קהילת נימבוס CCoE

מפגש #4

מודל ההפעלה לענן – פן תהליכים ושינוי ארגוני

20.3.2023

נימבוס
Cloud Me In

let's gov
נימבוס CCoE

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

סדר יום

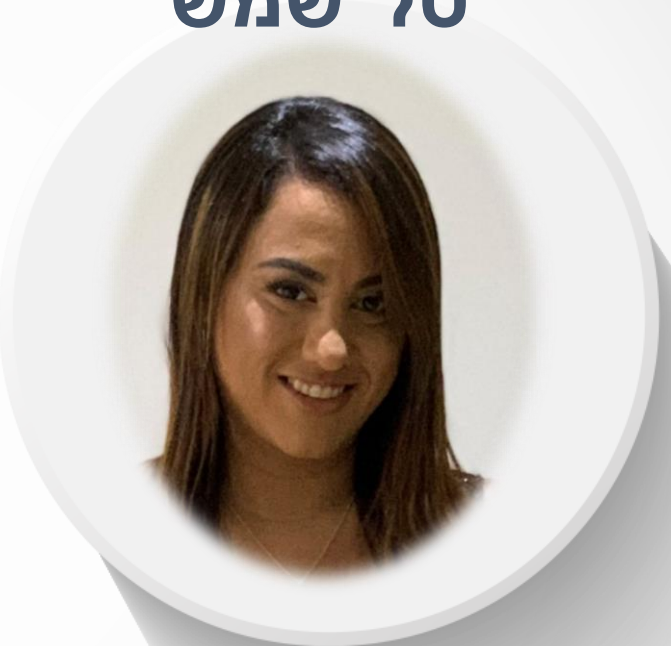
שעות	נושא	באחריות
9:00 -8:30	התכנסות	
9:00-9:30	פתיחת המפגש סטטוס יחידת ענן	קרן בר-לב
10:00 - 9:30	מודל ההפעלה הממשלתי בענן בפן התהליכים והשינוי הארגוני	קרן בר-לב
10:30 - 10:00	משרד משתף - ניהול תקציבי בענן בהיבט אגפי הטד"מ	נדב שרייבמן
11:00 - 10:30	הפסקה	
12:00 – 11:00	הרצאה – שינוי ארגוני	זיו מנדל
12:30 – 12:00	הגשר לענן – DevOps בהיבט השינוי הארגוני במעבר לענן	ויקטור חזנוב
13:00 - 12:30	הפסקה	
13:45- 13:00	בין הוירטואלי לפיננסי - השינוי בהיבט ניהול התקציב	ירון אמיר
14:45 - 13:45	ארכיטקטורת פרויקט בהיבט תקציבי - משחק המחשה ודיונים סביב שולחנות	ירון/ ויקטור/נדב
15:15 - 14:45	התכנסות וסיכום מפגש	קרן בר-לב

סטטוס פרויקט נימבוס
יחידת ענן

קרן בר-לב
CTO ממשלתי
מנהלת CCoE

מצטרפים חדשים לצוות CCoE,
נעים להכיר

טל שמש



- בעלת ניסיון בניהול פרויקטים אפיון תהליכים, ניהול הרכש ובניית תקציבים במערכות מידע
- ניסיון בניתוח מערכות, ניהול צוות HelpDesk ועולמות הפיתוח
- את זמני הפנוי מקדישה לבילוי עם המשפחה חברים, לימודים לתואר שני, טיולים ובישול.

