה דיגיטלית, בשיתוף עם CISPE, ובתמיכת איגודי סחר אירופאים אחרים של CIOs וספקים, כדי לטפל בשיטות עבודה ששני האיגודים רואים בהן פגיעה בטרנספורמציה הדיגיטלית של ארגונים מכל הגדלים בעת תהליך המעבר שלהם לענן.

שפת RFP לדוגמה: תוכנה

בכוונת ה<ארגון> להתקשר בחוזה בכתב עם המשתתף במכרז הזוכה בהתבסס על המונחים החוזיים של המשתתף במכרז. על המשתתף במכרז לספק מערך של מונחים חוזיים המוצעים לעיון ה<ארגון>, ומייצגים את ההצעה המסחרית והמשפטית הטובה ביותר שלו. ספקי התוכנה וה<ארגון> יכולים לדון בשני מערכי התנאים וההגבלות במהלך שלב ה<דיון/משא ומתן>.

⁹ <https://www.fairsoftware.cloud/principles/>

¹⁰ <https://www.cigref.fr/>

דרישה 1.0. ספקי תוכנה <u>חייבים</u> לספק תנאי רישוי ברורים, כולל פירוט של עלויות ברמות סיכום ופירוט.
דרישה 1.1. כל החיובים הנוגעים לכל אי עמידה בתנאי הרישיון <u>חייבים</u> להיות מסופקים ברמות סיכום ופירוט.
דרישה 2.0. רישיונות תוכנה <u>חייבים</u> לספק <ארגון> את היכולת להעביר את התוכנה המורשית מהתוכנה בשטח לענן שנבחר על ידם, מבלי לדרוש רכישת רישיונות נפרדים כפולים עבור אותה תוכנה.
דרישה 2.1. רישיונות תוכנה <u>חייבים</u> להיות חופשיים מהגבלות רישוי ומעלויות מוגברות המגבילות את יכולת <הארגון> להפעיל את התוכנה המורשית בענן שנבחר על ידם.
דרישה 3.0. רישיונות תוכנה <u>חייבים</u> לאפשר <ארגון> להפעיל את התוכנה המורשית על החומרה שלהם (המכונה בדרך כלל תוכנה "בשטח") וכן על הענן שנבחר על ידם.
דרישה 4.0. <u>אין אפשרות</u> לכך שרישיונות תוכנה ידרשו שהתוכנה המורשית תפעל באופן בלעדי על חומרה המיועדת אך ורק ל<ארגון>.
דרישה 5.0. <u>אין אפשרות</u> שספקי תוכנה יענישו את <הארגון> אם נעשה שימוש בתוכנה המורשית של הספקים בהצעת ענן של ספק אחר, למשל על ידי הכללת זכויות לביצוע ביקורת תוכנה מוגברת או חודרנית, או הטלת תשלומי רישוי תוכנה גבוהים יותר.
דרישה 6.0. תוכנת ספרייה <u>חייבת</u> לתמוך בסטנדרטים פתוחים לסנכרון ואימות זהויות משתמש בצורה שלא מפלה שירותי זהות אחרים.
דרישה 7.0. <u>אין אפשרות</u> שספקי תוכנה יגבו מחירים שונים עבור אותה תוכנה המבוססים אך ורק על מי שהוא הבעלים של החומרה עליה היא מותקנת.
דרישה 7.1. <u>אין אפשרות</u> לערוך הבחנה במחירי תוכנה בין תוכנות המותקנות במרכז נתונים של <הארגון>, מרכז נתונים המנוהל בידו צד שלישי, על מחשבים המושגרים מצד שלישי, או בספק הענן לפי בחירת <הארגון>.
דרישה 8.0. במהלך תקופת החוזה, <u>אין אפשרות</u> לספקי תוכנה לבצע שינויים מהותיים בתנאי הרישיון המגבילים את <הארגון> משימושים שהותרו בעבר, אלא אם כן נדרש על פי חוק או בשל חששות אבטחה.
דרישה 9.0. <u>אין אפשרות</u> לספקי תוכנה להטעות את <הארגון> בכך שיציגו מצג שרישיונות תוכנה יכסו את השימוש המיועד בתוכנה של <הארגון> כפי שמתואר ב<דרישות הארגון>, כאשר כיסוי שימוש כזה עשוי לדרוש רכישת רישיונות נוספים.
דרישה 10.0. אם <הארגון> תהיה הזכות למכור ולהעביר רישיונות תוכנה, ספקי תוכנה <u>חייבים</u> להמשיך להציע תמיכה ותיקונים בתנאים הוגנים ל<הארגון> שרכש רישיון מכר מחדש כדון.

2.5.3 איך לבחור בין זוכי מענקים לפי פרויקט

גופים במגזר הציבורי השותפים להסכם המסגרת יכולים להזמין או להגיש 'חוזה מרוכז' לשירותים הדרושים להם בעת הצורך. הצבת חוזה מרוכז במסגרת הסכם מסגרת מאפשרת ללקוחות לחדד דרישות עם מפרט פונקציונלי נוסף לחוזים מרוכזים, תוך שמירה על ההטבות המוצעות במסגרת הסכם המסגרת.

במידת הצורך, ניתן לקיים תחרות זעירה לאיתור הספק הטוב ביותר עבור עומס עבודה או פרויקט מסוימים. תחרות זעירה היא המקום שבו לקוח הולך לתחרות נוספת במסגרת הסכם המסגרת, על ידי הזמנת כל הספקים שבתוך חלקה להיענות למערך של דרישות. הלקוח יזמין את כל הספקים המתאימים בתוך החלקה להשתתף במכרז, ומכאן החשיבות של דרישות המינימום למקבלי מענקים על RFP לרכישת שירותי ענן - מכיוון שהן מבטיחות סטנדרט גבוה של אפשרויות בכל חלקה.

שוב יש לשים לב שחשוב שיהיו מערכים נפרדים של תנאים והגבלות חוזיים עבור כל אחת מקטגוריות החלקה של סוג ההצעה (למשל IaaS/PaaS ציבורי, IaaS/PaaS קהילתי, IaaS/PaaS פרטי), כיוון שגישת התקשרות בסגנון "מידה אחת המתאימה לכולם" בכל חלקה תוביל לבעיות הקשורות להיתכנות טכנית והתאמה.

יש לעיין בחלק 2.1.4 לשפת RFP לדוגמה כשזה נוגע לבחירת זוכי המענק.

2.5.4 הצטרפות ועזיבה

שיקול אחד שיש לזכור בעת הגדרת הסכם מסגרת לטכנולוגיית ענן הוא האפשרות של מערכת רכישה דינמית (DPS). עם מודל DPS, כל הספקים שעומדים בדרישות המינימום להסכם המסגרת יתקבלו למסגרת. אין הגבלה קשה על מספר הספקים שעשויים להצטרף למסגרת, ובניגוד למודל המסגרת המסורתי, ספקים יכולים גם להגיש בקשה להצטרף ל"מסגרת DPS" בכל נקודה במהלך חייה.

אנחנו ממליצים בחום לגופים במגזר הציבורי להציב סטנדרטים גבוהים כדי להבטיח איכות והבטחת שירות מספקים מוסמכים, אך לא להיות ספציפיים מדי כדי לפסול CISPs באופן שאינו מבטיח תחרות הוגנת. בסופו של דבר המטרה היא להימנע מרוויה של משתמש הקצה בשל מספר עצום של אפשרויות, תוך שמירה על סטנדרט טכנולוגיות הענן הזמין גבוה.

3.0 שיטות עבודה מומלצות/לקחים שנלמדו

בהמשך הדברים נדגיש כמה לקחים שהופקו בנוגע למימוש מוצלח של הסכם מסגרת לטכנולוגיית ענן בעזרת RFP לרכישת שירותי ענן.

3.1 משילות בענן

משילות בענן הוא באחריות משותפת. CISP מספקים תכונות ושירותים להטמעת משילות בענן בכל היבט בסביבת הענן, בזמן שהלקוחות מביאים איתם את הסטנדרטים שקיימים אצלם למשילות בענן ולומדים כיצד הענן מאפשר משילות בענן.

בענן, ללקוחות ניתנת הזדמנות לבנות את סביבת ה-IT הרצויה, ולא רק לנהל את הסביבה שיש להם. הענן מאפשר ללקוחות: (1) להתחיל עם רשימת מצאי מלאה של כל נכסי ה-IT; (2) לנהל את כל הנכסים הללו ממוקד אחד מרכזי; ו-(3) ליצור התראות בנוגע לשימוש/חייב/אבטחה וכדומה. כל היתרונות החיוניים הללו שיש לענן עוזרים ללקוחות לקבל ארכיטקטורה ממוטבת – ואוטומטית ככל שניתן – ללא צורך ברכישה בלתי פוסקת ובהתקנה של חומרה חדשה. ה-CISP מבצע זאת, דבר שמאפשר ללקוחות להתמקד ברמה התפעולית הקריטית למשימה במקום בניהול בלתי מובחן של התשתית.

דרך שימושית אחת לבחון ענן CISP היא לבחון אותו באופן יעיל כ-API גדול מאוד. בין אם מפעילים שרת חדש או משנים הגדרת אבטחה, למעשה מבצעים התקשרויות API. כל שינוי בסביבה מתועד ונרשם (המי, מה, היכן ומתי של כל שינוי מתועדים). דבר זה מספק משילות, בקרה ונראות בענן שמתאפשרים רק בסביבת ענן. בכך מתאפשר ללקוחות לחשוב מחדש על המודלים הקיימים שלהם למשילות IT, ולקבוע כיצד ניתן ליעל ולשפר אותם בהתחשב ביתרונות שהענן מביא.

המשמעות של משילות בענן יכולה להיות גם העברה ושילוב של השינויים החיוניים בתהליך ושל מערכי מיומנויות חדשים שמגיעים עם הענן. לדוגמה, מנהלי פרויקטים מכירים מהי המתנה שנמשכת חודשים לבניית סביבת IT, ובעקבות כך הם יכולים להעריך יתר על המידה את לוחות הזמנים ליצירת פיתוח או סביבת בדיקה בענן (דבר שעם הענן יכול לקחת דקות ספורות). ההסתגלות לזריזות ולגמישות החדשות האלה תהיה תהליך שיתפתח עם הזמן ותתרחש תוכנית אחר תוכנית. יש לשתף את הלקחים האלה כדי שהסכם מסגרת לטכנולוגיית ענן יוכל להמשיך ולהתפתח בצורה כזו שהדרישות יתאימו לתהליכים החדשים ולזריזות והגמישות.

3.2 תקצוב בענן

בכל הנוגע לאופן הבניית תמחור הענן מסוג תשלום לפי שימוש כך שיתאים לדרישות הרכישה והתקצוב במגזר הציבורי, גילינו שאיגוד שירותי CISP לשורת פריטים אחת (מחשוב, אחסון, עבודה ברשת, מסד נתונים, IoT וכו') יכול לעזור, הכול תחת שורת פריטים אחת שנקראת **טכנולוגיות ענן**. הגמישות בגישה זו מאפשרת להציע למשתמשים את כל טכנולוגיות ה-CISP העדכניות והחדשות בזמן אמת, ומספקת למשתמשים גישה מהירה למשאבים הדרושים להם, בזמן שהם צריכים אותם. גישה זו מתאימה גם לביקוש משתנה, מה שמוביל לניצול מיטבי ולעלויות נמוכות.

ארגונים במגזר הציבורי יכולים להוסיף שורת פריטים נוספת להזמנות מחלקות אחרות במסגרת ענן, במידה שהם זקוקים לשירותי ייעוץ, שירותים מקצועיים או שירותים מנוהלים, תוכנה מ-Marketplace, שירותי תמיכה בענן והדרכה בנושא ההצעות של CISP.

ניתן לספק גמישות נוספת בחוזה על ידי שימוש בשורת פריטי חוזה אופציונלית בתוך קטגוריות משאבים מתאימות כך שיתאימו לצמיחה עתידית. לחלופין, אם ארגון רוצה לאגד טכנולוגיות ענן עם שירותי ייעוץ או שירותים מקצועיים/מנוהלים לשורת פריטים אחת, ניתן לעשות זאת באמצעות שורת פריטים כדוגמת "טכנולוגיות ענן ועבודה נלווית".

להלן דוגמה מייצגת לגישה זו. בדוגמה שלמטה, כל יחידה בשורת הפריטים #1001 - טכנולוגיות ענן, שווה לשימוש בסך €1.00 ב-"טכנולוגיות ענן". בכל חודש, ניתן לממן תוספות להזמנה בהתבסס על תחזיות שימוש נוכחיות וחזויות.

טבלה 3 - דוגמה למבנה תמחור של שורת פריטים אחת.

פריט מס'	מצרכים/שירותים	כמות	יחידה	מחיר ליחידה	סכום
1001	טכנולוגיות ענן	1,000	כל אחת	€1	€1,000
1002	שירותי ייעוץ	1	בשבוע	€3,000	€3,000
1003	תמיכה בענן	1	בחודש	€1,000	€1,000
1004	הדרכת ענן	1	ליום	€3,00	€3,000
1005	Cloud Marketplace	10	כל אחת	€10	€100

כדוגמה לאופן שבו המבנה הזה יכול לעבוד: ארגון במגזר הציבורי יוצר קשר עם CISP כדי להעריך את הכמות של שירותי טכנולוגיית ענן שהארגון צפוי להשתמש בה. הארגון מסכים לתנאים עם הספק, למשל 10 מיליון אירו במשך 5 שנים, שמגיעים ל-2 מיליון אירו בשנה. הארגון מתחייב לסכום השנתי הראשוני בסך 2 מיליון אירו. בכל חודש מגיע חיוב והספק לתשלום נלקח מהקופה. יש משיכה מהחשבון הזה. הכספים הנותרים מנוטרים לצורך מעקב אחר קצב שריפת המזומנים באמצעות כלי ניטור וחיזוי של CISP. אם הקופה עומדת להתרוקן, הארגון מבקש ממנהל הכספים כספים נוספים שניתן להפקיד כדי להמשיך בשירותים כסדרם.

ניסוח RFP לדוגמה: תמחור - התקשרות בחוזה**תנאי תשלום**

יש לבנות את תנאי התשלום כך שיתאימו לתשלום רק עבור המשאבים שבהם נעשה שימוש על ידי **<הארגון>**, כפי שמצוין להלן:

1. התשלום החודשי יתבסס על שימוש/צריכה של שירותים בפועל ובהתאם לתמחור של CIPs שפתוח לציבור.

התחייבות מינימלית והוצאה מקסימלית

מאחר שיהיה זה בלתי אפשרי עבור **<הארגון>** לקבוע במדויק מה יהיה נפח השימוש במשאבים של ספק שירותי ענן. לאורך תקופה מסוימת, ההזמנות יצוינו בכמויות של יחידת מחיר קבועה עבור שורת פריטים יחידה של "טכנולוגיות ענן".

כל יחידה בשורת הפריטים שהוזמנה תהיה שוות ערך לטכנולוגיות ענן שהוזמנו בסך **<€1.00>**. הזמנות מצטברות יבוצעו מעת לעת באמצעות שינוי בהזמנה זו בכמויות שונות כדי לספק ל**<הארגון>** את הגמישות להזמין מראש כמויות שונות של טכנולוגיות ענן של CISP ב"כמות אירו" בהתבסס על השימוש המשוער לצרכים לפי משך זמן משתנה. הכמויות יוזמנו מראש מעת לעת על ידי ה**<הארגון>** בסכומים שמספיקים לכיסוי העלות המשוערת של טכנולוגיות ענן שישמשו כדי לעמוד במגוון דרישות.

פריט מס'	תיאור	כמות	יחידה	מחיר
01	טכנולוגיות ענן של CISP	1,000	כל יחידה	€1,000.00

מינימום הזמנה/הזמנה מצטברת

הזמנות יבוצעו מעת לעת עבור כמויות משתנות של יחידות שורת פריטים בסך **<10.000>** בהתבסס על השימוש המשוער של ה**<הארגון>** בטכנולוגיות הענן. הסדר זה יספק ל**<הארגון>** את הגמישות להזמין מראש יחידות של "טכנולוגיות ענן" בסך **<10,000>** שאותן צריך כדי לתמוך בתפעול וכדי להישאר עקביים עם השיטה המסחרית של מחשוב הענן, "תשלום לפי שימוש".

תוספת ראשונית בסך **<100,000>** יחידות בעלות **<€100.000>** תוזמן עם הזמנת החוזה המרוכז. המספר המינימלי של סך יחידות שורת הפריטים שניתן להוסיף להזמנה מצטברת אחת באמצעות שורת פריטים אחת או יותר הוא **<x>**. המספר המרבי של יחידות שניתן להזמין במסגרת הזמנת המשלוח לא יכול לעלות על **<x>**, אך אינו יכול לעולם לחרוג מערך החוזה המרוכז בשילוב עם כל היחידות הקודמות שהוזמנו. באחריות ה**<הארגון>** להבטיח שכל ההזמנות יהיו בגבולות המפורטים בסעיף זה.

הזמנה מרבית

ערך ההזמנה המרבי הכולל הוא עד **<x>** ומורכב מעד **<x>** יחידות של שורת פריטים יחידה במחיר של **<x>** ליחידה. הערך מבוסס על אומדן הדרישות של ה**<הארגון>** לאורך תקופת הביצועים, אך אינו מובטח.

3.3 הבנת המודל העסקי של שותפים

על גופים במגזר הציבורי לשאוף להבין את המודלים שלפיהם CISPs מספקים את ההצעות שלהם ולהכיר בכך ששותפים שמספקים ייעוץ, שירותים מנוהלים, הפצה ועוד הרבה מעבר הם חיוניים לתהליך. לקוחות רבים צריכים ספק ענן עבור התשתית שלהם, ומבצעים מיקור חוץ של "עבודות מקלדת" הקשורות לתכנון, העברה וניהול אל משלב מערכות (SI) או לספק שירותים מנוהלים. בהתחשב בתמהיל ה'שירותים' הזה, עשויות להיות דרישות שאינן חלות על ספקי ענן, כגון סעיפים במודל הזרם המחייבים קבלני משנה.