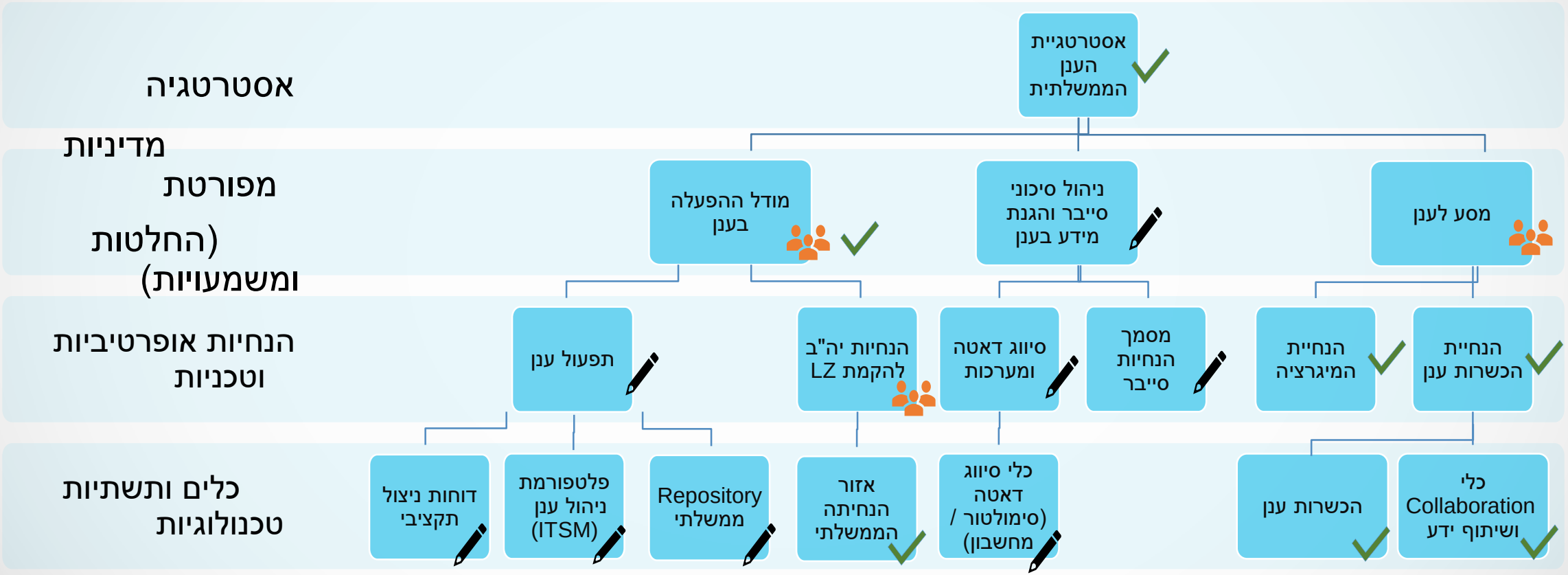
ויקטור חזנוב



- עם 15+ שנות ניסיון בעולמות פיתוח ו- IT כמוביל טכנולוגי בחברות Enterprise / Startup בארץ ובחו"ל.
- בשנים האחרונות עיקר העיסוק הוא כארכיטקט ענן וניהול קבוצות פיתוח
- את זמנו הפנוי מקדיש בעיקר לבילוי עם המשפחה וספורט.

סטטוס תוצרי ה-CCoE

סטטוס הפעילות: ✓ פורסם/עלה לאוויר | הועבר להתייחסות | בעבודה



* כל מסמך יתייחס ליעדים הרלוונטיים מתוך מסמך האסטרטגיה

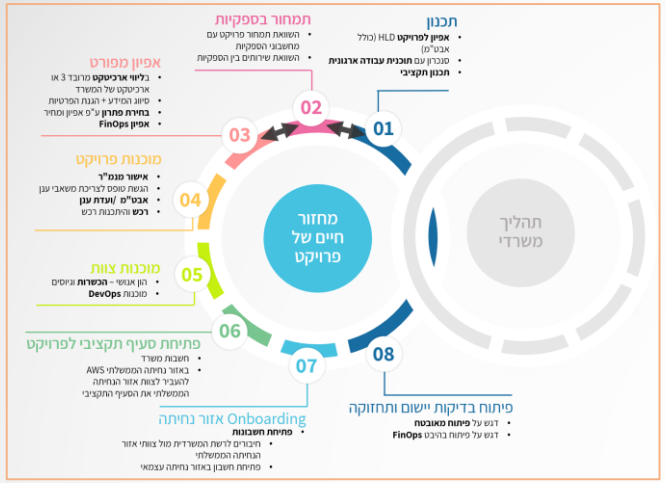
CCoE - מסמך מסע משרדי לענן

סטטוס הפעילות: הכתיבה הסתיימה
בתהליך אישורים לפני פרסום

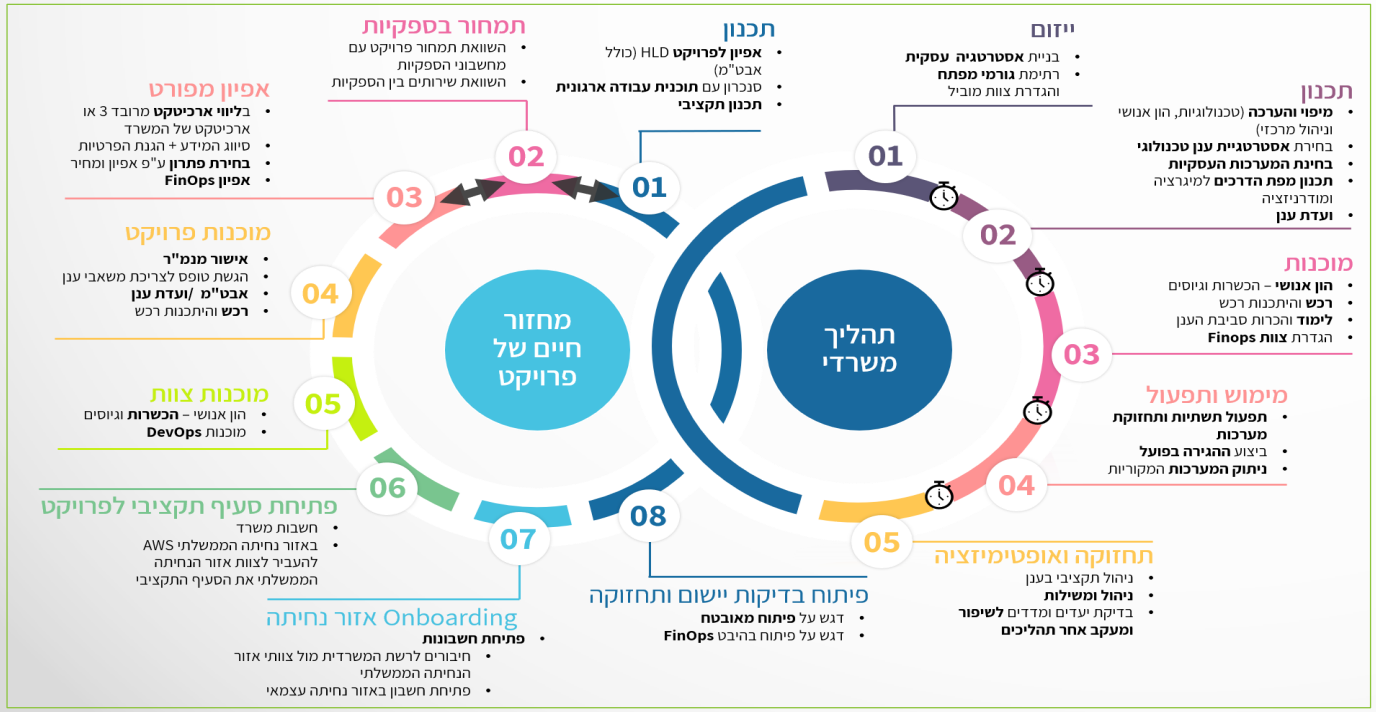
נכתבו שני מסמכים:

- מסע לענן בהיבט המשרדי
- מסע לענן בהיבט הפרויקטלי

נכתב כלי סיוע במבנה Checklist







תוצר של חשיבה בקהילה

CCoE - ליווי משרדים

סטטוס הפעילות:

- ירון אמיר, ליווי פעיל של משרדים
- ויקטור חזנוב, יתחיל פעילות ליווי משרדים
- בתהליך הקמת מתודולוגיית ליווי ובקרה

הדרכת חברות מלוות מרובד 3	שיפורי ארכיטקטורה במיגרציה לענן
ליווי בתמחור מגרציות עם מחשבוני ספקיות	דגשים על פיתוח: תחת מדיניות אבט"מ ממשלתית שיקולי Finops

14 משרדים בתהליך ליווי

תהליך ליווי משרדים מתואם מול אלרן לביא ממערך השירות

CCoE – וובינר ספקים רובד 3

סטטוס הפעילות: תכנון והכנת חומרים



CCoE - ניהול תקציבי

תכנון תהליכי עבודה של ניהול תקציבי

סטטוס הפעילות:

- הקמת דוחות + דשבורדים לסביבת AWS (שלבי סיום)
- הקמת דוחות + דשבורדים לסביבת GCP (שלבי בדיקה)
- קבצי מחירונים בפורמט אקסל לחישוב תעבורת נתונים ורכיבי תקשורת
- בניית מסמכי FinOps Best Practice

	Legend		Cost per month	Cost per GB	
	IGW	Internet Gateway	$0.000	$0.090	
	TGW	Transit Gateway	$74.400	$0.020	
	TGW	Transit Gateway attachment	$37.200	$0.000	
		Endpoints / Private link	$8.333	$0.010	
	ALB	Application Load Balancer	$18.749	$0.030	~LCU
	NLB	Network Load balancer	$18.749	$0.025	~LCU
	Nat-GW	Network Address Translation (NAT) Gateway	$35.712	$0.045	
	DTO	Data Transfer Out	$0.000	$0.090	
		Gateway endpoint (s3, dynmoDB)	$0.000	$0.000	
	FW	WAF AWS	$5.000		
	FW	FW (checkpoint)			
	DX AWS	AWS Direct connect (1GB)	$223.200	$0.100	
	DX AWS	AWS Direct connect (10GB)	$1,674.000	$0.100	
		VPC Peering Connection (same AZ)	$0.000	$0.000	
		VPC Peering Connection (other AZ)	$0.000	$0.020	
	AZ	az1 to az1	$0.000	$0.000	
	AZ	az1 to az2	$0.000	$0.020	
	API GW	api gateway for internet facing	$0.000	$1.000	per million

CCoE - מאגר שיתוף קוד ממשלתי

סטטוס הפעילות: בתהליך ניתוח מצב קיים והגדרת הדרישות העסקיות

הפתרון יתייחס לקודים מסוגים שונים שיש צורך לשתף בין משרדי הממשלה, כגון:



קוד פתוח שאושר לשימוש ממשלתי



קוד שפותח על ידי גוף ממשלתי שמיועד לשיתוף



Images



IAC - Infrastructure as Code



מדיניות כקוד (policy code files)

תיעדוף להקמה על בסיס מוצרים קיימים ברובד 1 (או רובד 5)

CCoE - פורטל ידע אתר Cloud Me In

סטטוס הפעילות: פורטל קיים, הרחבת יכולות והנגשת מידע



אזור נחיתה
ממשלתי



פרסום טפסים ומסמכים
מאחורי כרטיס חכם

סטטוס הפעילות: **בפיתוח**



מסמכים הנחיות

הרחבת התוכן למידע נגיש באתר
(בנוסף לאפשרות של הורדת מסמכי המדיניות כ pdf)

סטטוס הפעילות: **בפיתוח**

CCoE - תוכנית הכשרות ענן ממשלתית



AWS



GCP

תובנות משנת 2022

- עדיפות ללמידה בעברית
- השקת פורטל וקורסים נוספים של AWS (מתבצעת בחינה של AWS לקורסים וירטואליים)
- לשים לב לעמידה בהתחייבות ברישום (בקורסים וירטואליים)