אם לוקחים סעיפי חיוב כאלה כדי להמחיש מדוע חשוב להבין כיצד פועלים שותפים ומפצים ביחס ל-CISPs, בחלק מסוגי הרכש יש סעיפים שמחייבים את הקבלן הראשי לגלגל הלאה סעיפים מחייבים מסוימים לכל השותפים/קבלני המשנה שלו. בדרך כלל, CISPs לא יספקו או יציעו עצמם כשותפים רשמיים בקבלנות משנה, שכן הם מציעים שירות מתוקנן בסקייל מסיבי שאינו מעוצב להתאים לדרישות הייחודיות של לקוח קצה מסוים (כולל הצרכים של לקוח במגזר הציבורי במסגרת חוזה במגזר הציבורי). במודל רכש עקיף (רכישת שירותי ענן באמצעות מפץ CISP), CISP רשאי לדחות סעיפים אלה מהמפץ שלו, כיוון שאינם חלים על ספק שירותים מסחריים "משבבה שנייה". במקרה כזה, ה-CISP אינו מבצע בעצמו את היקף העבודה שבמסגרת החוזה, אלא שותף CISP משתמש בתשתית של CISP לשם כך. לפיכך, ה-CISP הוא ספק מסחרי (לא קבלן משנה) לפעילות של שותף. במודל רכש ישיר (קניית שירותי ענן ישירות מ-CISP), CISP בדרך כלל ידחה את סעיפי ה"חובה" הללו שמתאימים לקבלן משנה טיפוסי של סחורות, בשל האופי המסחרי של השירותים במסגרת החוזה והעובדה שרוב ה-CISPs אינם מצריכים קבלני משנה שיספקו את השירותים המסחריים שלהם.

3.4 מתווכי ענן

הרעיון של מתווך ענן כאמצעי לצמצום האפשרות לנעילת ספק יכול להיות בעייתי. על אף שרעיון מתווך הענן יכול להיות טוב בתיאוריה, בפועל סביר להניח שהוא יציג יותר מורכבות ובלבול מאשר ערך ממשי.

הניסיון לעצב יישומים לעבודה על פני מספר עננים בזמנית או בצורה חליפית מוביל בהכרח להתפשרות על היכולות (אין אבן רוזטה לענן). גישה זו יכולה בסופו של דבר להוסיף שכבת מורכבות מיותרת בין לקוחות המגזר הציבורי ושירותי הענן שלהם, שעלולה לפגוע ביעילות וביתרונות האבטחה שמבקשים להשיג—מה שמוביל להפחתה במדרגיות, בזריזות ובגמישות, להגדלת עלויות ולהאטת החדשנות.

3.5 איסוף מידע טרום-RFP/תחקיר שוק

כאשר ישות במגזר הציבורי מתכננת RFP לרכישת שירותי ענן, עליה לכלול בעלי עניין מכל היבטיו של הארגון - הנהלה בכירה, בעלי העניין העסקיים, טכנולוגיה, פיננסים, רכש, משפטים וחוזים - כבר מתחילת התהליך. גישה זו מבטיחה שכל בעלי העניין יבינו את מודל הענן, וכתוצאה מכך גישה מושכלת להערכה מחדש של שיטות רכש IT מסורתיות.

יחד עם זה מגיע דו-שיח עם התעשייה, אנחנו ממליצים בחום לגופים במגזר הציבורי להקדיש זמן לשיחות מעמיקות כדי לקבל משוב מהתעשייה - CISPs, שותפי CISP, ספקי PaaS/SaaS Marketplace ומומחים בתעשייה. לדוגמה, דו-שיח כזה יכול להתבצע בצורה של ימי תעשייה או סדנאות אבטחה ורכש. דרך יעילה נוספת להגיע להבנה מעמיקה בנושא רכישת ענן היא לשחרר RFI, או באופן אידיאלי, טיוטה של מסמך RFP. לעתים קרובות הם כוללים בעיות פוטנציאליות שניתן לזהות, לדון בהן ולשנות בהתאם לפני פרסום ה-RFP הסופי לרכישת שירותי הענן.

3.6 קיימות

קיימות טבועה במחשוב ענן והמעבר לענן מספק יתרון ביעילות אנרגטית, בהשוואה לשרתים בשטח או למרכזי נתונים ארגוניים. זיהוי CISP שנותן עדיפות לקיימות ושלקח על עצמו התחייבויות ציבוריות להשגת יעדי קיימות מספק ביטחון נוסף לכך שהענן בר קיימה. CISPs ומפעילי מרכזי נתונים אירופאים (בתמיכת הנציבות האירופית) יצרו את ה"הסכם לניטרליות אקלימית למרכזי נתונים"¹¹, יוזמה רגולטורית עצמית שמטרתה לקבוע קריטריוני קיימות ברורים, פשוטים ומרחיקי לכת עבור תעשיית מרכזי הנתונים ולהבטיח שמפעילי מרכזי הנתונים וספקי שירותי הענן הם בעלי ניטרליות אקלימית עד שנת 2030.

¹¹ <https://www.climate-neutral-data-centre.net/self-regulatory-initiative/>

יוזמת הרגולציה העצמית כוללת יעדים ברורים ליעילות אנרגטית במרכזי נתונים, חיסכון במים, שימוש חוזר ותיקון שרתים, ושימוש באנרגיה נטולת פחמן להפעלת מרכזי נתונים. CISOs שנרשמים ליוזמת הרגולציה העצמית מסכימים לעמוד ביעדים אלו ומאשרים לפי הקריטריונים הללו להיחשב כמפעיל בעל ניטרליות אקלימית.

על RFP לרכישת שירותי ענן לשאול את ה-CISOs אם הם התחייבו לקריטריונים כאלה, ולשאול באופן ספציפי אם הם התחייבו לרגולציה עצמית ומתי קיבלו על עצמם התחייבות זו.

ניסוח RFP לדוגמה: קיימות

האם התחייבת להפעיל מרכזי נתונים בעלי ניטרליות אקלימית בכך שחתמת על יוזמת הרגולציה העצמית למרכזי נתונים בעלי ניטרליות אקלימית? אם כן, מתי חתמת על היוזמה?

האם יש באפשרותך לספק הוכחה לכך שהוענק לך החותם לשימוש של הסכם הניטרליות האקלימית למרכזי נתונים?

נספח א' - דרישות טכניות להשוואה בין משתתפים במכרז

להלן פירוט שלנו לגבי כמה מהדרישות הגנריות של טכנולוגיית ענן שניתן להשתמש בהן כדי להשוות בין CISOs שונים במהלך חוזים מרוכזים או תחרויות זעירות על הסכם מסגרת טכנולוגיית ענן.

1. פרופיל ספק הענן

דרישה	
1. ניסיון בשוק: כמה שנים פועל ספק הענן בפלח שוק הענן?	
2. פתיחות והגנה על נתונים: האם ספק הענן נצמד לכללי ההתנהלות הראויה בתעשייה בנושא הגנת נתונים והפיקוח? האם ספק הענן נצמד לעקרונות פיתוח קוד פתוח API-י פתוח?	

2. תשתית גלובלית

דרישה	
1. טווח גלובלי: האם ספק הענן מציע תשתית גלובלית כדי לעזור למשתמשים להשיג זמן השהיה נמוך ותפוקה גבוהה?	
2. אזורים: האם לספק הענן יש נוכחות אזרית בתחומים הגאוגרפיים הדרושים?	
3. דומיינים/אזורים: האם ספק הענן מיישם את רעיון הדומיינים או האזורים שבהם מקובצים מרכזי נתונים מרובים דרך רשת בעלת זמן השהיה נמוך כדי לספק רמה גבוהה יותר של זמינות גבוהה ועמידות בפני תקלות? • אם כן, יש לרשום את מספר הדומיינים או האזורים ואת מספר מרכזי הנתונים באזור הגאוגרפי הדרוש	
4. מרחק בין דומיינים/אזורים: האם הדומיינים או האזורים של ספק הענן בנויים ממרכזי נתונים שממוקמים פיזית בנפרד כדי לתמוך ביתירות, בזמינות גבוהה ובזמן השהיה נמוך?	
5. מרכזי נתונים שנבנו: האם ספק הענן מציע מרכזי נתונים שתוכננו להיות מבודדים מתקלות במרכזי נתונים אחרים, עם כוח עודף, קירור ועבודה ברשת?	
6. שכפול מרכז הנתונים: האם ספק הענן מציע שכפול נתונים בין מרכזי נתונים בתוך דומיין או אזור בעל מעבר אוטומטי לגיבוי בעת כשל?	
7. שכפול דומיין/אזור: האם ספק הענן מציע שכפול נתונים בין דומיינים או אזורים ששייכים לאזור מסוים?	

3. תשתית

3.1 מחשוב

דרישה	
1.	מחשוב – מופע שרת רגיל – מטרה כללית: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • מטרה כללית – מותאם ליישומים גנריים ומספק איזון בין משאבי מחשוב, זיכרון ורשת. ○ אם כן, מהו מופע השרת הגדול ביותר?
2.	מחשוב – מופע שרת רגיל – מותאם לניצול זיכרון מרבי: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • ניצול זיכרון מרבי – מותאם ליישומים עתירי זיכרון ○ אם כן, מהו מופע השרת הגדול ביותר?
3.	מחשוב – מופע שרת רגיל – מותאם לחישוב אופטימלי: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • חישוב אופטימלי – מותאם ליישומים עתירי זיכרון ○ אם כן, מהו מופע השרת הגדול ביותר?
4.	מחשוב – מופע שרת רגיל – מותאם לניצול אחסון מרבי: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • ניצול אחסון מרבי – מציע כמות גדולה של קיבולת אחסון מקומית ○ אם כן, מהי קיבולת האחסון המרבית (כלומר 5, 10, 20, 50 TB) ומספר הדיסקים המרבי (כונני HDD/SSD) שניתן לספק ולצרף למופע השרת?
5.	מחשוב – מופע שרת רגיל – מותאם לגרפיקה אופטימלית: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • גרפיקה בעלות נמוכה – מציע האצת גרפיקה בעלות נמוכה למופעים של שרתי מחשוב ○ אם כן, מהו מופע השרת הגדול ביותר?
6.	מחשוב – מופע שרת רגיל – מעבד גרפי אופטימלי: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • מעבד גרפי – מציע חומרת מעבד גרפי (GPU) עבור יישומים עתירי גרפיקה ○ אם כן, כמה מעבדים גרפיים ואילו דגמים של מעבדים גרפיים ספק הענן יכול להציע לכל מופע שרת?
7.	מחשוב – מופע שרת רגיל – FPGA אופטימלי: האם ספק הענן מציע את סוגי מופעי השרתים הבאים? • FPGA – מציע מעגלים משולבים שניתנים לתכנות בשטח (FPGA) לפיתוח ופריסה של האצת חומרה מותאמת ליישומים. ○ אם כן, כמה FPGA יכול ספק הענן להציע לכל שרת?
8.	מחשוב – שרת מתפרץ: האם ספק הענן מציע מופעי שרתים בעלי יכולת התפרצות שמספקים רמה בסיסית של ביצועי יחידת עיבוד מרכזית (CPU) עם יכולת לפרוץ מעל לקו הבסיס? • אם כן, מהו מופע השרת המתפרץ הגדול ביותר?

9.	מחשוב – מופעי שרתים עתירי קלט-פלט: האם ספק הענן מציע שרתים שמשתמשים בכוננים שבביים (SSD) עם זיכרון לא נדיף מהיר (NVMe) שמותאמים לזמן השהיה נמוך, ביצועי קלט/פלט אקראיים גבוהים מאוד ותפוקת קריאה רציפה גבוהה? אם כן, מהי קיבולת הקלט/פלט המרבית לשנייה (IOPS) של מופע השרת הגדול ביותר?
10.	מחשוב – אחסון מקומי זמני: האם ספק הענן תומך באחסון מקומי למופעים של שרתי מחשוב שימשו לאחסון זמני של מידע שמשתנה לעתים קרובות?
11.	מחשוב – תמיכה במספר כרטיסי רשת: האם ספק הענן תומך בכרטיסי רשת (NIC) מרובים (ראשוניים ונוספים) שיוקצו עבור מופע שרת נתון? אם כן, מהו המספר המרבי של כרטיסי רשת לכל מופע שרת?
12.	מחשוב – קרבה בין מופעי שרתים: האם ספק הענן מציע למשתמשים את היכולת לקבץ באופן הגיוני מופעי שרתים שנמצאים בתוך אותו מרכז נתונים?
13.	מחשוב – נוגד-זיקה בין מופעי שרתים: האם ספק הענן מציע למשתמשים את היכולת לקבץ באופן הגיוני מופעי שרתים ולמקם אותם במרכזי נתונים שונים בתוך אזור?
14.	מחשוב – אספקת שירות עצמי: האם ספק הענן מציע אספקת שירות עצמי למספר מופעי שרתים במקביל, בין אם דרך ממשק תכנותי, קונסולת ניהול או פורטל אינטרנט?
15.	מחשוב – התאמה אישית: האם ספק הענן מציע מופעי שרתים בהתאמה אישית, כלומר, אפשרות לשנות הגדרות תצורה כמו למשל מעבד וירטואלי (vCPUs) וזיכרון גישה אקראית (RAM)?
16.	מחשוב – דיור בענן: האם ספק הענן מציע שרתי דיור יחיד שפועלים על חומרה ייעודית למשתמש יחיד? אם כן, מהו מופע שרת הדיור היחיד הזמין הגדול ביותר?
17.	מחשוב – זיקה בין מארחים: האם ספק הענן מציע את היכולת להפעיל מופע שרת ולציין שמופע שרת זה יופעל מחדש על אותו מארח פיזי תמיד?
18.	מחשוב – נוגד זיקה בין מארחים: האם ספק הענן מציע את היכולת לפצל ולארח מופעי שרתים ספציפיים על גבי מארחים פיזיים שונים?
19.	מחשוב – AUTOMATIC SCALING: האם ספק הענן מציע את היכולת להגדיל אוטומטית את מספר מופעי השרתים במהלך עליות חדות בביקוש כדי לשמור על רמת הביצועים (כלומר 'התרחבות')?
20.	מחשוב – מנגנון ייבוא תמונות: האם ספק הענן מציע למשתמשים את האפשרות לייבא את התמונות הקיימות שלהם ולשמור אותן כתמונות חדשות וזמינות באופן פרטי, שבעתיד ניתן יהיה להשתמש בהם לצורכי הקצאת מופעי שרתים? אם כן, אילו פורמטים נתמכים?
21.	מחשוב – מנגנון ייצוא תמונות: האם ספק הענן תומך ביכולת לקחת מופע שרת פועל קיים או עותק של מופע שרת ולייצא את מופע השרת לפורמט של מחשב וירטואלי? אם כן, אילו פורמטים נתמכים?
22.	מחשוב – הפרעה בשירות: האם ספק הענן מציע מנגנונים שבעזרתם ניתן להימנע מהפסקות או מהשבתת מופע שרת בזמן שהספק מבצע כל סוג של תחזוקת חומרה או שירות ברמת המארח?

23.	מחשוב – הפעלה מחדש של מופע השרת: האם ספק הענן מציע מנגנונים להפעלת שרתים מחדש באופן אוטומטי במארח תקין במקרים שהמארח הפיזי המקורי נכשל?
24.	מחשוב – הודעות: במקרה של אירוע חסין מחשוב, האם לספק הענן יש את היכולת להודיע למשתמש שאירוע כזה התרחש, והאם המשתמש יכול להצטרף לתקשורת זו או לוותר עליה דרך אמצעי שירות עצמי?
25.	מחשוב – תזמון אירועים: האם ספק הענן מציע את היכולת לתזמן אירועים עבור מופעים של שרתי המשתמש, כגון אתחול מחדש, עצירה, הפעלת מופע השרת או הוצאתו משימוש?
26.	מחשוב – מנגנון גיבוי ושחזור: האם ספק הענן מציע מנגנון גיבוי ושחזור משולב?
27.	מחשוב – מנגנון צילום בזק: האם ספק הענן מציע מנגנון צילום בזק ידני ולפי דרישה?
28.	מחשוב – מטה נתונים: האם ספק הענן מציע שירות מטה נתונים של מופע השרת המאפשר למשתמשים להגדיר זוגות מפתח-ערך שרירותיים עבור מופע השרת?
29.	מחשוב – קריאת מטה נתונים: האם ספק הענן מציע שירות מטה נתונים למופע שרת שמספק ממשק תכנות יישומים (API) שאותו מופע שרת יכול להתקשר אליו כדי לברר מידע על עצמו?
30.	מחשוב – מנגנון הגשת מכרזים: האם ספק הענן מציע מנגנון הגשת מכרזים למכרז עבור מופעי שרתים בעלות נמוכה יותר שניתן ליצור באופן מיידי כדי לארח עומסי עבודה שאינם חיוניים למשימה?
31.	מחשוב – מנגנון תזמון: האם ספק הענן מציע דרך כלשהי לתזמן ולשמור קיבולת מחשוב נוספת על בסיס מחזורי, כלומר לוח זמנים יומי, שבועי, חודשי?
32.	מחשוב – מנגנון הזמנה: האם ספק הענן מציע דרך כלשהי לשמור קיבולת מחשוב נוספת לעתיד (כלומר שנה אחת, שנתיים, 3 שנים וכו')?
33.	מחשוב – מערכת ההפעלה של LINUX: האם ספק הענן תומך בשתי הגרסאות האחרונות הנתמכות לטווח ארוך של לכל הפחות: מהדורת Linux ארגונית אחת (כגון SUSE, Red Hat) ומהדורת Linux חינוכית אחת שנמצאת בשימוש נפוץ (כגון CentOS, Ubuntu, Debian)?
34.	מחשוב – מערכת הפעלה של WINDOWS: האם ספק הענן תומך בשתי הגרסאות העיקריות האחרונות של Windows Server (Windows Server 2017 ו-Windows Server 2016)?
35.	מחשוב – נידודת רישוי: האם ספק הענן מציע נידודת רישוי ותמיכה בו? • אם כן, יש לציין את ספקי התוכנות, שמות התוכנות, המהדורות והגרסאות שלה.
36.	מחשוב – הגבלות שירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף המחשוב שלעיל? דוגמה: מספר מופעי שרתים מרבי לכל חשבון מספר מרבי של מארחים ייעודיים לכל חשבון מספר מרבי של כתובות פרוטוקול אינטרנט (IP) שמורות