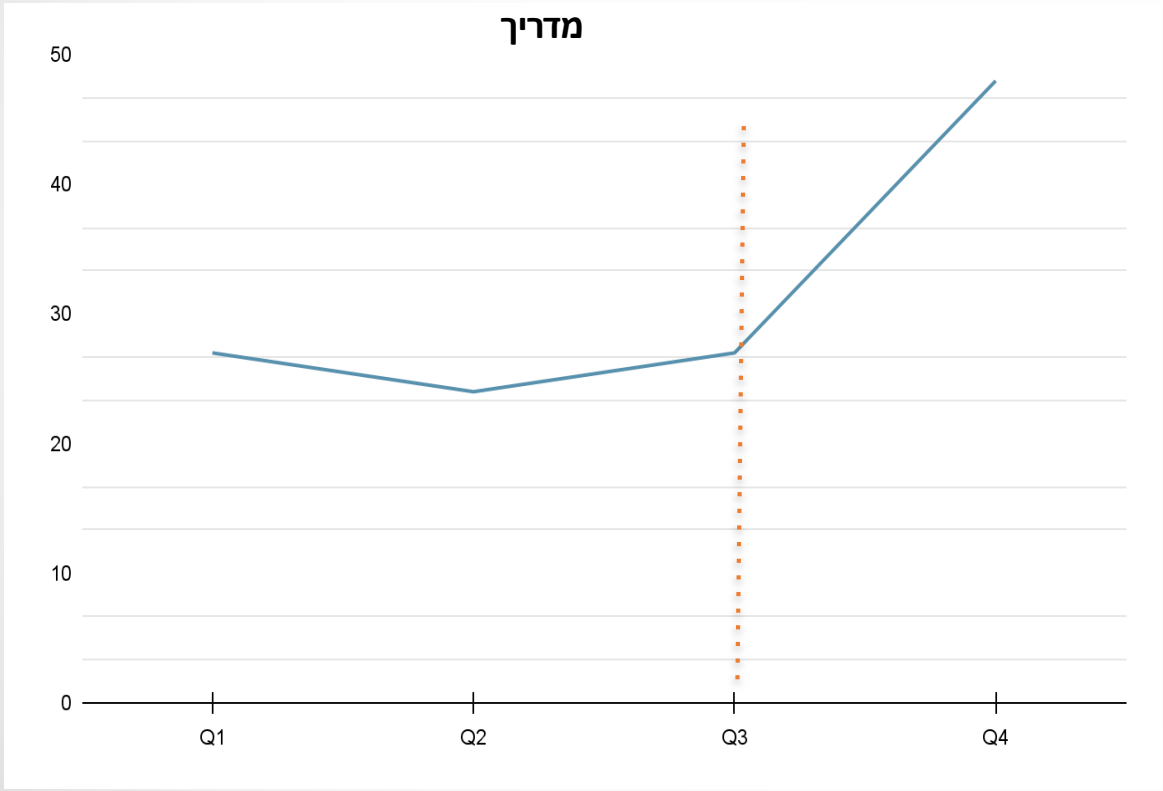
ILTs and On-Demand Activities by Q, 2022

Proprietary + Confidential

47% Growth in ILTs during H2.