3.2 עבודה ברשת

דרישה	
1. עבודה ברשת – רשתות וירטואליות: האם ספק הענן תומך ביכולת ליצור רשת וירטואלית לוגית ומבודדת שמייצגת את הרשת של החברה עצמה בענן?	
2. עבודה ברשת – קישוריות בתוך אותו אזור: האם ספק הענן תומך בחיבור שתי רשתות וירטואליות בתוך אותו אזור כדי לנתב תעבורה ביניהן באמצעות כתובות IP פרטיות?	
3. עבודה ברשת – קישוריות בין אזורים שונים: האם ספק הענן תומך בחיבור שתי רשתות וירטואליות באזורים שונים כדי לנתב תעבורה ביניהן באמצעות כתובות IP פרטיות?	
4. עבודה ברשת – רשת משנה פרטית: האם ספק הענן מציע את היכולת ליצור רשתות וירטואליות מבודדות לחלוטין (פרטיות) ורשתות משנה שבהן ניתן להקצות שרתים ללא כל כתובת IP ציבורית או ניתוב אינטרנט?	
5. עבודה ברשת – טווח כתובות של רשת וירטואלית: האם ספק הענן תומך בטווחי כתובות IP שצוינו בבקשה להערוך 1918 (RFC), כמו גם ב-Classless Inter-Domain Routing (CIDR)?	
6. עבודה ברשת – פרוטוקולים מרובים: האם ספק הענן תומך בפרוטוקולים מרובים כולל פרוטוקול בקרת שידור (TCP), פרוטוקול מנת מידע של משתמש (UDP) ופרוטוקול הודעות בקרת אינטרנט (ICMP)?	
7. עבודה ברשת – הקצאה אוטומטית עבור כתובות IP: האם ספק הענן תומך ביכולת הקצאה אוטומטית של כתובות IP ציבוריות למופעי שרתים?	
8. עבודה ברשת – כתובות IP סטטיות שמורות: האם ספק הענן תומך בכתובות פרוטוקול אינטרנט (IP) שמשויכות לחשבון משתמש ולא לשרת מסוים? כתובת ה-IP צריכה להישאר משויכת לחשבון עד שהיא משוחררת באופן מפורש.	
9. עבודה ברשת – תמיכה ב-IPv6: האם ספק הענן תומך בפרוטוקול אינטרנט בגרסה 6 (IPv6) ברמת השער או מופע השרת וחושף פונקציונליות זו למשתמשים?	
10. עבודה ברשת – כתובות IP מרובות לכל כרטיס רשת: האם ספק הענן תומך ביכולת להקצות כתובת IP ראשית ומשנית לכרטיס ממשק רשת (NIC) שמחובר למופע שרת נתון?	
11. עבודה ברשת – כרטיסי ממשק רשת (NIC) מרובים: האם ספק הענן תומך ביכולת להקצות מספר כרטיסי ממשק רשת (NIC) למופע שרת נתון?	
12. עבודה ברשת – נידודת כרטיסי ממשק רשת וכתובות IP: האם ספק הענן תומך ביכולת להעביר כרטיסי ממשק רשת (NIC) וכן כתובות IP בין מופעי שרתים?	
13. עבודה ברשת – תמיכה ב-SR-IOV: האם ספק הענן תומך ביכולות כגון וירטואליזציה של קלט/פלט שורש יחיד (SR-IOV) לביצועים גבוהים יותר (כלומר מנות לשנייה - PPS), זמן השהיה נמוך יותר וריצוד נמוך יותר?	
14. עבודה ברשת – סינון כניסה: האם ספק הענן תומך בהוספה או בהסרה של כללים החלים על תעבורה נכנסת (כניסה) למופעי שרתים?	
15. עבודה ברשת – סינון יציאה: האם ספק הענן תומך בהוספה או בהסרה של כללים החלים על תעבורה יוצאת (יציאה) שמקורה במופעי שרתים?	
16. עבודה ברשת – ACL: האם ספק הענן מציע רשימות בקרת גישה (ACL) לשליטה בתעבורה נכנסת ויוצאת לרשתות משנה?	

17.	עבודה ברשת – תמיכה ביומן זרימה: האם ספק הענן מציע את היכולת ללכוד יומנים של זרימת תעבורת רשת?
18.	עבודה ברשת – NAT: האם ספק הענן מספק Network Address Translation (NAT) כדי לאפשר למופעי שרתים ברשת פרטית להתחבר לאינטרנט או לשירותי ענן אחרים, אך למנוע מהאינטרנט ליזום חיבור לאותם מופעי שרתים?
19.	עבודה ברשת – בדיקת מקור/יעד: האם לספק הענן יש את היכולת להשבית בדיקת מקור/יעד בברטיסי ממשק רשת (NIC)?
20.	עבודה ברשת – תמיכה ב-VPN: האם ספק הענן תומך בקישוריות רשת וירטואלית פרטית (VPN) בין ספק הענן למרכז הנתונים של המשתמש?
21.	עבודה ברשת – מנהרות VPN: האם ספק הענן תומך בחיבורי VPN רבים לכל רשת וירטואלית?
22.	עבודה ברשת – תמיכה ב-IPsec של VPN: האם ספק הענן מאפשר למשתמשים לגשת לשירותי ענן באמצעות מנהרת אבטחת פרוטוקול אינטרנט (IPsec) של רשת וירטואלית פרטית (VPN) או באמצעות מנהרת (SSL) Secure Sockets Layer של רשת וירטואלית פרטית (VPN) דרך האינטרנט הציבורי?
23.	עבודה ברשת – תמיכה ב-BGP: האם ספק הענן משתמש ב-Border Gateway Protocol (BGP) כדי לשפר את המעבר לגיבוי בעת כשל בין מנהרות אבטחת פרוטוקול אינטרנט (IPsec) של רשת וירטואלית פרטית (VPN)?
24.	עבודה ברשת – קישוריות ייעודית פרטית: האם ספק הענן מציע שירותי קישוריות ישיר ופרטי בין מיקומי ספק הענן לבין מרכז הנתונים, המשרד או סביבת המיקום המשותפת של המשתמש, שמאפשר העברות נתונים גדולות ומהירות?
25.	עבודה ברשת – מאזן עומסים בצד הלקוח: האם ספק הענן מציע שירותי איזון עומסים בצד הלקוח (פונה לאינטרנט) שלוקח בקשות מלקוחות דרך האינטרנט ומפיץ בקשות אלו בין שרתים שרשומים במאזן העומסים?
26.	עבודה ברשת – מאזן עומסים עורפי: האם ספק הענן מציע שירותי איזון עומסים עורפי (פרטי) שמנתב תעבורה למופעי שרתים שמתארחים ברשתות משנה פרטיות?
27.	עבודה ברשת – מאזן עומסים שכבה 7: האם ספק הענן מציע שירותי איזון עומסים שכבה 7 (פרוטוקול העברת היפרטקסט - HTTP) שלו יכולת לאזן את תעבורת הרשת במספר מופעי שרתים?
28.	עבודה ברשת – מאזן עומסים שכבה 4: האם ספק הענן מציע שירותי איזון עומסים שכבה 4 (פרוטוקול בקרת שידור - TCP) המסוגל לאזן עומסי תעבורת רשת במספר מופעי שרתים?
29.	עבודה ברשת – זיקה להפעלה עבור מאזני עומסים: האם ספק הענן מציע שירותי איזון עומסים התומך בזיקה להפעלה?
30.	עבודה ברשת – איזון עומסים על בסיס DNS: האם ספק הענן מציע שירותי איזון עומסים בעל יכולת לאזן עומסי תעבורה עבור מופעי שרתים שמתארחים אצל מספר מארחים ששייכים לדומיין יחיד?
31.	עבודה ברשת – יומני מאזן עומסים: האם ספק הענן מספק יומנים שלוכדים מידע מפורט לגבי כל הבקשות שנשלחות למאזן העומסים?
32.	עבודה ברשת – DNS: האם ספק הענן מציע שירותי (DNS) Domain Name System בעל זמינות גבוהה ומדרגיות?

33.	עבודה ברשת – ניתוב DNS מבוסס השהיה: האם ספק הענן מציע שירות DNS שתומך בניתוב מבוסס-השהיה (כלומר שירות DNS שמגיב לשאלות DNS בעזרת משאבים שמספקים את ההשהיה הטובה ביותר)?
34.	עבודה ברשת – ניתוב DNS מבוסס GEO: האם ספק הענן מציע שירות DNS שתומך בניתוב GEO (כלומר שירות DNS שמגיב לשאלות DNS על סמך מיקום גאוגרפי של משתמשים)?
35.	עבודה ברשת – ניתוב DNS על בסיס מעבר לגיבוי בעת כשל: האם ספק הענן מציע שירות DNS שתומך בניתוב על בסיס מעבר לגיבוי בעת כשל (כלומר, שירות DNS מנתב שאלות DNS למשאב שפעיל באותה עת, בעוד משאב שני ממתיך והופך לפעיל רק במקרה של כשל במשאב הראשי)?
36.	עבודה ברשת – שירותי רישום דומיין: האם ספק הענן מציע שירותי רישום שמות דומיין (כלומר, משתמשים יכולים לחפש ולרשום שמות דומיניים זמינים)?
37.	עבודה ברשת – בדיקות תקינות DNS: האם ספק הענן מציע שירות DNS שמשתמש בבדיקות תקינות כדי לפקח על התקינות ועל ביצועי המשאבים?
38.	עבודה ברשת – שילוב DNS ומאזן עומסים: האם ספק הענן מציע שירות DNS שמשתלב עם מאזן העומסים של ספק הענן?
39.	עבודה ברשת – עורך ויזואלי: האם ספק הענן מציע כלי שמאפשר למשתמשים לבנות מדיניות לניהול תעבורה?
40.	רשת אספקת תוכן (CDN): האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) להפצת תוכן שלו זמן השהיה נמוך ומהירויות העברת נתונים גבוהות?
41.	עבודה ברשת – תפוגת מטמון CDN: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שמאפשר להסיר אובייקט ממטמון קצה לפני שפג תוקפו, כולל תכונות כמו ביטול תוקף אובייקטים וניהול גרסאות של אובייקטים?
42.	עבודה ברשת – מקורות חיצוניים ל-CDN: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שתומך במקור מותאם אישית, כלומר שרת פרוטוקול העברת היפרטקסט (HTTP)?
43.	עבודה ברשת – מיטוב CDN: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שבו שליטה פרטנית לקביעת תצורה של שרתי מקור מרובים ומאפייני אחסון במטמון עבור מעני משאבים אחידים (URL) שונים?
44.	עבודה ברשת – CDN מוגבל מיקום גאוגרפי: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שתומך בהגבלת מיקום גאוגרפי, כלומר מונע ממשתמשים בתחומים גאוגרפיים ספציפיים לקבל גישה לתוכן?
45.	עבודה ברשת – אסימוני CDN: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שתומך במעני משאבים אחידים (URL) שבדרך כלל יכללו מידע נוסף כגון תאריך/שעת תפוגה על מנת לתת למשתמשים שליטה רבה יותר על הגישה לתוכן שלהם?
46.	עבודה ברשת – אישורי CDN: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שתומך באישורי (SSL) Secure Sockets Layer מותאמים אישית על מנת לספק תוכן בצורה מאובטחת באמצעות פרוטוקול העברת היפרטקסט מאובטח (HTTPS) מאתרי קצה?
47.	עבודה ברשת – מטמון CDN רב-שכבתי: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שמשתמש בגישת מטמון רב-שכבתי עם שימוש במטמוני קצה אזוריים על מנת להפחית את זמן ההשהיה?
48.	עבודה ברשת – דחיסת CDN: האם ספק הענן מציע שירות רשת אספקת תוכן (CDN) שתומך בדחיסת קבצים?

49.	עבודה ברשת – העלאות CDN מוצפנות: האם ספק הענן מציע רשת אספקת תוכן (CDN) שמאפשרת למשתמשים להעלות נתונים רגישים בצורה מאובטחת כך שרק רכיבים ושירותים מסוימים בתשתית המקור של המשתמש יכולים לצפות בו?
50.	עבודה ברשת – נקודות קצה: האם שירות הרשת של ספק הענן מציע למשתמשים נקודות קצה שמסוגלות לנתב תעבורה דרך קישוריות הרשת הפנימית של הספק (כלומר קישוריות פרטית) על מנת להפחית את עלויות התקשורת ולשפר את אבטחת התעבורה?
51.	עבודה ברשת – הגבלות שירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף העבודה ברשת שלעיל? דוגמה: מספר מרבי של רשתות וירטואליות לכל חשבון גודל מרבי של רשת וירטואלית מספר מרבי של רשתות משנה לכל חשבון מספר מקסימלי של מאזני עומסים לכל חשבון מספר מרבי של ערכי רשימת בקרת גישה (ACL) מספר מרבי של מנהרות רשת וירטואלית פרטית (VPN) מספר מרבי של מקורות לכל התפלגות מספר אישורים מרבי לכל מאזן עומסים

3.3 אחסון

	דרישה
1.	שירות אחסון בלוקים: האם ספק הענן מציע נפחי אחסון ברמת הבלוק לשימוש במופעים של שרתי מחשוב?
2.	אחסון בלוקים – IOPS: האם ספק הענן מציע אפשרות לרכוש יעד ביצועים מפורש או שכבת ביצועים בנפחי אחסון בלוק, כגון מספר מסוים של ביצועי קלט/פלט בשנייה (IOPS) או מגה-בייט לשנייה (MB/S) בתפוקה?
3.	אחסון בלוקים – כונני SOLID STATE: האם ספק הענן תומך באמצעי אחסון שמגובים בכונן Solid State (SSD) שמציע זמני השהיה חד ספרתיים ברמת אלפית השנייה? • אם כן, מהו המספר המרבי של כונני SSD שניתן לחבר לכל מופע שרת?
4.	אחסון בלוקים – סקוילינג: האם ספק הענן מציע למשתמשים את היכולת להגדיל את נפח אחסון הבלוקים הקיים מבלי להקצות אמצעי אחסון חדש ולהעתיק/להעביר את הנתונים?
5.	אחסון בלוקים – צילומי בזק: האם לספק הענן יש יכולת צילום בזק עבור שירות אחסון הבלוקים שלו?
6.	אחסון בלוקים – מחיקת נתונים: האם ספק הענן תומך במחיקת נתונים מלאה כך שהנתונים אינם ניתנים לקריאה או גישים למשתמשים לא מורשים ו/או צדדים שלישיים?
7.	אחסון בלוקים – הצפנה בזמן מנוחה: האם ספק הענן מציע הצפנת נתונים במנוחה בצד השרת עבור נתונים שנשמרים באמצעי אחסון ובצילומי הבזק שלהם? • אם כן, מהו אלגוריתם ההצפנה?

8.	שירותי אחסון אובייקטים: האם ספק הענן מציע אחסון אובייקטים מאובטח, עמיד ובעל מדרגיות גבוהה לאחסון ואחזור כל כמות נתונים שהיא מהאינטרנט?
9.	אחסון אובייקטים – גישה נדירה: האם ספק הענן מציע שכבת שירות אחסון בעלות נמוכה יותר שמטרתו לאחסן אובייקטים וקבצים שניגשים אליהם בתדירות נמוכה יותר?
10.	אחסון אובייקטים – עמידות נמוכה יותר: האם ספק הענן מציע שכבת יתירות מופחתת שבה משתמשים יכולים לאחסן אובייקטים לא חיוניים וניתנים לשחזור במחיר נמוך יותר?
11.	אחסון אובייקטים – גישה לא תכופה: האם ספק הענן מציע שכבה לנתונים שניגשים אליהם בתדירות נמוכה יותר, אך עדיין מצריכים גישה מהירה?
12.	אחסון אובייקטים – ארגון אובייקטים בשכבות: האם ספק הענן מציע יכולת אחסון אובייקטים המאורגן בשכבות, כלומר היכולת להמליץ על העברת אובייקט בין מחלקות או שכבות של אחסון אובייקטים על סמך תדירות הגישה אליו?
13.	אחסון אובייקטים – ניהול מחזור חיים: האם ספק הענן תומך בניהול מחזור החיים של אובייקט באמצעות תצורת מחזור חיים שמגדירה כיצד אובייקטים מנוהלים במהלך חייהם, מהיצירה ועד למחיקה?
14.	אחסון אובייקטים – ניהול מבוסס מדיניות: האם ספק הענן מציע את היכולת ליצור מדיניות נתונים ולהשתמש בה לצורך ניהול של אחסון הנתונים, מחזור החיים שלהם והגדרה של ארגון הנתונים בשכבות?
15.	אחסון אובייקטים – מדיניות מבוססת מיקום וזמן: האם ספק הענן מציע למשתמשים את היכולת ליצור מדיניות שיכולה להגביל את הגישה לנתונים בהתבסס על מיקום המשתמש וזמן הבקשה?
16.	אחסון אובייקטים – אירוח אתרי אינטרנט: האם ספק הענן תומך באירוח אתרי אינטרנט סטטיים מתוך שירות אחסון האובייקטים שלו?
17.	אחסון אובייקטים – הצפנה בזמן מנוחה: האם ספק הענן תומך בהצפנה בצד השרת (SSE) של נתונים במנוחה, כשספק הענן מנהל את מפתחות ההצפנה? • אם כן, מהו אלגוריתם ההצפנה?
18.	אחסון אובייקטים – הצפנה בעזרת מפתחות משתמש: האם ספק הענן מציע יכולת הצפנה בצד השרת (SSE) באמצעות מפתחות מוצפנים שסופקו על ידי הלקוח?
19.	אחסון אובייקטים – שירות מנוהל בעזרת מפתחות: האם ספק הענן תומך בהצפנה בצד השרת (SSE) באמצעות שירות ניהול מפתחות שיוצר מפתחות הצפנה, מגדיר את המדיניות ששולטת באופן השימוש במפתחות ומנהל ביקורת על השימוש במפתחות כדי לוודא שהם בשימוש נכון?
20.	אחסון אובייקטים – מפתח מאסטר בצד הלקוח: האם ספק הענן מציע למשתמשים את האפשרות לשמור על השליטה במפתחות ההצפנה ולהשלים את ההצפנה/פענוח של אובייקטים בצד הלקוח?
21.	אחסון אובייקטים – עקביות חזקה: האם ספק הענן תומך בעקביות קריאה אחרי כתיבה עבור פעולות PUT הקשורות לאובייקטים חדשים?
22.	אחסון אובייקטים – מיקום נתונים: האם ספק הענן מציע בידול אזורי חזק, כך שאובייקטים שמאוחסנים באזור לעולם לא עוזבים את האזור אלא אם המשתמש מעביר אותם במפורש לאזור אחר?
23.	אחסון אובייקטים – שכפול: האם ספק הענן מציע תכונת שכפול המכסה מספר אזורים שתשכפל אובייקטים בצורה אוטומטית באזורים שנבחרו על ידי המשתמש?

24.	אחסון אובייקטים - ניהול גרסאות: האם ספק הענן תומך בניהול גרסאות, כלומר ביכולת לאחסן ולתחזק מספר גרסאות של אובייקט?
25.	אחסון אובייקטים - סמן בלתי מחיק: האם ספק הענן מאפשר למשתמש לסמן פריט כבלתי ניתן למחיקה?
26.	אחסון אובייקטים - מחיקת MFA: האם ספק הענן תומך באימות בשני שלבים (MFA) עבור פעולות מחיקה כאפשרות אבטחה נוספת?
27.	אחסון אובייקטים - העלאה מרובת חלקים: האם ספק הענן מאפשר להעלות אובייקט כקבוצת שמורכבת מחלקים שבה כל חלק הוא חלק רציף מנתוני האובייקט וניתן להעלות את חלקי האובייקטים הללו באופן עצמאי ובכל סדר?
28.	אחסון אובייקטים - תגיות: האם ספק הענן מציע את היכולת ליצור ולשייך תגיות דינמיות וניתנות לשינוי ברמת האובייקט?
29.	אחסון אובייקטים - הודעות: האם ספק הענן מציע את היכולת לשלוח הודעות כאשר מתרחשים אירועים מסוימים ברמת האובייקט (למשל פעולות הוספה/מחיקה)?
30.	אחסון אובייקטים - יומני רישום: האם ספק הענן מציע את היכולת ליצור יומני ביקורת הכוללים פרטים על בקשת גישה בודדת, כמו למשל מי המבקש, זמן הבקשה, פעולת הבקשה, סטטוס התגובה וקוד השגיאה?
31.	אחסון אובייקטים - רשימת מצאי עבור אובייקטים: האם ספק הענן מציע יכולת עריכת רשימת מצאי עבור אובייקטים כדי לתת למשתמשים את היכולת לראות במהירות את האובייקטים ואת מצבם, מה שיאפשר למשתמשים לזהות במהירות אובייקטים בעלי גישה ציבורית?
32.	אחסון אובייקטים - רשימת מצאי עבור מטה נתונים: האם ספק הענן מציע יכולת עריכת רשימת מצאי עבור אובייקטים כדי לתת למשתמשים את היכולת לראות במהירות מטה נתונים של אובייקטים?
33.	אחסון אובייקטים - מיטוב העלאות: האם לספק הענן יש את היכולת לנתב נתונים מאתרי קצה לשירות האחסון באמצעות נתיב רשת ממוטב?
34.	אחסון אובייקטים - יכולת שאילתות: האם ספק הענן מציע למשתמשים את היכולת לבצע שאילתות בשירות אחסון האובייקטים שלו באמצעות ביטויי שפת שאילתות מובנית (SQL)?
35.	אחסון אובייקטים - אחזור מערכי משנה: האם ספק הענן מציע למשתמשים את היכולת לאחזר רק מערכי משנה של נתונים מאובייקט באמצעות ביטויי שפת שאילתות מובנית (SQL) פשוטים?
36.	שירות אחסון קבצים: האם ספק הענן מציע שירות אחסון קבצים פשוט ומדרגי לשימוש במופעים של שרתי מחשוב בענן?
37.	אחסון קבצים - יתירות: האם ספק הענן מאחסן ביתירות אובייקטים של מערכת הקבצים (כלומר ספרייה, קובץ וקישור) במספר מרכזי נתונים או מתקנים כדי להשיג רמות גבוהות יותר של זמינות ועמידות?
38.	אחסון קבצים - מחיקת נתונים: האם ספק הענן תומך במחיקה מוחלטת של נתוני אחסון קבצים כך שהם אינם ניתנים לקריאה או גישים למשתמשים לא מורשים או לצדדים שלישיים?
39.	אחסון קבצים - זמינות גבוהה: האם מערכת הקבצים המנוהלת של ספק הענן מספקת רמה גבוהה של זמינות גבוהה?

40.	אחסון קבצים - NFS: האם ספק הענן תומך בפרוטוקול מערכת קבצים ברשת (NFS)?
41.	אחסון קבצים - SMB: האם ספק הענן תומך בפרוטוקול בלוק הודעת שרת (SMB)?
42.	אחסון קבצים - הצפנה בזמן מנוחה: האם שירות אחסון הקבצים של ספק הענן תומך בהצפנה במצב מנוחה?
43.	אחסון קבצים - הצפנה בזמן תעבורה: האם שירות אחסון הקבצים של ספק הענן תומך בהצפנת נתונים בתעבורה?
44.	אחסון קבצים - כלי העברת נתונים: האם ספק הענן מציע כלי העברת נתונים כלשהו שיאפשר למשתמשים להעביר נתונים ממערכות בשטח למערכת קבצים מבוססת ענן?
45.	שירות אחסון ארכיון: האם ספק הענן מציע שירות אחסון בעלות נמוכה מאוד שמטרתו לאחסן בארכיון אובייקטים וקבצים שניגשים אליהם בתדירות נמוכה ושכמעט בלתי ניתנים לשינוי?
46.	אחסון ארכיון - עמידות בפני תקלות: האם ארכיטקטורת ספק הענן מספקת עמידות בפני תקלות לשירות אחסון הארכיון שלה?
47.	אחסון ארכיון - בלתי ניתן לשינוי: האם ספק הענן תומך בהיעדר היכולת להשתנות של האובייקטים והקבצים המאוחסנים בארכיון?
48.	אחסון בארכיון - WORM: האם ספק הענן מציע יכולת כתיבה בודדת קריאה מרובה (WORM)?
49.	אחסון ארכיב - אחזור מערכי משנה: האם ספק הענן מציע למשתמשים את היכולת לאחזר רק מערכי משנה של נתונים מאובייקט שנשמר בארכיון באמצעות ביטויי שפת שאילתות מובנית (SQL) פשוטים?
50.	אחסון בארכיון - אחזור מהיר: האם ספק הענן מציע למשתמשים אפשרויות אחזור נתונים מרובות בעלויות שונות ובזמני אחזור שונים?
51.	אחסון בארכיון - הצפנה בזמן מנוחה: האם שירות אחסון הארכיון של ספק הענן תומך בהצפנה במצב מנוחה?
52.	אחסון - הגבלות שירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף האחסון שלעיל? דוגמה: נפח אחסון מרבי מספר מרבי של כוננים שמחוברים למופע שרת מספר פעולות קלט/פלט לשנייה (IOPS) מרבי גודל אובייקט מרבי מספר אובייקטים מרבי לחשבון אחסון מספר צילומי בזק מרבי

4. אדמיניסטרציה

דרישה	
1. אדמיניסטרציה - משתמשים וקבוצות: האם ספק הענן מציע שירות ליצירה ולניהול של משתמשים וקבוצות משתמשים בתשתית שלו ובמשאביו?	
2. אדמיניסטרציה - איפוס סיסמה: האם ספק הענן מאפשר למשתמשים לאפס את הסיסמה שלהם בשירות עצמי?	
3. אדמיניסטרציה - הרשאות: האם ספק הענן מציע את היכולת להוסיף הרשאות למשתמשים ולקבוצות ברמת המשאב?	
4. אדמיניסטרציה - הרשאות זמניות: האם ספק הענן מציע את היכולת ליצור הרשאות שתקפות לפרק זמן מסוים?	
5. אדמיניסטרציה - אישורים זמניים: האם ספק הענן מציע למשתמשים את היכולת ליצור ולספק אישורי אבטחה זמניים למשתמשים מהימנים שמוגדרים להימשך בין מספר דקות למספר שעות?	
6. אדמיניסטרציה - בקרת גישה: האם ספק הענן מציע בקרות גישה מדוקדקות למשאבי התשתית שלו? • אם כן, באילו תנאים ניתן להשתמש בבקרות אלה (כלומר שעה ביום, כתובת ה-IP המקורית וכו')?	
7. אדמיניסטרציה - מדיניות מובנית: האם תשתית ספק הענן מכילה מדיניות בקרת גישה מובנית שניתן לצרף למשתמשים ולקבוצות?	
8. אדמיניסטרציה - מדיניות מותאמת אישית: האם תשתית ספק הענן מאפשרת ליצור ולהתאים אישית את מדיניות בקרת הגישה שניתן לצרף למשתמשים ולקבוצות?	
9. אדמיניסטרציה - הדמיית מדיניות: האם ספק הענן מציע מנגנון לבדיקת ההשפעות של מדיניות בקרת הגישה לפני החלת מדיניות זו?	
10. אדמיניסטרציה - הזדהות רב שלבית בענן: האם ספק הענן תומך בשימוש באימות בשני שלבים (MFA) כשכבה נוספת של בקרת גישה ואימות עבור התשתית שלו?	
11. אדמיניסטרציה - הגבלות השירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף האדמיניסטרציה שלעיל? דוגמה: מספר משתמשים מרבי מספר קבוצות מרבי מספר מרבי של סוגי מדיניות מנוהלים	

5. אבטחה

דרישה	
1. אבטחה - בדיקות רקע: האם כל חבר העובדים של ספק הענן שלהם יש גישה לתשתית השירות (בין אם פיזית או לא) כפופים לבדיקות רקע?	
2. אבטחה - גישה פיזית: האם ספק הענן מגביל את הגישה של חבר העובדים לתשתית השירות מלבד במקרים שבהם יש כרטיס תקלה ספציפי, בקשת שינוי או הרשאה רשמית פעילה דומה?	

3.	אבטחה - יומני גישה: האם ספק הענן מנהל יומן לגישת חבר העובדים לתשתית שלו, שבו גישה כזו מתועדת תמיד והיומנים נשמרים למשך 90 יום לפחות?
4.	אבטחה - כניסות מארח: האם ספק הענן מגביל את כניסת חבר העובדים שלו למארחי מחשוב, ובמקום זאת הופך את כל המשימות שמבוצעות במארחי המחשוב לאוטומטיות ומתעד את תוכן המשימות האוטומטיות האלה, ושומר את היומנים למשך 90 יום לפחות?
5.	אבטחה - מפתחות מוצפנים: האם ספק הענן מציע שירות ליצירת מפתחות ההצפנה שמשמשים להצפנת נתוני המשתמש ולשליטה בהם?
6.	אבטחה - ניהול מפתחות גישה: האם ספק הענן מציע את היכולת לזהות מתי נעשה שימוש אחרון במפתח גישה, לסובב מפתחות ישנים ולהסיר משתמשים לא פעילים?
7.	אבטחה - מפתחות שסופקו על ידי הלקוח: האם ספק הענן מאפשר למשתמשים לייבא מפתחות מתשתית ניהול המפתחות שלהם לשירות ניהול המפתחות של ספק שירותי הענן?
8.	אבטחה - שילוב שירות מפתחות מוצפנים: האם שירות ניהול המפתחות של ספק הענן משתלב עם שירותי ענן אחרים כדי לספק יכולת הצפנת נתונים במנוחה?
9.	אבטחה - HSM: האם ספק הענן מציע מודולים ייעודיים של אבטחת חומרה (HSM), כלומר מכשירי חומרה שמספקים אחסון מפתחות מאובטח ופעולות מוצפנות בתוך מודול חומרה עמיד בפני פגיעה?
10.	אבטחה - עמידות מפתחות מוצפנים: האם ספק הענן תומך בעמידות של מפתחות, כולל אחסון עותקים מרובים כך שהמפתחות יהיו זמינים בעת הצורך?
11.	אבטחה - SSO: האם ספק הענן מציע שירות מנוהל לכניסה יחידה (SSO) שמאפשר למשתמשים לנהל בצורה מרוכזת גישה למספר חשבונות ויישומים עסקיים?
12.	אבטחה - אישורים: האם ספק הענן מציע שירות מנוהל להקצאה, ניהול ופריסה של אישורי (SSL) Secure Sockets Layer/אבטחת שכבת תעבורה (TLS)?
13.	אבטחה - חידוש אישורים: האם שירות ניהול האישורים של ספק הענן מקל על חידוש אישורים?
14.	אבטחה - אישורי WILDCARD: האם שירות ניהול האישורים של ספק הענן תומך בשימוש באישורי Wildcard?
15.	אבטחה - רשות אישורים: האם שירות ניהול האישורים של ספק הענן פועל גם כרשות אישורים (CA)?
16.	אבטחה - ACTIVE DIRECTORY: האם ספק הענן מציע שירות (AD) Active Directory של Microsoft שמונהל בענן?
17.	אבטחה - ACTIVE DIRECTORY בשטח: האם שירות ה-(AD) Microsoft Active Directory המנוהל של ספק הענן תומך בשילוב עם (AD) Microsoft Active Directory בשטח?
18.	אבטחה - LDAP: האם שירות ה-(AD) Microsoft Active Directory המנוהל של ספק הענן תומך ב-(LDAP) Lightweight Directory Access Protocol?
19.	אבטחה - ACTIVE DIRECTORY: האם שירות ה-(AD) Microsoft Active Directory המנוהל של ספק הענן תומך בפרוטוקול (SAML) Security Assertion Markup Language?

20.	אבטחה – ניהול אישורים: האם ספק הענן מציע שירות מנוהל שמסייע למשתמשים לסובב, לנהל ולאחזר בקלות אישורים כגון מפתחות ממשק תכנות יישומים (API), אישורי מסד נתונים וסודות אחרים?
21.	אבטחה – WAF: האם ספק הענן מציע חומת אש של יישומי אינטרנט (WAF) שמסייעת להגן על יישומי אינטרנט מפני תקיפות נפוצות שעשויות להשפיע על זמינות היישום, לפגוע באבטחה או לגרום לצריכת משאבים מופרזת?
22.	אבטחה – DDOS: האם ספק הענן מציע שירות להגנה מפני התקפות מניעת שירות (DDoS) הנפוצות והשכיחות ביותר שמופצות בשכבות הרשת והתעבורה, יחד עם היכולת לכתוב כללים מותאמים אישית כדי להפחית התקפות מתוחכמות בשכבת היישום?
23.	אבטחה – המלצות אבטחה: האם ספק הענן מציע שירות להערכה אוטומטית של נקודות תורפה פוטנציאליות ביישומים ובמשאבים?
24.	אבטחה – איתור איומים: האם ספק הענן מציע שירות מנוהל לזיהוי איומים?
25.	אבטחה – הגבלות השירות: האם לספק הענן יש מגבלות כלשהן (למשל הגבלות שירות) ביחס לסעיף האבטחה שלעיל? דוגמה: מספר מרבי של מפתחות מאסטר של לקוחות מספר מרבי של מודולי אבטחת חומרה (HSM)

6. תאימות

הרשימה שלהלן סופקה למטרות המחשה בלבד ואין לראות בה כממצא את האישורים והתקנים שיכולים לחול על שירותי ענן.

יש לציין באיזה מערך של תקני תאימות בינלאומיים וספציפיים לתעשייה עמד ספק הענן:

אישורים \ הסמכות	חוקים, תקנות ופרטיות	התאמות \ מסגרות
☐ C5 [גרמניה] ☐ קוד התנהלות ראווה להגנת מידע של CISPE ☐ CNDP (הסכם ניטרליות אקלימית של מרכזי נתונים)	☐ צו הגנת מידע של האיחוד האירופי ☐ סעיפים במודל האיחוד האירופי	☐ CDSA
☐ DIACAP ☐ DoD SRG רמות 2 ו-4 ☐ FedRAMP ☐ FIPS 140-2 ☐ HDS (צרפת, שירותי בריאות) ☐ ISO 9001	☐ FERPA ☐ GDPR ☐ GLBA ☐ HIPAA ☐ HITECH ☐ IRS 1075	☐ CIS ☐ מידע על משפט פלילי שירות (CJIS) ☐ CSA ☐ מגן הפרטיות של האיחוד האירופי-ארה"ב ☐ נמל מבטחים של האיחוד האירופי ☐ FISC

FISMA ☐	ITAR ☐	ISO 27001 ☐
G-Cloud [בריטניה] ☐	PDPA – 2010 [מלזיה] ☐	ISO 27017 ☐
GxP (21 FDA CFR חלק 11) ☐	PDPA – 2012 [סינגפור] ☐	ISO 27018 ☐
ICREA ☐	PIPEDA [קנדה] ☐	IRAP [אוסטרליה] ☐
IT Grundschatz [גרמניה] ☐	חוק הפרטיות [אוסטרליה] ☐	MTCS שכבה 3 [סינגפור] ☐
MARS – E ☐	חוק הפרטיות [ניו זילנד] ☐	PCI DSS רמה 1 ☐
MITA 3.0 ☐	הרשות הספרדית DPA ☐	SEC כלל (f) 17-a-4 ☐
MCAA ☐	בריטניה 1988 DPA ☐	SOC1 / ISAE 3402 ☐
NIST ☐	508 חלק/VPAT ☐	SOC2 / SOC3 ☐
		SWIPO IaaS קוד ☐
Uptime Institute Tiers ☐		
עקרונות אבטחת ענן בבריטניה ☐		

שימוש בדוחות התאימות שלעיל מאפשר לארגונים במגזר הציבורי להעריך הצעות ייחודיות מול תקנים מקובלים בתחום האבטחה, התאימות והתפעול. דוחות כאלה יכולים להראות שה-CISP, בכך שהם מציינים להם, עומדים בבקורות תפעול מרכז הנתונים שלהם, שנדרשות מספקי שירותי הענן הציבוריים. דרישת תאימות לדוחות כאלה עוזרת לגופים במגזר הציבורי להיות בטוחים שהבקורות שלהם מבוצעות.