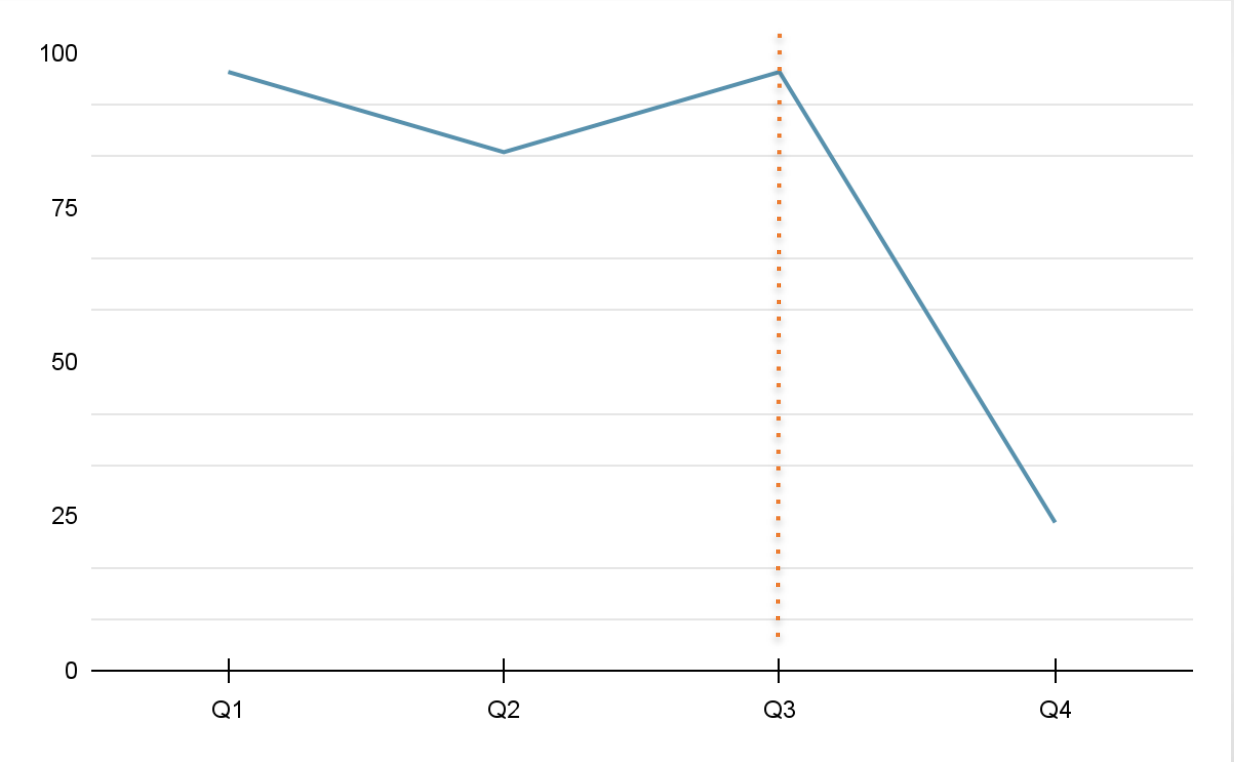
ILTs Sessions

קורס וירטואלי בביתה מונחית מדריך



On-Demand New Learners

קורס דיגיטילי



Google

CCoE - בחינת הסמכות

סטטוס הפעילות: בתוכנית עבודה - טרם החל



AWS

- AWS Certified Solutions Architect Associate
- AWS Certified Solutions Architect Professional
- AWS Certified Security – Specialty
- AWS Certified Advanced Networking
- etc.



GCP

- GCP Professional Cloud Architect
- GCP Associate Cloud Engineer
- GCP Professional Cloud Security Engineer
- GCP Professional Cloud Network Engineer
- etc

תכנון מפגשי הקהילה הקרובים



קהל יעד: ארכיטקטים

- אזור הנחיתה בממשלה
- מדיניות SCP
- דיון והצגת ארכיטקטורה AWS ו-GCP

קהל יעד: מובילי ענן משרדי ארכיטקטים

מאי 2023

- תכנון משרדי למיגרציה

קהל יעד: מובילי ענן משרדי

20 מרץ 2023
מתארחים ברשות המסים

- מודל ההפעלה פן תהליכים וניהול השינוי
- תפקידים חדשים
- תחומים חדשים (Finops/Devops)

- מסע משרדי לענן
- במודל ההפעלה בענן הפן הטכנולוגי
- סיפור ההגירה לענן של הלשכה המרכזית לסטטיסטיקה – ממשלת קנדה

ניימבוס
Cloud Me In

תכנון עבודת הקבוצות

סטטוס הפעילות: נבחרו הנושאים לקבוצות העבודה ובוצעה חלוקה לקבוצות. **מפגשים ראשונים יתקיימו אחרי פסח.**



בנייה ותכנון
ארכיטקטורה
High Level Design

מוביל קבוצה: ויקטור חזנוב

תוצר סופי:
דיאגרמות רשת ודיאגרמות זרימת המידע
מותאמות לכל ספק ענן
תבנית של אזור משרדי באזור הנחיתה,
תבנית של מבנה פרויקט/אפליקציה, סביבות עבודה NON-PROD/PROD ודרכי התקשורת ביניהם



השוואת שירותים ופתרונות בין הספקיות (בסיסי נתונים /אחסון /API)

מוביל קבוצה: ירון אמיר

תוצר סופי:
טבלה שתכיל את ההשוואה בין הספקיות בהתאם לשירותים



CI/CD בענן + SDLC
(אימוץ סטנדרטים לפיתוח נכון בענן)

מוביל קבוצה: ויקטור חזנוב

תוצר סופי:
TEMPLATE DIAGRAM
נכין תבניות של pipeline בהתאם ל best practice
לדוגמא לאפליקציית web/תהליכי ETL

מפגש פתיחה אחרי פסח

מספר פגישות מתוכנן:
מספר המפגשים יקבע בפגישה הראשונה ולאחר סקירה ותיאום צפיות של צוות העבודה

מועד סיום עבודת הקבוצות
אוקטובר 2023

תוצרים:
התוצרים של קבוצות העבודה יהיו לשימוש המשרדים בתהליך מעבר לענן

הצגה התוצרים:
התוצרים יוצגו בפגישות הקהילה בנובמבר \ דצמבר

אזור נחיתה ממשלתי - נתוני חיבור משרדים

GCP

- **12 משרדים מחוברים** – שיכון, מערך הדיגיטל, הגנ"ס , מנהל התכנון, רשות שוק ההון, בטחון פנים , חינוך, כבאות והצלה, מכס, רשות התחרות, מס"ל הנהלת בתי המשפט,
- **3 משרדים מתוכננים** – הנהלת בתי המשפט, המשרד לשוויון חברתי, רמ"י

AWS

- **12 משרדים מחוברים** – הבינוי ושיכון, הנהלת בתי המשפט, רשות האוכלוסין, מנהל התכנון, אכיפה וגביה, מערך הדיגיטל, מפ"י, רמ"י, משרד הרווחה, נציבות שירות המדינה, למ"ס, כלכלה
- **3 משרדים מתוכננים** – משרד הפנים, חינוך, תיירות