- **מתן גישה לאחר בדיקה:** על CISP להגביל את הגישה הפיזית לאנשים שצריכים להיות במקום מסיבה עסקית מוצדקת. אם מוענקת גישה, יש לבטל אותה מיד עם השלמת העבודה הדרושה.
- **כניסה מבוקרת ומפוקחת:** הכניסה למתחם מרכז הנתונים צריכה להיות תהליך מבוקר. על CISP לאייש שערי כניסה בקציני אבטחה ולהעסיק בקרים שיפקחו על בעלי תפקידים ועל מבקרים דרך מצלמות אבטחה. כאשר אנשים בעלי אישור נמצאים באתר, יש לתת להם תג שדורש אימות בשני שלבים ומגביל את הגישה לאזורים שאושרו מראש.
- **עובדי מרכז הנתונים של ה-CISP:** לעובדי CISP שזקוקים לגישה למרכז נתונים באופן שוטף יש לתת הרשאות לאזורים הרלוונטיים במתקן בהתבסס על אופי התפקיד, ובכפוף לבחינת הגישה בקביעות. רשימות צוות צריכות להיבדק באופן שגרתי על ידי מנהל גישה לאזור כדי להבטיח שההרשאה של כל עובד עדיין נחוצה. אם לעובד אין צורך עסקי מתמשך להיות במרכז הנתונים, יש לדרוש ממנו לעבור את תהליך המבקרים.
- **ניטור כניסה לא מורשית:** CIPSP צריכים לפקח באופן רציף אחר כניסה לא מורשית למתחם מרכז הנתונים, באמצעות מעקב וידאו, זיהוי פריצות ומערכות ניטור יומני גישה. הכניסות צריכה להיות מאובטחות במכשירים שמשמיעים אזעקה אם דלת נדחפת בכוח או מוחזקת פתוחה.
- **מרכזי תפעול האבטחה של CISP דואגים לאבטחה גלובלית:** מרכזי תפעול האבטחה של CISP צריכים להיות ממוקמים ברחבי העולם ולהיות אחראים לניטור, למיון ולביצוע תוכניות אבטחה עבור מרכזי נתונים של CISP. עליהם לפקח על ניהול הגישה הפיזית ועל התגובה לזיהוי פריצה תוך מתן תמיכה גלובלית 24/7 לצוותי האבטחה של מרכז הנתונים שבשטח; ולספק פעילויות ניטור מתמשכות כגון מעקב אחר כניסות, ביטול הרשאות גישה, ולהיות זמינים להגיב לאירוע אבטחה פוטנציאלי ולנתח אותו.
- **סקירת גישה שכבה אחר שכבה:** יש להגביל את הגישה לשכבת התשתית בהתבסס על הצורך העסקי. על ידי יישום סקירת גישה שכבה אחר שכבה, הזכות להיכנס לכל שכבה אינה ניתנת כברירת מחדל. יש להעניק גישה לשכבה מסוימת רק אם יש צורך ספציפי לגשת בדיוק לשכבה הזו.
- **תחזוקת הציוד היא חלק מהפעילות השוטפת:** צוותי CISP צריכים להריץ בדיקות על מכונות, רשתות וציוד גיבוי כדי להבטיח שהם תקינים באותו זמן, ובמקרה חירום. בדיקות תחזוקה שגרטיות של הציוד וכלי העזר במרכזי נתונים צריכות להיות חלק מהפעילות הרגילה במרכז נתונים של CISP.

- **ציוד גיבוי מוכן לשעת חירום:** מים, חשמל, מכשירי תקשורת וקישוריות לאינטרנט צריכים להיות מתוכננים עם יתירות, כך שה-CISP יוכלו לשמור על פעילות רציפה במצב חירום. מערכות חשמל צריכות להיות מתוכננות כבעלות יתירות מלאה, כך שבמקרה של הפרעה, ניתן להפעיל יחידות אל-פסק לפונקציות מסוימות, וגנרטורים יכולים לספק כוח גיבוי לכל המתקן. אנשים ומערכות צריכים לפקח ולשלוט על הטמפרטורה והלחות כדי למנוע התחממות יתר, ובכך להפחית עוד יותר הפסקות שירות אפשריות.
- **טכנולוגיה ואנשים עובדים יחד למען אבטחה נוספת:** צריכים להיות נהלים מחייבים לקבלת הרשאה לכניסה לשכבת הנתונים. כולל סקירה ואישור של בקשת הגישה של אדם על ידי מורשים. בינתיים, מערכות זיהוי של איומים ופריצות אלקטרוניות צריכות לנטר ולהפעיל אוטומטית התראות על איומים שזוהו או על פעילות חשודה. לדוגמה, אם דלת מוחזקת פתוחה או נפתחת בבוח, מופעלת התראה. על CISP לפרוס מצלמות אבטחה ולשמור צילומים בהתאם לדרישות החוק והתאימות.
- **מניעת פריצה פיזית וטכנולוגית:** יש לחזק את נקודות הגישה לחדרי שרתים במכשירי בקרה אלקטרוניים שדורשים אימות בשני שלבים. CISP גם צריכים להיות מוכנים למנוע פריצה טכנולוגית. שרתי CISP צריכים להיות מסוגלים להזהיר עובדים מכל ניסיון להסיר נתונים. במקרה הבלתי סביר של פריצה, על השרת להיות מושבת באופן אוטומטי.
- **שרתים ומדיה זוכים לתשומת לב קפדנית:** התקני אחסון מדיה שמשמשים לאחסון נתוני לקוחות צריכים להיות מסווגים על ידי ה-CISP כקריטיים ובשל כך יש להתייחס אליהם בהתאם, כבעלי השפעה גבוהה, לאורך כל מחזור החיים שלהם. ל-CISP צריכים להיות סטנדרטים מדויקים בנוגע לאופן ההתקנה והטיפול במכשירים, ובסופו של דבר הריסתם כאשר הם אינם שימושיים יותר. כאשר התקן אחסון הגיע לסוף חייו השימושיים, ה-CISP ישביתו את המדיה באמצעות טכניקות שמפורטות ב-NIST 800-88. מדיה שאחסנה נתוני לקוחות אינה מוסרת משליטת CISP עד שהיא הושבתה באופן מאובטח.
- **מבקרים מצד שלישי מאמתים את הנהלים והמערכות של CISP:** הביקורות שמתבצעות על ה-CISP צריכות להיעשות על ידי מבקרים חיצוניים שיבדקו את מרכזי הנתונים, יבצעו מחקר מעמיק כדי לאשר שה-CISP פועלים לפי הכללים שדרושים להשגת אישורי האבטחה שלהם. בהתאם לתוכנית התאימות ולדרישותיה, מבקרים חיצוניים עשויים לראיין עובדי CISP לגבי האופן שבו הם מטפלים במדיה ונפטרים ממנה. מבקרים יכולים גם לצפות בעדכונים (feeds) של מצלמות אבטחה ולצפות בכניסות ובמסדורנות שברחבי מרכז נתונים. והם יכולים לבחון ציוד כגון התקני בקרת גישה אלקטרוניים של CISP ומצלמות אבטחה.
- **מוכנים לבלתי צפוי:** CISP צריכים להתכונן באופן יזום לאיומים סביבתיים פוטנציאליים, כמו אסונות טבע ושריפות. התקנת חיישנים אוטומטיים וציוד מגיב הן שתי דרכים שבעזרתן ה-CISP ישמרו על מרכזי הנתונים. יש להתקין מכשירים לזיהוי כילות מים כדי להתריע בפני העובדים על בעיות כמו פעילות משאבות אוטומטיות כדי שישלכו נזלים וימנעו נזקים. באופן דומה, ציוד אוטומטי לגילוי וכיבוי אש מפחית סיכון ויכול להודיע לעובדי CISP ולכבאים על בעיה.
- **זמינות גבוהה דרך אזורי זמינות מרובים:** CISP צריכים לספק מספר אזורי זמינות לעמידות גבוהה יותר בפני תקלות. כל אזור זמינות צריך להיות מורכב ממרכז נתונים אחד או יותר שמופרדים פיזית זה מזה, ולהיות בעל רשתות וכוח יתירים. אזורי זמינות צריכים להיות מחוברים זה לזה באמצעות רשת סיבים אופטיים מהירה ופרטית, על מנת לתכנן יישומים שעוברים לגיבוי בעת כשל בין אזורי זמינות ללא הפרעה.
- **הדמיית שיבושים ומדידת התגובה שלנו:** ל-CISP צריכה להיות תוכנית המשכיית עסקית כמדריך לתהליך תפעול שמתאר כיצד להימנע משיבושים עקב אסונות טבע ולהפחית אותם, עם צעדים מפורטים שיש לנקוט לפני, במהלך ואחרי אירוע. כדי לצמצם סיכונים ולהתכונן לבלתי צפוי, על CISP לבדוק את תוכנית ההמשכיית העסקית באופן קבוע בעזרת תרגילים המדמים תרחישים שונים. CISP צריכים לתעד את הביצועים של העובדים והתהליכים שלהם, ולאחר מכן לתחקר על לקחים שנלמדו ועל כל פעולה מתקנת שעשויה להידרש לשיפור אופי התגובה. על צוותי CISP להיות מיומנים ומוכנים להתאושש מהפרעות במהירות, ושבידם תהליך התאוששות שיטתי כדי למזער זמן השבתה נוסף עקב שגיאות.
- **עזרה בעמידה ביעדי יעילות:** בנוסף לטיפול בסיכונים סביבתיים, CISP צריכים גם לשלב שיקולי קיימות בתכנון מרכז הנתונים. CISP צריכים לספק פרטים על מחויבותם להשתמש באנרגיה מתחדשת עבור מרכזי הנתונים שלהם, ולספק מידע בנוגע לאופן שבו לקוחותיהם יכולים להפחית את פליטת הפחמן לעומת מרכזי הנתונים שלהם.
- **בחירת אתר:** לפני בחירת מיקום, ה-CISP צריכים לבצע הערכות סביבתיות וגאוגרפיות ראשוניות. מיקומי מרכזי נתונים צריכים להיבחר בקפידה כדי לצמצם סיכונים סביבתיים, כגון שיטפונות, מזג אוויר קיצוני ופעילות סיסמית. אזורי הזמינות של ה-CISP צריכים להיבנות כך שיהיו עצמאיים ומופרדים זה מזה פיזית.
- **יתירות:** מרכזי נתונים צריכים להיות מתוכננים כדי לצפות ולספוג כשלים תוך שמירה על רמות השירות. במקרה של כשל, תהליכים אוטומטיים צריכים להרחיק את התעבורה מהאזור שנפגע. יש לפרוס אפליקציות ליבה בהתאם לתקן N+1, כך שבמקרה של תקלה במרכז הנתונים, ישנה קיבולת מספקת כדי לאפשר איזון של עומס התעבורה לאתרים הנותרים.
- **זמינות:** על CISP לזהות רכיבי מערכת קריטיים שנדרשים כדי לשמור על זמינות המערכת שלהם, ולשחזר שירות במקרה של השבתה. יש לגבות רכיבי מערכת קריטיים במספר מיקומים מבודדים. כל מיקום או אזור זמינות צריכים להיות מתוכננים כך שיעלו באופן עצמאי ושהיו בעלי אמינות גבוהה. יש לחבר אזורי זמינות כדי לאפשר ליישומים לעבור לגיבוי בעת כשל בין אזורי זמינות באופן אוטומטי וללא הפרעה. מערכות בעלות חסינות גבוהה, ובהתאם לכך זמינות השירות, צריכות להיות פונקציה בתכנון המערכת. תכנון מרכזי נתונים עם אזורי זמינות ושכפול נתונים אמור לאפשר ללקוחות CISP להשיג זמינות התאוששות קצרים ביותר ונקודות שחזור מידע מינימליות, כמו גם את רמות זמינות השירות הגבוהות ביותר.

- **תכנון קיבולת:** על CISP לפקח באופן רציף על השימוש בשירות כדי לפרוס תשתית לתמיכה בהתחייבויות ובדרישות זמינות. על CISP לשמור על מודל תכנון קיבולת שמעריך את השימוש והדרישות בתשתית CISP לפחות מדי חודש. מודל זה צריך לתמוך בתכנון דרישות עתידיות ולכלול שיקולים כגון עיבוד מידע, טלקומוניקציה ואחסון יומני ביקורת.

המשכיות עסקית והתאוששות מאסונות

- **תוכנית המשכיות עסקית:** תוכנית המשכיות העסקית של CISP צריכה לתאר בקווים כלליים אמצעים למניעת והפחתת שיבושים סביבתיים. עליה לכלול פרטים תפעוליים לגבי הצעדים שיש לנקוט לפני, במהלך ואחרי אירוע. תוכנית המשכיות העסקית צריכה להיתמך על ידי בדיקות שכוללות סימולציות של תרחישים שונים. במהלך ואחרי הבדיקה, על ה-CISP לתעד את ביצועי העובדים והתהליכים, פעולות מתקנות ולקחים שנלמדו במטרה לשיפור מתמיד.
- **תגובה למגיפה:** על ה-CISP לשלב בתכנון ההתאוששות שלהם מאסונות מדיניות ונהלים לתגובה למגיפה כדי להתכונן לתגובה מהירה לאיומי התפרצות מחלות מידבקות. אסטרטגיות הפחתה כוללות מודלי איוש חלופיים להעברת תהליכים חיוניים למשאבים מחוץ לאזור, ולהפעלה של תוכנית לניהול משברים כדי לתמוך בפעולות עסקיות חיוניות. תוכנית מגיפה צריכה להתייחס לסוכנויות ולתקנות בריאות בינלאומיות, לרבות נקודות מגע בין סוכנויות בינלאומיות.

רישום וניטור

- **סקירת גישה למרכז נתונים:** יש לבדוק באופן קבוע את הגישה למרכז הנתונים. הגישה צריכה להתבטל באופן אוטומטי כאשר תיק עובד נסגר במערכת משאבי האנוש של CISP. בנוסף, כאשר פג תוקף הגישה של עובד או קבלן בהתאם למשך הבקשה שאושר, יש לבטל את גישתם, גם אם הם ממשיכים להיות עובדים של CISP.
- **יומני גישה למרכז נתונים:** יש לרשום ביומן, לנטר ולשמור גישה פיזית למרכז הנתונים של CISP. CISP צריכה לתאם מידע שנרכש ממערכות ניטור לוגיות ופיזיות כדי לשפר את האבטחה לפי הצורך.
- **ניטור גישה למרכז נתונים:** על CISP לפקח על מרכזי נתונים באמצעות מרכזי תפעול אבטחה גלובליים - שאחראים על ניטור, מיון וביצוע תוכניות אבטחה. הם צריכים לספק תמיכה גלובלית 24/7 על ידי ניהול וניטור פעילויות הגישה למרכז הנתונים, וצידוד צוותים מקומיים וצוותי תמיכה אחרים כך שיוכלו להגיב לאירועי אבטחה על ידי מיון, ייעוץ, ניתוח ושליחת תגובות.

מעקב וזיהוי

- **מצלמות אבטחה במעגל סגור:** נקודות גישה פיזית לחדרי שרתים צריכות להיות מוקלטות באמצעות מצלמות אבטחה במעגל סגור (CCTV). התמונות נשמרות בהתאם לדרישות החוק והתאימות.
- **נקודות כניסה למרכז נתונים:** צוות אבטחה מקצועי צריך לשלוט בגישה הפיזית לנקודות הכניסה לבניין על ידי שימוש במערכות מעקב וזיהוי ובאמצעים אלקטרוניים אחרים. צוות מורשה צריך להשתמש במנגנוני אימות בשני שלבים כדי לגשת למרכזי נתונים. הכניסות לחדרי השרתים צריכות להיות מאובטחות במכשירי אזהרה כדי שיוכלו ליזום תגובה לאירוע אם הדלת נפתחת בכוח או מוחזקת פתוחה.
- **זיהוי פריצה:** יש להתקין מערכות אלקטרוניות לזיהוי פריצה בתוך שכבת הנתונים כדי לנטר, לזהות ולהתריע באופן אוטומטי על אירועי אבטחה. נקודות כניסה ויציאה לחדרי השרת צריכות להיות מאובטחות במכשירים שדורשים מכל אדם לספק אימות בשני שלבים לפני אישור כניסה או יציאה. מכשירים אלה ישמיעו אזהרה אם הדלת תיפתח בכוח ללא אימות או תוחזק פתוחה. יש להגדיר התקני אזהרה לדלתות כך שיהיו מקרים שבהם אדם יוצא או נכנס לשכבת נתונים מבלי לספק אימות בשני שלבים. התראות צריכות להישלח מיידית למרכזי פעולות האבטחה של CISP שפועלים 24/7 לטובת רישום ביומן, ניתוח ותגובה מיידית.

ניהול מכשירים

- **ניהול נכסים:** על נכסי CISP להיות מנוהלים באופן מרכזי באמצעות מערכת ניהול מלאי שמאחסנת ומבצעת מעקב על הבעלים, המיקום, הסטטוס, התחזוקה והמידע התיאורי עבור נכסים שבבעלות CISP. לאחר הרכישה, יש לסרוק את הנכסים ולעקוב אחריהם, ויש לבדוק ולנטר את הבעלות, הסטטוס והרזולוציה של נכסים שעוברים תחזוקה.
- **השמדת מדיה:** על התקני אחסון מדיה שמשמשים לאחסון נתוני לקוחות להיות מסווגים על ידי ה-CISP כקריטיים ובשל כך יש להתייחס אליהם בהתאם, כבעלי השפעה גבוהה, לאורך כל מחזור החיים שלהם. ל-CISP צריכים להיות סטנדרטים מדויקים בנוגע לאופן ההתקנה והטיפול במכשירים, ובסופו של דבר הריסתם כאשר אינם שימושיים יותר. כאשר התקן אחסון הגיע לסוף חייו השימושיים, ה-CISP ישבית את המדיה באמצעות טכניקות שמפורטות ב-NIST 800-88. מדיה שאחסנה נתוני לקוחות אינה מוסרת משליטת CISP עד שהושבתה באופן מאובטח.

מערכות תמיכה תפעוליות

- **חשמל:** על מערכות החשמל של מרכז הנתונים של CISP להיות מתוכננות כך שהן יתירות לחלוטין וניתנות לתחזוקה ללא השפעה על הפעילות, 24 שעות ביממה. על CISP להבטיח שמרכזי הנתונים מצוידים באספקת גיבוי של חשמל כדי להבטיח חשמל זמין לשמירה על תפעול במקרה של כשל חשמלי בעומסים קריטיים והכרחיים במתקן.
- **אקלים וטמפרטורה:** על מרכזי הנתונים של CISP להשתמש במנגנונים לשליטה באקלים ולשמור על טמפרטורת פעילות מתאימה עבור שרתים וחומרה אחרת כדי למנוע התחממות יתר ולהפחית את האפשרות להפסקות שירות. כוח אדם ומערכות צריכים לפקח ולשלוט בטמפרטורה ובלחות ברמות המתאימות.
- **גילוי וכיבוי אש:** מרכזי נתונים של CISP צריכים להיות מצוידים בצידוד אוטומטי לגילוי וכיבוי אש. מערכות לגילוי אש צריכות להשתמש בחיישנים לגילוי עשן בתוך חללי עבודה ברשת, בתשתיות ובחללים מכניים. אזורים אלה צריכים להיות מוגנים גם על ידי מערכות כיבוי אש.
- **איתור דליפות:** על מנת לזהות נוכחות של דליפות מים, על CISP לצייד מרכזי נתונים בפונקציה לזיהוי נוכחות מים. אם זוהו מים, יש להפעיל מנגנונים לסילוק מים על מנת למנוע נזק נוסף מהמים.

תחזוקת תשתית

- **תחזוקת ציוד:** על CISP לבצע תחזוקה מונעת של ציוד חשמלי ומכני ולפקח עליה כדי לשמור על המשך תפעול המערכות במרכזי הנתונים של CISP. הליכי תחזוקת הציוד צריכים להתבצע על ידי שאנשים מוסמכים לכך ועליהם להשלים אותם על פי לוח זמנים מתועד לתחזוקה.
- **ניהול סביבה:** על CISP לפקח על מערכות וציוד חשמליים ומכניים כדי לאפשר זיהוי בעיות מיידי. על מנת לבצע זאת, יש להשתמש בכלי ביקורת ומידע רציפים שמסופקים דרך מערכות ניהול מבנים וניטור חשמל של CISP. יש לבצע תחזוקה מונעת כדי לשמור על המשך יכולת הפעילות של הציוד.

משילות וסיכונים

- **ניהול סיכונים מתמשך במרכז הנתונים:** על מרכז תפעול אבטחת המידע של CISP לבצע סקירות שוטפות למרכזי נתונים לזיהוי איומים ונקודות תורפה. יש לבצע באופן שוטף הערכה והפחתה של נקודות תורפה פוטנציאליות באמצעות פעילויות הערכת סיכונים במרכז הנתונים. הערכה זו צריכה להתבצע בנוסף לתהליך הערכת סיכונים ברמת הארגון שמשמשת לזיהוי וניהול הסיכונים שמוצגים לעסק בכללותו. תהליך זה צריך גם לקחת בחשבון סיכונים רגולטוריים ואזוריים וסיכונים סביבתיים.
- **אישור אבטחה של צד שלישי:** בדיקות מרכזי הנתונים של CISP שמתבצעות על ידי צד שלישי, כפי שמתועדות בדוחות של הצד השלישי, אמורות להבטיח שה-CISP הטמיעו כראוי אמצעי אבטחה שמותאמים לכללים הקבועים שדרושים להשגת אישורי אבטחה. בהתאם לתוכנית התאימות ולדרישותיה, בקרים חיצוניים יכולים לבצע בדיקות לסילוק מדיה, לבחון את צילומי מצלמות האבטחה, לצפות בכניסות ובמסדרונות ברחבי מרכז הנתונים, לבדוק התקני בקרת גישה אלקטרוניים ולבחון ציוד במרכזי נתונים.

7. העברות

דרישה	
1.	שירות העברה: כמה שירותים שונים להעברת נתונים מציע ספק הענן?
2.	העברות - ניטור ריכוזי: האם ספק הענן מציע לארגונים שירות מרוכז (כלומר חלון הצגת מידע), שבו הם יכולים לעקוב ולנטר אחר מצב העברות השרתים והיישומים שלהם?
3.	העברות - לוח בקרה: האם כלי ההעברה של ספק הענן מציע לוח בקרה להמחשה מהירה של סטטוס ההעברה, מדדים קשורים והיסטוריית העברה?
4.	העברות - כלים של ספקי הענן: האם כלי ההעברה של ספק הענן מציע אינטגרציה עם כלי העברה אחרים מספק הענן שיכולים לבצע העברות שרתים ויישומים?
5.	העברות - כלים של צד שלישי: האם כלי ההעברה של ספק הענן מאפשר לשלב כלי העברה של צד שלישי? • אם כן, מהם כלי ההעברה הנתמכים של הצד השלישי?

6.	העברות - העברות בין אזורים מרובים: האם כלי ההעברה של ספק הענן מציע יכולת מעקב וניטור עבור העברות שרתים ויישומים שמתרחשות באזורים שונים?
7.	העברות - העברת שרת: האם כלי ההעברה של ספק הענן מציע דרך להעביר לענן שרתים וירטואליים בשטח? • אם כן, אילו סביבות וירטואליות נתמכות כעת?
8.	העברות - גילוי שרתים: האם לכלי ההעברה של ספק הענן יש יכולת גילוי לאיתור אוטומטי של שרתים וירטואליים בשטח שיש להעביר לענן?
9.	העברות - נתוני ביצועי שרת: האם לכלי ההעברה של ספק הענן יש את היכולת לאסוף ולהציג ביצועי שרת ו/או מחשב וירטואלי כמו ניצול מעבד (CPU) או זיכרון גישה אקראית (RAM)?
10.	העברות - מסד נתונים של גילוי: האם לכלי ההעברה של ספק הענן יש את היכולת לאחסן את כל הנתונים שנאספו במסד נתונים מרכזי? • אם כן, האם לארגונים יש את היכולת לייצא נתונים אלה? לאילו פורמטים?
11.	העברות - הצפנה בזמן מנוחה: האם ספק הענן מצפין בזמן מנוחה את כל המידע שנאסף ומאוחסן במסד הנתונים של הגילוי?
12.	העברות - שכפול שרת מצטבר: האם כלי ההעברה של ספק הענן מציע שכפול שרתים מצטבר, אוטומטי וחי במהלך העברת השרת או המחשב הווירטואלי, כדרך לתמוך בכל השינויים שבוצעו בשרת או במחשב הווירטואלי והאם השינויים האלה כלולים בתמונה הסופית שהועברה? • אם כן, לכמה זמן שירות זה יכול לפעול?
13.	העברות - VMWARE: האם כלי ההעברה של ספק הענן תומך בהעברות מחשב וירטואלי של VMWare מהשטח לענן?
14.	העברות - HYPER-V: האם כלי ההעברה של ספק הענן תומך בהעברות מחשב וירטואלי של Hyper-V מהשטח לענן?
15.	העברות - גילוי יישומים: האם לכלי ההעברה של ספק הענן יש את היכולת לגלות ולקבץ יישומים לפני שהם מועברים?
16.	העברות - מיפוי תלות: האם לכלי ההעברה של ספק הענן יש את היכולת לגלות תלות בין שרתים ובין יישומים לפני שהם מועברים?
17.	העברות - העברת מסד נתונים: האם לכלי ההעברה של ספק הענן יש את היכולת להעביר מסדי נתונים שבשטח לענן?
18.	העברות - השבתה בזמן העברת מסד נתונים: האם לכלי ההעברה של ספק הענן יש את היכולת לבצע העברת מסד נתונים לענן בזמן השבתה מינימלי, כלומר מסד הנתונים שהוא המקור יוכל להישאר פעיל במלואו בזמן תהליך ההעברה?
19.	העברות - מקור מסד הנתונים: האם כלי ההעברה של ספק הענן תומך בהעברה ממקורות מסד נתונים שונים כמו שרת Oracle, SQL וכו'? • אם כן, רשמו את כל מקורות מסדי הנתונים הנתמכים שאותם ניתן להעביר לענן.
20.	העברות - העברות הטרוגניות: האם לכלי ההעברה של ספק הענן יש את היכולת לבצע העברות הטרוגניות של מסדי נתונים, כלומר ממקור מסד נתונים אחד ליעד מסד נתונים אחר כמו מ-Oracle לשרת SQL? • אם כן, יש לרשום את כל שילובי ההעברות ההטרוגניים האפשריים של מסדי נתונים.

21.	העברות - העברת נתונים בסקייל של פטה-בייט: האם ספק הענן מציע פתרון העברת נתונים בסקייל של פטה-בייט שמשתמש בכלים מאובטחים כדי להעביר כמויות גדולות של נתונים אל הענן וממנו?
22.	העברות - העברת נתונים בסקייל של אקסה-בייט: האם ספק הענן מציע פתרון העברת נתונים בסקייל של אקסה-בייט להעברת כמויות נתונים גדולות במיוחד לענן?
23.	העברות - גיבויים ארגוניים: האם ספק הענן מציע שירות שמשלב בצורה חלקה מרכז נתונים של לקוח עם שירותי אחסון בענן שיאפשר להעביר ולאחסן נתונים בשירות האחסון של ספק הענן?
24.	העברות - גיבויים ארגוניים - אחסון אובייקטים: האם שירות הגיבוי הארגוני של ספק הענן מציע אינטגרציה עם שירות אחסון האובייקטים בענן של הספק?
25.	העברות - גיבויים ארגוניים - גישה לקבצים: האם שירות הגיבוי הארגוני של ספק הענן מאפשר למשתמשים לאחסן ולאחזר אובייקטים באמצעות פרוטוקולי קבצים כמו פרוטוקול מערכת קבצים ברשת (NFS)?
26.	העברות - גיבויים ארגוניים - גישה לבלוקים: האם שירות הגיבוי הארגוני של ספק הענן מאפשר למשתמשים לאחסן ולאחזר אובייקטים באמצעות פרוטוקולים לאחסון בלוקים כמו פרוטוקול ממשק מערכות מחשב קטנות באינטרנט (iSCSI)?
27.	העברות - גיבויים ארגוניים - גישה לקלטות: האם שירות הגיבוי הארגוני של ספק הענן מאפשר למשתמשים לגבות את הנתונים שלהם באמצעות ספריית קלטות וירטואלית ולאחסן את גיבויי הקלטות הללו בענן של הספק?
28.	העברות - גיבויים ארגוניים - הצפנה: האם שירות הגיבוי הארגוני של ספק הענן מציע הצפנה של נתונים במנוחה ובמעבר?
29.	העברות - גיבויים ארגוניים - שילוב תוכנת צד שלישי: האם שירות הגיבוי הארגוני של ספק הענן משתלב בתוכנת גיבוי נפוצת של צד שלישי?
30.	העברות - הגבלות שירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף ההעברות שלעיל? דוגמה: מספר מרבי של העברות מחשב וירטואלי שמתרחשות בזמנית מספר מרבי להזמנת פתרונות העברת נתונים

8. חיוב

	דרישה
1.	חיוב - מעקב ודיווח: האם ספק הענן מציע שירות מעקב ודיווח לחיוב כדי לעזור למשתמשים לנהל את השימוש שלהם בהצעות הענן ולנטר אותו?
2.	חיוב - התראות והודעות: האם ספק הענן מציע למשתמשים מנגנון להגדרת הודעות התראה שמודיע למשתמשים כאשר ההוצאות שלהם חצו סף מסוים?
3.	חיוב - ניהול עלויות: האם ספק הענן מציע מנגנון לבניית והצגת גרפיקות שמסכמות עלויות והוצאות?

4.	חייב - תקציבים: האם ספק הענן מציע מנגנון להצגת תקציבים וניהולם ולספק תחזית עלויות משוערות?
5.	חייב - תצוגה מאוחדת: האם ספק הענן מציע מנגנון לאיחוד חייבים ממספר חשבונות תחת חשבון משלם אחד ועיקרי?
6.	חייב - הגבלות שירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף החייב שלעיל? דוגמה: מספר מרבי של חשבונות שניתן לקבץ יחד מספר התראות מרבי שניתן ליצור מספר מרבי של תקציבים שניתן לנהל

9. ניהול

	דרישה
1.	ניהול - שירות ניטור: האם ספק הענן מציע שירות ניטור לניהול משאבי ענן ויישומים שאוסף, מנטר ומדווח באמצעות מדדים מוגדרים מראש?
2.	ניהול - התראות: האם שירות הניטור של ספק הענן מאפשר למשתמשים להגדיר התראות?
3.	ניהול - מדדים מותאמים אישית: האם שירות הניטור של ספק הענן מאפשר למשתמשים ליצור ולנטר מדדים מותאמים אישית?
4.	ניהול - ניטור גרעיניות: האם שירות הניטור של ספק הענן מספק רמות שונות של ניטור גרעיניות, עד לרמת הדקה?
5.	ניהול - שירות מעקב API: האם ספק הענן מציע שירות שמבצע רישום ביומן, מנטר ומאחסן פעילות מול משאבי ענן הן בקונסולה והן ברמת ממשק תכנות היישומים (API) לשם שיפור הנראות? • אם כן, מהם השירותים של ספק הענן שמשתלבים עם שירות המעקב הזה?
6.	ניהול - הודעות: האם ספק הענן מאפשר את היכולת לשלוח הודעות על סמך רמות הפעילות של ממשק תכנות היישומים (API)?
7.	ניהול - דחיסה: האם ספק הענן מציע מנגנון לדחיסת יומנים שנוצרו על ידי מערכת המעקב של ממשק תכנות היישומים (API) על מנת לעזור למשתמשים להפחית את עלויות האחסון שקשורות לשירות זה?
8.	ניהול - צבירה אזורית: האם ספק הענן מציע את היכולת לתעד את פעילות ממשק תכנות היישומים (API) בחשבון בכל האזורים ולמסור מידע זה בצורה מצטברת לשם נוחות השימוש?
9.	ניהול - מלאי משאבים: האם ספק הענן מציע שירות לביצוע אומדן, ביקורת והערכת תצורות המשאבים שנפרסו על ידי המשתמש?
10.	ניהול - שינוי תצורה: האם ספק הענן מתעד אוטומטית שינוי בתצורת המשאב כאשר הוא מתרחש?

11.	ניהול - היסטוריית תצורה: האם ספק הענן מציע את היכולת לבחון את תצורת המשאבים בכל נקודה מסוימת בעבר?
12.	ניהול - כללי תצורה: האם ספק הענן מציע הנחיות והמלצות להקצאת תאימות, הגדרתה וניטור רציף שלה?
13.	ניהול - תבניות משאבים: האם ספק הענן מציע למשתמשים את היכולת ליצור, להקצות ולנהל אוסף משאבים בצורה דמוית תבנית?
14.	ניהול - שכפול תבניות משאבים: האם ספק הענן מציע את היכולת לשכפל במהירות את תבניות המשאבים הללו באזורים שונים לשם שימוש פוטנציאלי במצבי התאוששות מאסונות (DR)?
15.	ניהול - מעצב תבניות: האם ספק הענן מציע כלי גרפי קל לשימוש בעל פונקציית גרירה ושחרור שעוזרת להאיץ את תהליך היצירה של תבניות משאבים שכאלה?
16.	ניהול - קטלוג שירותים: האם ספק הענן מציע שירות ליצירת קטלוג שירותים וניהולו, כלומר שרתים, מחשבים וירטואליים, תוכנות, מסדי נתונים וכו'?
17.	ניהול - גישה לקונסולה: האם ספק הענן מציע ממשק משתמש מבוסס אינטרנט כדי להקל על ניהול וניטור שירותי הענן?
18.	ניהול - גישה ל-CLI: האם ספק הענן מציע כלי מאוחד לניהול וקביעת קונפיגורציה של מספר שירותי ענן מממשק שורת הפקודה (CLI) ומאפשר לבצע אוטומציה של משימות ניהול באמצעות שימוש בסקריפטים?
19.	ניהול - גישה סלולרית: האם ספק הענן מציע יישום לטלפון החכם שמאפשר למשתמשים להתחבר לשירות הענן ולנהל את המשאבים שלהם? • אם כן, האם יישום זה זמין גם ב-iOS וגם באנדרואיד?
20.	ניהול - שיטות מומלצות: האם לספק הענן יש שירות שעוזר למשתמשים להשוות את השימוש שלהם בענן לשיטות העבודה המומלצות?
21.	ניהול - הגבלות שירות: האם לספק הענן יש מגבלות כלשהן (כלומר הגבלות שירות) ביחס לסעיף הניהול שלעיל? דוגמה: מספר כללי תצורה מרבי לכל חשבון מספר התראות מרבי שניתן ליצור מספר יומנים מרבי שניתן לאחסן

10. תמיכה

	דרישה
1.	תמיכה - שירות: האם ספק הענן מציע תמיכה בכל עת, 24 שעות ביממה, 7 ימים בשבוע ו-365 ימים בשנה באמצעות טלפון, צ'אט ודוא"ל?
2.	תמיכה - שכבות תמיכה: האם ספק הענן מציע שכבות תמיכה ברמות שונות?

3.	תמיכה - הקצאת שכבות: האם ספק הענן מאפשר למשתמשים להקצות בעצמם את המשאבים/השירותים שנצרכים לרמות שונות של תמיכה בהתבסס על סיווג פרטני, ולא על ידי אילוף משתמשים להחזיק חשבונות ענן נפרדים כדי להשיג ולקבל רמות שונות של תמיכה?
4.	תמיכה - פורומים: האם ספק הענן מציע פורומי תמיכה ציבוריים ללקוחות בהם ניתן לדון בסוגיות שלהם?
5.	תמיכה - לוח בקרה לתקינות השירות: האם ספק הענן מציע לוח בקרה לתקינות השירות שמציג מידע עדכני לגבי זמינות השירות במספר אזורים?
6.	תמיכה - לוח בקרה מותאם אישית: האם ספק הענן מציע לוח בקרה שבו תצוגה מותאמת אישית של ביצועי זמינות השירותים שבבסיס המשאבים הספציפיים של המשתמש?
7.	תמיכה - היסטוריית לוח הבקרה: האם ספק הענן מציע היסטוריה של לוח הבקרה לתקינות השירות 365 ימים אחורה?
8.	תמיכה - יועץ ענן: האם ספק הענן מציע שירות שמתנהג כמו מומחה ענן מותאם אישית ועוזר להשוות את השימוש במשאבים לשיטות עבודה מומלצות?
9.	תמיכה - TAM: האם ספק הענן מציע מנהלים טכניים (TAM) שמספקים מומחיות טכנית עבור כל מגוון שירותי הענן?
10.	תמיכה - תמיכה ביישומי צד שלישי: האם ספק הענן מציע תמיכה במערכות הפעלה נפוצות וברכיבי מערום נפוצים של היישום?
11.	תמיכה - API ציבורי: האם ספק הענן מציע ממשק תכנות יישומים ציבורי (API) שמקיים אינטראקציה תכנותית עם מקרי תמיכה כדי ליצור, לערוך ולסגור מקרים כאלה?
12.	תמיכה - תיעוד השירות: האם ספק הענן מציע מסמכים טכניים באיכות טובה שניתנים לצפייה ציבורית עבור כל השירותים שלו, כולל, אך לא רק מדריכי משתמש, ערכות לימוד, שאלות נפוצות והערות מוצר?
13.	תמיכה - תיעוד CLI: האם ספק הענן מציע תיעוד טכני באיכות טובה שפתוח לצפייה ציבורית עבור ממשק שורת הפקודה שלו (CLI)?
14.	תמיכה - ארכיטקטורות התייחסות: האם ספק הענן מציע אוסף חינוכי ומקוון ובו מסמכי ארכיטקטורת התייחסות שנועדו לעזור ללקוחות לבנות פתרונות ספציפיים שמשלבים רבים משירותי הענן של ספקי הענן?
15.	תמיכה - פריסות התייחסות: האם ספק הענן מציע אוסף חינוכי ומקוון ובו מסמכים שמכילים נהלים מפורטים, בדוקים ומאומתים, שלב אחר שלב, כולל שיטות מומלצות, ליישום פתרונות נפוצים (כמו למשל, Big Data, DevOps, מחסן נתונים, עומסי עבודה של Microsoft, עומסי עבודה של SAP וכו') בהצעות הענן שלו?