אזור נחיתה ממשלתי

יכולת חשיפה לאינטרנט

פתרונות קיימים בשני ספקיות הענן על בסיס יכולות

IOT

קיימת הנחיה מאושרת על ידי יה"ב

SCP

קיים מסמך המתאר את ה scp של שתי הספקיות, נבחנת הרחבה בעתיד

ITSM

כתיבת מכרז לרכש והטמעת המוצר באזור הנחיתה הממשלתי

IDP

ממתינים לפרסום מכרז רכש והטמעת הפתרון בקרוב

מודל ההפעלה בענן פן תהליכים ושינוי ארגוני

קרן בר-לב
CTO ממשלתי
מנהלת ה CCoE

מסמכי מדיניות

מדיניות כוללת את שיטות **העבודה המומלצות** (Best Practices)
וחיבורן לאסטרטגיה הממשלתית למעבר לענן



השפעת המעבר לענן על יישום מערכות



- סקר שוק, מגמות טכנולוגיות, חלופות
- צורך עסקי

- הגדרת דרישות
- בחירת מוצר ותעדוף
- FinOps
- זמינות ושרידות
- ארכיטקטורה ארגונית

- Agile (MVP/SDLC)
- ניהול תשתיות קוד IAC
- ניהול תצורה

- DevOps
- CI\CD

- Unit testing
- אוטומציות

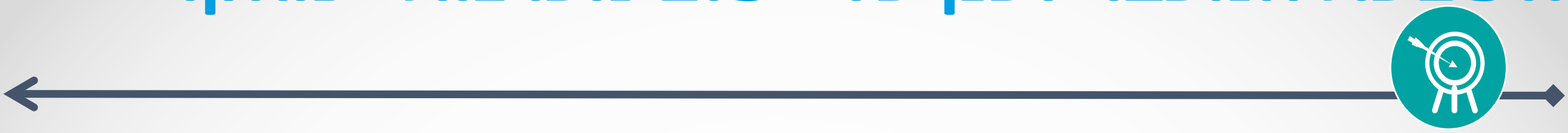
- ניהול גרסאות מוצר
- הקמת סביבות באמצעות קוד IAC
- Secure By Design
- ניהול קונפיגורציה

- ניהול ובחינת עלויות FinOps

- ניהול ספקי השירות AWS & GCP

- FinOps
- ניהול שינוי ארגוני
- ממשל, סיכונים ותאימות

השפעת המעבר לענן על יישום מערכות - מחקר



סקר שוק, מגמות טכנולוגיות, חלופות

במעבר לענן הופכים לצרכנים של שירותי שוק חיצוניים (SaaS). במודל זה, היכולת לעקוב אחר מגמות השוק ולהבין (או להשפיע) על מפות הדרכים של הספקים היא קריטית.

הכרת תרחישי שימוש ויישומם בענן בארגונים אחרים.

הצורך עסקי

אימוץ שירותי ענן מקושר עם מעבר למודל חיוב מבוסס צריכה, שבו השירותים מתומחרים לפי משתמש, עסקה או קיבולת מנוצלת. שימוש בשירותים אלו בצורה חסכונית יותר מאשר ב- On Premise, מחייב את הארגון להקים פונקציה חזקה לצורך הבנה, צבירה, חיזוי והשפעה על הביקוש לשירותי ענן.

יש לבחון את הצורך העסקי אל מול מודל התשלום של פתרונות זמינים.

מי מושפע?

- מנהל פרויקט
- ארכיטקט ענן
- מנתח מערכות

השפעת המעבר לענן על יישום מערכות - תכנון

FinOps

שיפור מיומנויות חדשות ספציפיות לענן כדי להבטיח שהבחירות הנכונות לענן, העקרונות והעיצוב הכולל של המערכת יותאמו לצריכת המשתמשים **ולחישוב עלויות המתוכננות למערכת.**

מי מושפע?

- מנהל פרויקט
- ארכיטקט ענן
- ארכיטקט יישומי
- מנתח מערכות
- Cloud DBA
- FINOPS

ארכיטקטורה ארגונית

ארכיטקטורה תצטרך להיות מתוכננת בהתאם לעקרון ' Cloud First' ובחינת הפתרון בהתאם לארכיטקטורה ארגונית – היכן נמצא המידע המשרדי, **ממשקים למערכות ארגוניות** אחרות, ממשקים למידע מארגונים אחרים, **ממשקים היברדיים** וכו'.

זמינות ושרידות

במעבר לענן הציפייה הינה שהמערכות יהיו זמינות ללא הפסקה אם יכולת של הגדלה לפי הצורך (scalabilty). ציפייה זו נכונה אך דורשת תכנון ארכיטקטוני של הפרויקט אשר תומכת בדרישות העסקיות של זמינות ושרידות.

בשלב תכנון המערכות יש לבחון את **משמעות ארכיטקטורת הפרויקט על התקציב ולדרישות העסקיות של זמינות ושרידות** המערכת.

העברת מערכת לענן אינה מבטיחה זמינות ושרידות.