נספח ב' - הערכה טכנית חיה

בעת בחירת CISP, חשוב לבצע הערכה 'חיה' ליכולות פלטפורמת הענן באמצעות התשתיות והשירותים של ה-CISP שזמינים לציבור. אנחנו ממליצים על לפחות יום שלם לכל CISP שברשימת הפונים לטובת הערכה טכנית. במהלך ההערכה ניתן: (1) לבצע הערכה מעמיקה כדי לאמוד האם היכולות שהוצגו תואמות לדרישות ה-RFP שלך ולתגובות בכתב של ה-CISP, (2) לספק פלטפורמה למומחים שלך כדי שיוכלו לחקור את ה-CISP ולהבטיח שהוא מתאים לצרכים הטכניים והארגוניים הספציפיים שלך ומתיישר איתם, וכן (3) לפתח אומן בשירותי ה-CISP וביכולתו של ה-CISP להתאים את גודלו, לפעול בצורה מאובטחת, לפעול בצורה עמידה ולהמשיך לחדש כדי לענות על צרכים עתידיים.

כאשר CISPs מגיבים לדרישות RFP לרכישת שירותי ענן, הם עשויים להצהיר על תאימות בהתבסס על פרשנות ברמה גבוהה של הדרישות, שחסרה את ההקשר המלא של צורכי סביבת ההפעלה/יישום של הארגון. אנחנו ממליצים לאייש פאנל הערכה טכנית חיה עם מומחים טכניים, מומחי תפעול, אבטחה ויישומים מובילים. על המעריכים לאתגר את ה-CISP לאורך כל ההערכה, ולפי שיטת העבודה המומלצת, עליהם לדרג CISPs באופן עצמאי, לדרג תרחישים בסולם מוגדר, כגון 0-4 (0=לא מקובל, 1=גבולי, 2=מקובל, 3=טוב, 4=יוצא מן הכלל). לאחר מכן, ניתן לאחד את ציוני ההדגמה, כאשר הציון הממוצע עבור כל תרחיש הערכה עובר להערכת ה-CISP הכוללת. יש לדון בתרחישים בעלי סטיית תקן גבוהה בתוך צוות ההערכה לפני הסיום. לאחר איחוד הציונים, ניתן להחיל שקלול שמבוסס על קריטריוני התרחישים.

מבחינת היקף ההדגמה, אנחנו ממליצים להסתכל על הפלטפורמה של ה-CISP במבט כללי, ולאחר מכן לרדת לעומק הדברים כדי להעריך עומסי עבודה ספציפיים שפועלים על הפלטפורמה. להלן מתווה לדוגמה של פלטפורמה והערכת עומס עבודה. ארגונים יכולים להתבסס על נקודת פתיחה זו או להתאים אותה כדי להבטיח שה-CISP שנבחר עומד בדרישות הפונקציונליות והלא-פונקציונליות הספציפיות שלהם. בתור שיטת עבודה מומלצת, ניתן לאפשר לספקים שהוצגו בפניהם רשימת התרחישים והדרישות להציע סדר יום להערכה החיה שממקסם את הסיקור וכולל זמן שאלות ותשובות בנפח של 20 אחוז.

הערכת הפלטפורמה: CISPs רבים אימצו את המונח 'Well Architected' כדי להתייחס לגישה לענן שמספקת ערך אופטימלי וממזערת סיכונים. תרחישים שהם Well Architected בהדגמה טכנית חיה יכולים לכלול:

1. **אבטחה:** זהות, משילות מרכזית, זיהוי אוטומטי של איומים, הגנת נתונים, מוכנות לאירועים
2. **יעילות ביצועים:** שינוי גודל נכון, מדרגיות/אלסטיות, שירות מנוהל
3. **אמינות:** זמינות גבוהה (עמידות בפני כשלים), הפחתת הסיכון לשינוי, התאוששות מאסונות, גיבוי
4. **ניהול עלויות:** תפעול פיננסי, אופטימיזציה מסחרית, תקציבים והקצאת עלויות
5. **מציאות תפעולית:** אוטומציה, ניטור, תמיכה, ניהול ויכולות שנדרשות כדי לעבור לענן ולפעול בתוך הענן

הערכת עומס עבודה: מערך נפוץ של סוגי יישומים שניתן להדגים כולל:

- **יישום אינטרנט:** אירוח ציבורי של אתר אינטרנט דינמי, כולל מסד נתונים עורפי ואחסון אובייקטים סטטיים.
- **ניתוח נתונים:** אגם נתונים או ארכיטקטורת מאגר מידע שמאפשרת איחוד נתונים מספקי נתונים שונים ויכולת להתמודד עם נפח גבוה (נתונים בנפח טרה-בייט או פטה-בייט), מגוון (מובנה, לא מובנה, פורמטים שונים וכו') ומהירות (קצב יצירת נתונים, דפוסי שינוי ושאלות).
- **פלטפורמת מדע הנתונים:** פלטפורמה שמאפשרת פיתוח, פריסה ושימוש ביכולות מבוססות AI/ML ברחבי הארגון שלכם.
- **יישום IoT:** פלטפורמת/יכולת IoT (האינטרנט של הדברים) שמתפרשת על פני הענן, יכולת רשת והמכשירים.

עבור כל עומס עבודה מייצג שחשוב לארגון שלך, אפשר להגדיר את התרחישים שיוצגו על ידי ה-CISP. התרחישים צריכים להדגים יכולות כוללות שמאפשרות את פריסת עומס העבודה בצורה שהיא Well Architected. הדפים הבאים כוללים קריטריונים לדוגמה של הערכה טכנית חיה (עבור: 1) הפלטפורמה של ה-CISP (2) דוגמה לעומס עבודה של יישום אינטרנט.

פלטפורמה - הערכה טכנית חיה לדוגמה

מזהה תרחיש	שם תרחיש	קריטיות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Plat.Sec.1	איחוד זהויות	4	להציג את היכולת לאחד ממאגר מזהים קיים לשירות הענן.	- תמיכה בפרוטוקולים סטנדרטיים כגון SAML. - תמיכה בשכפול זהות מבוסס SCIM. - היכולת להגדיר רמות גישה שונות בתוך מאגר הזהויות הארגוני ולהחיל אותן בתוך ספק הענן. - היכולת להגביל צוותים/אנשים ספציפיים רק לחשבונות/פרויקטים/עומסי עבודה מסוימים. - יכולת לתמוך בבקרת גישה מבוססת מאפיינים (ABAC) ולהשתמש במאפיינים אלה בתוך מערכת ניהול הזהויות והגישה (IAM) של ספק הענן כדי לשלוט בגישה למשאבי הענן.
Plat.Sec.2	משילות מרכזית	4	להציג יכולת הגדרת מדיניות ודרישות באופן מרכזי, ברמה ארגונית (מדיניות גלובלית) וגם ברמת יחידה עסקית ופרויקט.	- המדיניות צריכה לכלול: הפעלה/השבתה של שירותים, החלת הגבלות גאוגרפיות (הגבלת אזורים). - המדיניות צריכה גם להגביל משתמשים, לרבות מנהלי מערכת, מלהשביט כל בקרת ביקורת/משילות.
Plat.Sec.3	הגבלת הרשאת משתמש	3	להציג את ההמלצות האוטומטיות להידוק הרשאות המשתמש.	- יכולת להשוות הרשאות נוכחיות עם הרשאות נדרשות. - יצירה אוטומטית של מדיניות לקידום הרשאה פחותה.
Plat.Sec.4	רישום ביקורת	4	להציג רישום ביקורת של פעילות בענן, כולל פעולות מותרות ופעולות אסורות כאחד.	- יומנים מרכזיים לכל הארגון. - יומנים ספציפיים לחשבון/פרויקט לתמיכה במעקב ובאחריות דיווח ברמה נמוכה. - כלים לאפשר הצגת שאלות ביומנים. - כלים המאפשרים הזנקת פעולות על סמך אירועים/ערכי יומן ספציפיים. - יכולת צפייה בפעילות תמיכת ספקים. - יכולת למנוע מחיקה של יומנים, אפילו על ידי מנהלים.
Plat.Sec.5	בידוד רשת	4	להדגים ולהוכיח במידת האפשר את הבידוד של דיירים שונים בתוך הענן. להדגים את התצורה של רשתות משנה מבודדות (ללא קישוריות), פרטיות (ללא אינטרנט) וציבוריות (עם גישה לאינטרנט).	- הפרדת דיירים, כולל בשירותי VPN וחיבור צולב. - יכולת שליטה בזרימת התעבורה מחוץ לתשתית הענן (on-prem), בתוכה ואל האינטרנט. - כיצד חלה ההפרדה בעת שימוש בשירותים משותפים כגון אירוח בקונטיינר או פונקציה כשירות.
Plat.Sec.6	הצפנה במנוחה	4	להדגים את היכולת להצפין נתונים במצב מנוחה, כולל אפשרויות BYOK והצפנה מצד הלקוח.	- יכולת לדרוש הצפנה עבור נתונים רגישים. - יכולת להשתמש במפתחות מנוהלים של ספק או במפתחות מנוהלים של לקוחות. - הקפדה על FIPS 140-2. - יכולת להתריע על עמידה לקויה בדרישות ההצפנה ולרשום זאת ביומן.

מזהה תרחיש	שם תרחיש	קריטריות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
				- השפעה נוספת על העלות. - השפעה על הביצועים. - תמיכה באלגוריתמים מוגני קוונטום ובגדלי מפתח.
Plat.Sec.7	הצפנה במעבר	4	להדגים את היכולת להצפין נתונים במעבר.	- הצפנה כברירת מחדל עבור ממשקי API של שירות. - יכולת לאפשר הצפנה במעבר (TLS) במאזני עומסים ובממשקי API מנוהלים. - תמיכה באימות הדדי (לקוח ושרת).
Plat.Sec.8	ניהול מפתח	4	להדגים את יכולת ניהול המפתחות שלך. לכלול את מחזור החיים המלא של המפתח. לכלול אינטגרציה עם שירותי ענן.	רישום יצירת מפתחות, שימוש בהם, סיבובם והשמדתם.
Plat.Sec.9	ניהול תצורה	3	להדגים את יכולת ניהול התצורה שלך בפלטפורמת הענן.	- לשמור על CMDB מדויק. - לבדוק אם יש תאימות. - לעורר ביצוע אוטומטי של פעולות בהתבסס על אי תאימות. - יכולת להעריך שינויים בתצורה מול שיטות עבודה מומלצות או כללים מותאמים אישית.
Plat.Sec.10	אבטחת רשת	3	להדגים את יכולת חומת האש וה-Firewall של יישומי אינטרנט, כולל אינטגרציה עם ערכות כללים/חומת אש של צד שלישי והגנה מפני תקיפת נפח.	- יכולות WAF (Web Application Firewall): מדרגיות. - תמיכה ברשת פרטית כמו גם בציבורית. - יכולת להירשם לעדכוני תעשייה/ספקים לקבלת ערכות כללים. - לעורר אוטומטית פעולות בתוך התשתית בהתבסס על אירועים מה-WAF. - יכולות חומת אש, מדרגיות. - חומות אש מבוססות מארח ומבוססות רשת. - יכולת להתייחס לקבוצות יומנים או אובייקטים לוגיים בנוסף ליכולת לציין CIDR IP Blocks. - מספר הכללים הנתמכים בכל רמה/רכיב. - יכולת לתמוך במודל הפעלה מבוזר (צוות רשת + צוות מפתחים) באמצעות מדיניות ותצורת רשת.
Plat.Sec.11	קישוריות רשת	3	להדגים את היכולת להתחבר לרשתות מקומיות וכן לחבר נקודות קצה/לקוחות לרשתות פרטיות בתוך הענן.	- קישוריות פרטית (רוחב פס גבוה < 10GBs). - יכולת לשלוט במדיניות ניתוב וחומת אש ברחבי הארגון. - קישוריות VPN (מאתר לאתר ומבוססת לקוח). - תמיכה ב-IPv6.
Plat.Sec.12	ניהול מופעי שרת	3	להדגים יכולות ניהול מופעי שרת.	- יכולת לנטר ולנהל מצב תיקון בנפח גדול של מופעי שרת. - תמיכה בניהול תיקוני מערכת הפעלה מסוג Windows-I Linux.

מזהה תרחיש	שם תרחיש	קריטיות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
				- יכולת ביצוע פקודות על פני צי שרתים ללא צורך ב-Ssh. - יכולת שליטה וביקורת בגישה מרחוק למחשבים וירטואליים באופן מרכזי. - יכולת לשנות גודל מופע שרת, לצרף אמצעי אחסון נוספים, לשנות תצורת רשת וכו' באמצעות Console, CLI ו-API.
Plat.Sec.13	יישום מדיניות	3	להציג את היכולת להגדיר שירותים כדי למנוע גישה מהאינטרנט הציבורי.	- יכולת לבדוד תעבורה לרשת פרטית עבור שירותים שעשויים להכיל נתונים קריטיים/סודיים. - יכולת להגדיר מדיניות השולטת בגישה לנתונים על סמך רשת המקור. - החלת הגבלות גישה אלו על כל המשתמשים, כולל משתמשים בעלי אישורים בדרגה גבוהה.
Plat.Sec.14	סריקת פגיעות	2	להדגים את היכולת לסרוק תמונות (קונטיינר ומחשב וירטואלי (VM)) לאיתור נקודות תורפה.	- יכולת לסרוק אוטומטית קונטיינרים ברישום. - יכולת לסרוק מחשבים וירטואליים לאיתור נקודות תורפה ידועות. - יכולת ביצוע סריקת רשת.
Plat.Sec.15	בדיקת רשת	2	להדגים את היכולת ללכוד/לשקף תעבורת רשת (NetFlow וחבילת מנות מלאה) מתוך סביבת לקוח.	- יכולת לשקף חלק/כל התעבורה בתוך תשתית ספק הענן (מנקודת מבט של דייר הלקוח), כולל לכידת מנות מלאה. - יכולת לבחור איזו תנועה רוצים לתפוס. - יכולת להתאים לנפחי תעבורה גדולים מאוד ($50\text{Gbps} <$).
Plat.Sec.16	איתור איומים	3	להדגים את יכולת זיהוי החדירה של הפלטפורמה שלך, כולל איומים מרשת, שימוש באישורים וניתוח דפוסי שימוש לדוגמה.	- יכולת לזהות פעילויות חשודות כמו "כרייה". - יכולת לזהות התקפות כוח גס (Brute Force) לצורך אימות כמו כניסות Ssh. - יכולת לזהות דליפה של אישורים או שימוש לרעה. - יישום של ML, ניתוח מספרים גדולים של אירועים והצגת אירועים עם עדיפות. - מאמץ להפעיל/להגדיר (היופי בפשטות). - יכולת שילוב עם שירותים חיצוניים והפעלת הודעות. - יכולת להגדיר את ה-IDS ברמה גלובלית עבור כל הפרויקטים/חשבונות.
Plat.Perf.1	אופטימיזציה של מחשב	2	להציג המלצות אוטומטיות לאופטימיזציה של עלויות מחשב וירטואלי ופונקציה כשירות.	- המלצות המבוססות על ניצול בפועל ודפוסי עומס עבודה. - ההמלצות כוללות חישובן משוער ותובנות לגבי רמת עומס צפויה/השלכות טכניות. - אופטימיזציות צריכות לכלול גם חישובן וגם "סיכון ביצועים" כאשר ייתכן למשל שמחשבים וירטואליים יהיו קטנים מדי.

מזהה תרחיש	שם תרחיש	קריטריות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Plat.Perf.2	אופטימיזציה של הסביבה	2	להציג המלצות אוטומטיות לרכיבי ענן אחרים כגון מאזני עומסים, עבודה ברשת, מסדי נתונים, אחסון וכו'.	המלצות מזהות חיסכון והזדמנויות פוטנציאליות ליעילות ביצועים ברכיבים אחרים מעבר למחשוב הליבה.
Plat.Perf.3	חישוב Auto-Scaling	4	להציג את יכולות ה-Auto-Scaling של יישום הפרוס מאחורי מאזן עומסים בסביבת מחשוב וירטואלית. להציג את האפשרויות/הגישות השונות הזמינות ואת היכולת לעורר פעולות אחרות (אופציונליות) לפני/אחרי אירועי שינוי סקייל, כגון הודעה.	- אפשרויות שונות לשינוי סקייל, גישות מבוססות גורם מפעיל, מבוססות זמן, ידניות או חכמות יותר המיישמות למידת מכונה כדי לחזות את הקיבולת הנדרשת. - שינוי סקייל אוטומטי לחלוטין, כולל רישום עם מאזן עומסים ובדיקות תקינות. - היכולת לבצע קטע קוד שרירותי בנקודות ספציפיות של מחזור החיים של שינוי הסקייל.
Plat.Perf.4	שינוי סקייל מקוון לאחסון	3	להדגים את היכולת להתאים את הקיבולת ואת התפוקה של אחסון בלוק ללא הפרעה לעומס העבודה.	- יכולת העברת אחסון בלוק בין סוגי אחסון שונים ללא צורך בבנייה מחדש לחלוטין של שירותים. - יכולת להגדיל את גודל הנפחים המוצגים ל-VMs.
Plat.Perf.5	Auto-Scaling עבור שירותים מנוהלים	3	להדגים את היכולת של מאגר האובייקטים, ה-API Gateway, פלטפורמת FaaS ומסד הנתונים של NoSQL לשנות את הגודל מכמה (עשרות) להרבה (אלפים) משתמשים בו-זמנית.	- להציג את יכולת ה-Auto-Scaling חלק, יתבצע באופן אידיאלי ללא התערבות מנהל. - ביצועים עקביים במהלך תקופה מואצת של שינוי סקייל כלפי מעלה שמוותאם לדרישות שינוי הסקייל של הייצור. - עבור חלק מהרכיבים, כמו FaaS, יש לבדוק במידת הצורך אפשרויות לחימום מוקדם ולניהול מגבלות ביצוע במקביל.
Plat.Perf.6	עומסי עבודה מבוססי קונטיינר	3	להדגים את היכולת לארח עומסי עבודה מבוססי קונטיינר.	- אפשרויות לפלטפורמות אירוח קונטיינרים. - אינטגרציה עם רכיבי IaaS אחרים כגון מאזני עומסים. - זמינות של פתרון רשת שירות. - אפשרויות לא קנייניות לאירוח קונטיינרים, כגון Kubernetes. - תמיכה מקורית לזמינות גבוהה בתוך מישור הבקרה בקונטיינר. - יכולת ניהול מארחי קונטיינר באתר.
Plat.Rel.1	חוסן אזורי	4	להדגים את המעבר האוטומטי לגיבוי בעת כשל של מופע שרת מסוג מסד נתונים קשור בתוך אזור כאשר יש הדמיה של כשל מקומי גאוגרפי (כגון הפסקת חשמל).	- מעבר אוטומטי לגיבוי בעת כשל. - אזורי שבר מבוססים בתוך אזור ענן. - תחום באופן ברור ופשוט לביצוע ארכיטקטורה לקבלת זמינות גבוהה.
Plat.Rel.2	שחזור אוטומטי של מופע שרת	2	יש להדגים את השחזור האוטומטי של מופע שרת/מערך מופעי שרת לאחר בדיקת תקינות שנכשלה.	- בדיקות תקינות הניתנות להגדרה. - שחזור/הקצאה מחדש של מופע שרת אוטומטי לחלוטין.
Plat.Rel.3	מודעות לתקינות מאזני עומסים	3	להדגים כיצד מאזן עומסים מזהה אוטומטית מופע שרת פגום ומנתב מחדש את התעבורה למארחים תקינים אחרים.	- בדיקות תקינות הניתנות להגדרה. - ניתוב תעבורה אוטומטי למארחים תקינים.