השפעת המעבר לענן על יישום מערכות – פיתוח, אינטגרציה, בדיקות, פריסה בייצור



DevOps

ניהול תשתיות קוד IAC

Secure By Design

Agile

ניהול קונפיגורציה

אוטומציות

מי מושפע?

- מנהל פרויקט
- מפתח / מפתח אוטומציה
- ארכיטקט ענן/ארכיטקט יישומי
- אבט"מ
- בודק תוכנה
- DevOps
- FINOPS

השפעת המעבר לענן על יישום מערכות תפעול, מדידה, ניטור, שו"ב



ניהול ובחינת עלויות FinOps תהליך מתמשך

המעבר מניהול CAPEX ל-OPEX מצריך לעתים קרובות שינוי בשיטות המימון והחשבונאות, אך מעל הכל, מצריך שינוי תרבות משמעותי עבור פונקציות הכספים ואגפי הטד"מ.

מי מושפע?
- מנמ"ר
- מנהל רכש משרדי
- ארכיטקט ענן/ארכיטקט יישומי
- מוביל ענן משרדי

ניהול שינוי ארגוני

אימוץ ענן ודרכי עבודה אג'יליות מגדיל את נפח השינוי בתוך הארגון בעיקר אל מול עולם ה- Onprem שעצם טיבו לא הרבה בשינויים.
הקלות היחסית של מעבר מפתרון אחד למשנהו בעולם הענן (שירות מנהול) ואספקה תכופה של תכונות ופונקציות חדשות ידרשו מהעובדים ומבעלי העניין ללמוד ולהסתגל לשינויים יותר מהר מבעבר.
תרבות של הסתגלות לשינויים ארגוניים תכופים יהיה קריטי להצלחת המעבר לענן.

ניהול ספקי ענן

ככל שארגונים הופכים לצרכנים של שירותי ענן, היכולת שלהם להגדיר, למדוד ולנהל את השירותים המדויקים המסופקים על ידי ספקים חיצוניים הופכת חיונית יותר ויותר.
אגף הטד"מ הופך ל"מתווכת שירות Broker-" עבור המשרד ולכן חייבת להיות בעלת יכולת לנהל מספר הולך וגדל של רמות שירות מורכבות יותר ויותר.

השפעת המעבר לענן על יישום התפקידים



כל התפקידים באגף טד"מ יושפעו ממעבר ארגוני לעבודה בענן:

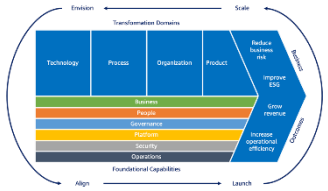
- היכרות סביבת הענן
- היבטי ניהול תקציבי החל משלב תכנון פרויקט
- היבט תקציבי לסביבות פיתוח/בדיקות
- היכרות עם פלטפורמות חדשות כולל LOW CODE
- SECURITY בכל שלבי הפרויקט