מזהה תרחיש	שם תרחיש	קריטיות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Plat.Rel.4	מעבר לגיבוי בעת כשל אזורי	3	להדגים ארכיטקטורה מרובת אזורים, כולל מעבר אוטומטי של תעבורה לאזור משני.	- בדיקות תקינות עם מודעות גלובלית. - אפשרויות ניתוב אוטומטיות: השהיה, שקלול ומעבר לגיבוי בעת כשל. - תמיכה בעומסי עבודה של מחשבים וירטואליים כמו גם שירותים מנהלים כמו שירות מסד נתונים של Object Store/NoSQL.
Plat.Rel.5	גיבוי ושחזור	4	להדגים את אפשרויות הגיבוי והשחזור עבור: מחשבים וירטואליים, מסדי נתונים, שירותים מנהלים.	- רמת אוטומציה. - יכולת שחזור לאותו אזור ענן/אזור ענן אחר. - יכולת העתקת גיבויים לאזור ענן אחר.
Plat.Cost.1	תקציבים	3	להדגים יכולת ניהול תקציב, כולל כיצד לבנות אותו עבור חשבונות משנה ופרויקטים.	- לשקול את היכולת ליישם בקרות תקציביות וניטור ברמות השונות של הארגון שלך. - לבדוק גמישות, למשל ביכולת לקבץ רכיבים (באמצעות תיוג), להגדיר תקציבים לשירותי ענן ספציפיים ולהגדיר ספים לשליחת הודעות/ניטור.
Plat.Cost.2	הקצאת תקציב	1	להדגים הקצאת סביבת פרויקט חדשה (חשבון), כולל תהליך הקצאת התקציב לפרויקט. ההקצאה צריכה לכלול שלבי אישור ידני עבור 1 IT/סקירה טכנית, 2 סקירה מסחרית/פיננסים.	- יכולת הקצאה עצמית, עם האישורים המתאימים. - אוטומציה של תצורת הגדרת התקציב המתאימה, הודעות או מדיניות תקציב בהתאם לארגון שלך.
Plat.Cost.3	דיווח תקציב	2	להדגים את היכולת לדווח על תקציבים ברחבי הארגון. דיווח למחלקה ספציפית לעומת דיווח לכל הארגון (הצורך לדעת). הדיווח צריך לכלול ערכי הוצאה "ממשיים" כמו גם חזויים/משוערים.	- היכולת לספק נראות ברמות שונות של הארגון, יצירת מודעות ושקיפות, אך על בסיס "הצורך לדעת". - החיזוי צריך להתבסס על מגמות הצריכה הנוכחיות והקודמות ולספק אזהרה מוקדמת על חריגה פוטנציאלית בתקציב.
Plat.Cost.4	בקורות תקציב	1	להדגים את היכולת לנקוט פעולות כאשר מגיעים לסף התקציב. הפעולות יכולות לכלול הודעות, החלת אילוצים או התערבות אקטיבית למניעת הוצאות מעל התקציב.	- היכולת להגדיר פעולות בפשטות לפרויקטים שונים. - היכולת של הפעולות להשתנות מפרויקט אחד למשנהו, למשל - תוך התחשבות בפיתוח (Dev) לעומת ההשלכות על הייצור (Prod). - היכולת להגדיר מספר פעולות וספים לאותו תקציב/פרויקט. - היכולת להגדיר פעולות מותאמות אישית בנוסף ליכולות הסטנדרטיות.
Plat.Cost.5	מחזוריות תקציב	1	להדגים את היכולת ליישם תקציבים לתקופות זמן שונות, יומי/חודשי/שנתי וכו'. עבור תקציבים שנתיים, יש להדגים את היכולת ליישם התפלגות משתנה של ההוצאה הצפויה לאורך השנה.	- יכולת הגדרת תקציבים לתקופות זמן שונות. - יכולת להגדיר התפלגות של הוצאות על פני השנה עבור תקציבים שנתיים, חשוב במיוחד עבור עומסי עבודה עונתיים/אלסטיים במיוחד כמו החזר מס שנתי למשל.
Plat.Cost.6	Marketplace של צד שלישי	3	להדגים את היכולת לקנות ולפרוס מוצרים של צד שלישי. יש להדגים כיצד להגדיר תקציב עבור מערך של מוצרים מגורמי צד שלישי הזמינים דרך Marketplace וכן את היכולת להגביל את המוצרים הזמינים.	- יכולת קביעת תקציב למוצר ספציפי; תקציב גלובלי, תקציב למערך של פרויקטים/חשבונות. - יכולת להציג רק תת-מערך של ה-Marketplace הרחב יותר למשתמשי הענן.

מזהה תרחיש	שם תרחיש	קריטיות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Plat.Cost.7	חישוב מודלים של תמחור	3	להדגים את המודלים השונים של תמחור/מסחר שניתן ליישם על מחשבים וירטואליים.	- היכולות צריכות לכלול תמחור לפי שימוש בפועל, ללא התחייבות לטווח ארוך ופרטני (לדקה/שעה). - התחייבויות אופציונליות לטווח ארוך בתמורה להנחה. - יכולת לקנות מופעי שרת עם הסכמה שייתכנו הפרעות בתמורה להנחה. - חשוב לציין, ערבוב המודלים הללו בתוך אותו פרויקט/חשבונות אמור להיות אפשרי, כמו גם לחלוק הטבות בין חשבונות שונים.
Plat.Cost.8	המלצות אופטימיזציה מסחרית	3	להדגים את היכולת לקבל המלצות אופטימיזציה מסחריות לאופטימיזציה של ההוצאות (ללא צורך לבצע שינויים טכניים).	- המלצות הוליסטיות למספר שירותים, כולל למשל למחשבים וירטואליים ולמאגרי מידע מנוהלים. - יכולת להוציא לפועל המלצות בפשטות ולהבין את החיסכון/התועלת הצפויים.
Plat.Cost.9	מארחים ייעודיים	4	להדגים את היכולת להקצות מארח ייעודי כדי לאפשר שימוש ברישוי בשטח הקשור למארח ספציפי.	- קלות ההקצאה. - יכולת ניהול ניצול המארח. - היכולת לשתף את המארח בפרויקטים/דיוורים שונים.
Plat.Ops.1	העברת מחשבים וירטואליים	3	להדגים יבוא של מחשב וירטואלי (VM) משירות באתר לשירות מבוסס ענן.	- יכולת לייבא מערכות הפעלה שהן גם מבוססות Windows וגם Linux. - יכולת לייבא מספר מחשבים בו זמנית. - יכולת לתחזק הפעלת שכפול כדי לאפשר מעבר מהיר לגיבוי בענן בעת כשל.
Plat.Ops.2	יכולות DevOps ואוטומציה	4	להדגים את יכולות ה-DevOps/אוטומציה, כולל איך סביבות מוגדרות כקוד, תמיכה מפריסות אוטומטיות לחלוטין, בדיקות אוטומטיות וחזרה למצב קודם.	- יכולת להגדיר את כל רכיבי המערכות כקוד, כולל רשת, מחשבים וירטואליים, אחסון, מסדי נתונים. - יכולת ליצור Pipeline. - יכולת ליצור מאגר קודים. - יכולת לבצע אוטומציה לגרסאות Build. - יכולת לבצע פריסות כחולות/ירוקות. - יכולת ליצור סביבות מרובות ולהחיל מספר שלבים לפריסות. - חזרה אוטומטית למצב קודם לאחר פריסות שנכשלו.
Plat.Ops.3	אחסון יישומים	2	להדגים אירוח של יישום דו-שכבתי פשוט בשירות Low-Code/פלטפורמה. כולל מסד נתונים קשור ו-Auto-Scaling עבור שכבת היישום/האינטרנט.	- תצורה פשוטה באמצעות ממשק המשתמש. - הכללת בדיקות תקינות, שינוי סקיל, זמינות גבוהה. תמיכה בפלטפורמה, Windows ו-Linux.
Plat.Ops.4	שילוב אבטחה	2	להדגים את יכולות האינטגרציה של הפלטפורמה של מנקודת המבט של אירועי אבטחה וניהול אירועים.	יכולת לשלב בקלות ולצורך יומנים הקשורים לאבטחה מספק הענן + ממשקי API לשילוב.

מזהה תרשי	שם תרשי	קריטיות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Plat.Ops.5	שילוב של ITSM	3	להדגים את יכולות השילוב של הפלטפורמה שלך מנקודת מבט של ITSM (ניהול שירות IT).	- יכולת להעלות, לנטר ולעדכן מקרה תמיכה באמצעות API. - יכולת להקצות שירותים או מערכים של שירותים כ"מוצרים" באמצעות API.
Plat.Ops.6	תמיכה	4	להדגים את הצעת התמיכה שלך.	- רמות שונות של תמיכה עבור סוגים שונים של עומסי עבודה. - יכולת לתמוך גם במערכת ההפעלה/מנוע מסד נתונים וכו' בהתאם לשירות נתון. - יכולת להציע כפפות לבנות עם מובילי תמיכה בעלי שם לעומסי עבודה קריטיים. - יכולת להציע מוכנות מובנית לאירועים ותהליך סקירת ארכיטקטורה. - תובנה לגבי מפת הדרכים של הספק.
Plat.Ops.7	יכולת ביקורת	4	להדגים את הכלים שיש לך כדי לתמוך בביקורות תאימות.	- יכולת לקבל פרטי ביקורת תאימות דרך הקונסולה. - יכולת ניהול ואוטומציה של ביקורות סביבה.
Plat.Ops.8	מחשב וירטואלי (VM) לקונטיינר	1	להדגים המרה של יישום במחשב וירטואלי לקונטיינר, והגשתו באמצעות פלטפורמת הקונטיינר של ספק הענן.	- קלות השימוש בהמרה. - זמן המרה. - תמיכה בפלטפורמה, .Net ו-Java.

עומס עבודה: יישום אינטרנט - הערכה טכנית חיה לדוגמה

הסעיף הבא מספק גיליון הערכת עומס עבודה לדוגמה עבור עומס ספציפי של "יישום אינטרנט". כאשר מפתחים גיליון הערכה עבור יישום נתון, מומלץ מאוד לערב את המשתמשים, המפתחים והמנהלים של היישום, כיוון שהם צפויים להבין את הדרישות, האתגרים והאילוצים הנוכחיים בצורה הטובה ביותר.

מזהה תרחיש	שם תרחיש	קריטיות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Web.Sec.1	אבטחה - הגנת יישומים	3	להדגים את היכולת לחסום ניסיונות זדוניים לנצל את היישום באמצעות החדרת SQL, התקפת Scripting XSS והתקפות אחרות.	- יכולת הגנה מפני התקפות נפוצות "מחוץ לקופסה" עם כללים/יכולות סטנדרטיים. - יכולת ליצור בדיקות/כללים/פונקציות מותאמים אישית.
Web.Sec.2	אבטחה - הגנה מבוססת תעריפים	3	להדגים את היכולת לחסום/להגן מפני התקפות הכוללות שיעורי בקשות גדולים או נפחי נתונים המכוונים ליישום.	יכולת להגדיר מגבלות ולהגביל את שיעורי הבקשות מכתובת IP נתונה או מרשימה של כתובות.
Web.Sec.3	אבטחה - הגנה מבוססת מקור	3	להדגים את היכולת להגביל גישה על סמך רשת/מקור גאוגרפי.	- יכולת להגביל לפי חסימת רשת או לפי רשימה של חסימות רשת. - יכולת להגביל לפי ארץ מקור (ללא צורך בניהול רשימות IP).
Web.Sec.4	אבטחה - פילוח רשת	4	להדגים את היכולת לבדד/להגן על רכיבים (שרת אינטרנט, שרת יישומים/שרת DB) כדי להגן מפני התפשטות לכיוון צפון-דרום וגם לכיוון מזרח-מערב דרך התשתית.	- יכולת למקם רכיבים ברשתות משנה שונות ולשלוט בזרימת התעבורה בין רשתות משנה שונות. - יכולת שליטה בזרימת התעבורה ברמת ממשק רשת. - יכולת התייחסות לקבוצות יומנים כמו גם לבלוקים של CIDR.
Web.Sec.5	אבטחה – תמיכה וניהול אישורים של אבטחת שכבת תעבורה (TLS)	4	להדגים את היכולת לספק נקודת קצה מאובטחת TLS ולנהל אוטומטית את הרכיבים התומכים כדי לספק זאת, כולל למשל סיבוב אוטומטי של אישורים.	- תמיכה בפרוטוקולי TLS העדכניים ביותר והיכולת להשביט גרסאות מדור קודם במידת הצורך. - הפקה, ניהול ורענון של אישורים פשוטים (באופן אידיאלי אוטומטיים לחלוטין).
Web.Perf.1	ביצועים - מדרגיות	4	להדגים את היכולת לשנות את הגודל של יישום האינטרנט מ-10 ל-100,000 משתמשים בו-זמנית באמצעות Auto-Scaling דינמי.	- יכולת להגדיר כללי שינוי סקייל מבוססי זמן כמו גם מבוססי גורם מפעיל. - שינוי סקייל חלק עבור משתמש הקצה ומנהל המערכת. ביצוע הרחבה אופקית אוטומטית כאשר העומס גדל והפחתה כאשר העומס יורד. - יש לוודא שקיימת מדרגיות בכל שכבה של יישום האינטרנט (מאזן עומסים, שכבת אינטרנט, שכבת נתונים וכו'). - הזמינות לשירותי אחסון במטמון בשכבות שונות של היישום לפי הצורך.
Web.Perf.2	ביצועים - משלוח גלובלי	3	להדגים את יכולת ה-CDN שכולל הדגמת זמן השהיה מנקודות שונות ברחבי העולם, כולל: אוסטרליה, אסיה, אפריקה, המזרח התיכון, צפון אמריקה, דרום אמריקה ואירופה.	- יכולת ליצור ולהגדיר CDN דרך קונסולה/CISP/ממשקי API. - כללי הפצה הניתנים להגדרה עבור אזורים גאוגרפיים שונים. - מטמון ניתן להגדרה עבור מקרי שימוש/יישומים שונים.

מזהה תרחיש	שם תרחיש	קריטריות (1=נמוכה, 4=קריטית)	דרישות הדגמה	שיקולי ניקוד
Web.Rel.1	אמינות - חוסן אזור יחיד	4	להדגים את היכולת לסבול אירוע מקומי כגון אובדן קישוריות רשת למרכז הנתונים של CISP.	מעבר אוטומטי לגיבוי בעת כשל וזמינות גבוהה בתוך אזור ענן (עיר).
Web.Rel.2	אמינות - פריסה מרובת אזורים	3	להדגים פריסה מרובת אזורים של יישום אינטרנט כולל מסד נתונים משוכפל גלובלית.	- יכולת לפרוס יישום מרובה אזורים באופן תכנותי. - שכפול בין האזורים עבור מאגר הנתונים. - ניתוב אוטומטי של משתמשים לאזור האופטימלי שלהם.
Web.Rel.3	אמינות - מעבר לגיבוי מרובה אזורים בעת כשל	3	להדגים את המעבר האוטומטי לגיבוי בעת כשל של יישום אינטרנט במקרה של בעיית שירות המשפיעה אזורית.	מעבר אוטומטי לגיבוי בעת כשל וזמינות גבוהה בתוך אזורי ענן מרחבים.
Web.Cost.1	עלות - נראות	2	להדגים את היכולת לעקוב אחר עלות לכל יישום.	יכולת לראות עלויות היסטוריות עבור יישום ספציפי, כולל מתי הוא מבצע סקייל למעלה/למטה.
Web.Cost.2	עלות - תקציבים	2	להדגים את היכולת להגדיר תקציבים והתראות הקשורות לכל יישום.	תקציבים המוגדרים לפי יישום והיכולת לעורר פעולות/התראות על סמך ערכי סף מוגדרים.
Web.Ops.1	צוות התפעול - חלונות תחזוקה	3	להדגים את היכולת להגדיר חלונות תחזוקה כך שיתאימו לדרישות העסקיות, במיוחד כאשר התחזוקה עשויה להשפיע על זמינות היישומים.	חלונות תחזוקה הניתנים להגדרה עבור רכיבים כמו שירות מסד נתונים קשור.
Web.Ops.2	צוות התפעול - רישום ביומנים	3	להדגים את היכולת לרכז רישום ביומנים עבור יישום עם מספר רכיבים, כולל התמדה של יומנים עם סיום/כשל של מחשבים וירטואליים.	- יכולת להגדיר שירות רישום מרוכז שיכול להתאים את גודלו לפי דרישות היישום. - יכולת להגדיר כללים/מסננים להפעלת הודעות או פעולות על סמך אירועי יומן ספציפיים.
Web.Ops.3	צוות התפעול - ניטור	3	להדגים ניטור של היישום, לרבות ביצועים, זמינות, זמני תגובה, ספירת שגיאות וכו' ופונקציונליות לביצוע פעולה/הפעלת הודעות על סמך ספי מדדים שונים.	- אוסף של מדדים סטנדרטיים זמינים כגון CPU, IO, מדדי מסד נתונים, רשת, מאזן עומסים וכו'. - יכולת להגדיר מדדים וספים מותאמים אישית. - יכולת ליצור לוח בקרה מותאם אישית כדי לייצג את המדדים החשובים ביותר ולשתף את לוחות המחוונים הללו עם משתמשים רלוונטיים.