עקרונות פיתוח מערכות להיערכות לענן מפיתוח לפרסום - REST API

תפקידים חדשים ייעודיים לענן

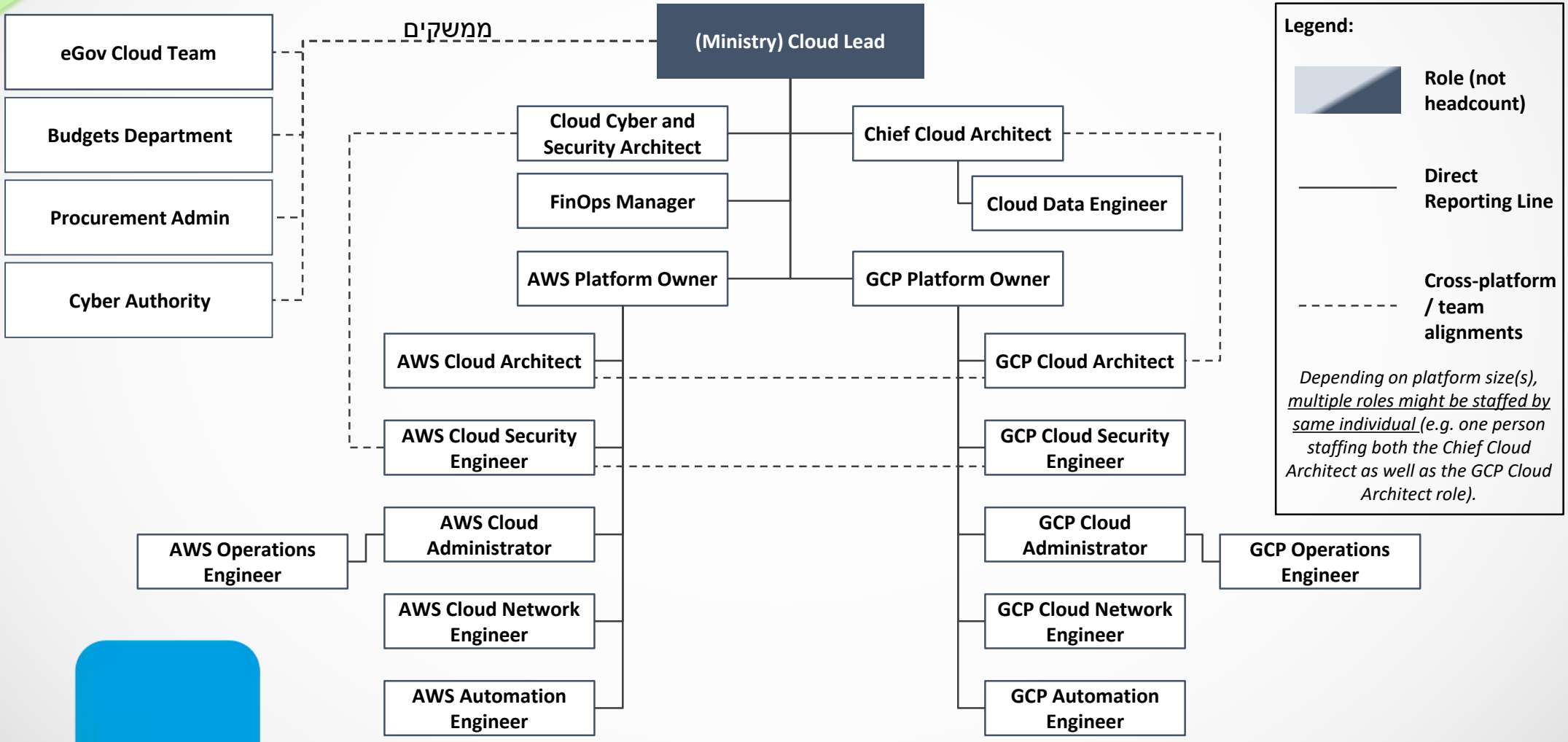
 **Cloud (Chief) Architect**	Plan, Develop	Define Cloud architecture roadmaps, standards and patterns. Also, support agile delivery teams with expertise and technical advice.
 **Cloud Engineer**	Build, Test, Operate	Manage all aspects of solution build and operations, including engineering/configuration, deployment and ongoing support.
 **Platform Owner**	Build, Test, Operate	Manage the setup, coordination and availability of Cloud environments, ensuring that they are available as needed to support changes and business as-usual.
 **Cloud Administrator**	Operate	Manage Cloud service catalogues and provide overall coordination, integration and brokerage between the organisation's various Cloud services.
 **Cloud Network Engineer**	Operate	Define API standards and manage the API catalogue and publishing processes.
 **FinOps Manager**	Manage, Govern	Define and manage processes and tools optimise the financial aspects of Cloud management. This includes the definition of cost analytics and allocation models.
 **DevOps**	Build, Test, Operate	

תרבות ארגון לומד ענן

	aws	
CSP Cloud Adoption Framework	 **AWS Cloud Adoption Framework**	 **Google Cloud Adoption Framework**
Further CSP Cloud Adoption Guidance	AWS whitepaper **“Accelerating cloud adoption through culture, change, and leadership”**	Google whitepaper **“Managing change in the cloud”**
	AWS whitepaper **“An Overview of the AWS Cloud Adoption Framework”**	Google tool **“Cloud Maturity Assessment”**
CSP Cloud Certifications	• AWS Certified Solutions Architect Associate • AWS Certified Solutions Architect Professional • AWS Certified Security – Specialty • AWS Certified Advanced Networking • etc.	• GCP Professional Cloud Architect • GCP Associate Cloud Engineer • GCP Professional Cloud Security Engineer • GCP Professional Cloud Network Engineer • etc.

מבנה ארגוני ליחידת ענן משרדי

One Size does not fit all



הקמת צוות מוביל ענן



מתפקידי הצוות (רשימה חלקית)

- הבנה ותפיסה אחודה לגבי המטרות העסקיות ויעדי פרויקט הענן
- תמיכה והובלת השינוי הארגוני
- תקשור חזון ויעדי הפרויקט
- הנחיות ביצוע לצוותים המקצועיים (בהתאם למתודולוגיית מסע לענן)
- הטמעת תפיסת Cloud Ready למערכות חדשות בפיתוח
- הטמעת תפיסת Cloud First

פרויקט נימבוס –השפעה על אגפי טד"מ



Business Led IT



Shadow IT



Low Code/
No Code

Business Led IT

אגף טד"מ כגוף בעל הידע הרחב בענן משמש כ- Enabler משרדי לפתרונות הענן

המעבר לענן מביא איתו הזדמנות לשינוי בהיבט העסקי ובחדשנות פתרונות העסקיים.
תמיכה בשינוי זה על ידי אגפי טד"מ הינה קריטית להובלת השינוי.



Innovation with Regulation

הודעה מס' 16.2.2 – https://takam.mof.gov.il/document/HM.16.2.2. בנספח ג'

Business Led IT

Integrate ‘Shadow IT’ and Business-Led IT Into the I&T Operating Model to Enable Enterprise Agility

Key Challenges

- Distributed and “shadow IT” can create a perfect storm of architectural and organizational complexity and isolated islands of capability and data, impeding the enterprise’s digital ambitions.
- Without the IT organization fulfilling a stewardship and orchestration role, the enterprise’s highly distributed information and technology assets and capabilities will introduce significant inefficiency and risk.
- There is cognitive dissonance between the executive team’s desire to have a single point of accountability for all IT-related things while also supporting highly distributed I&T-related decision rights or turning a blind eye to the bypassing of governance mechanisms and policy.

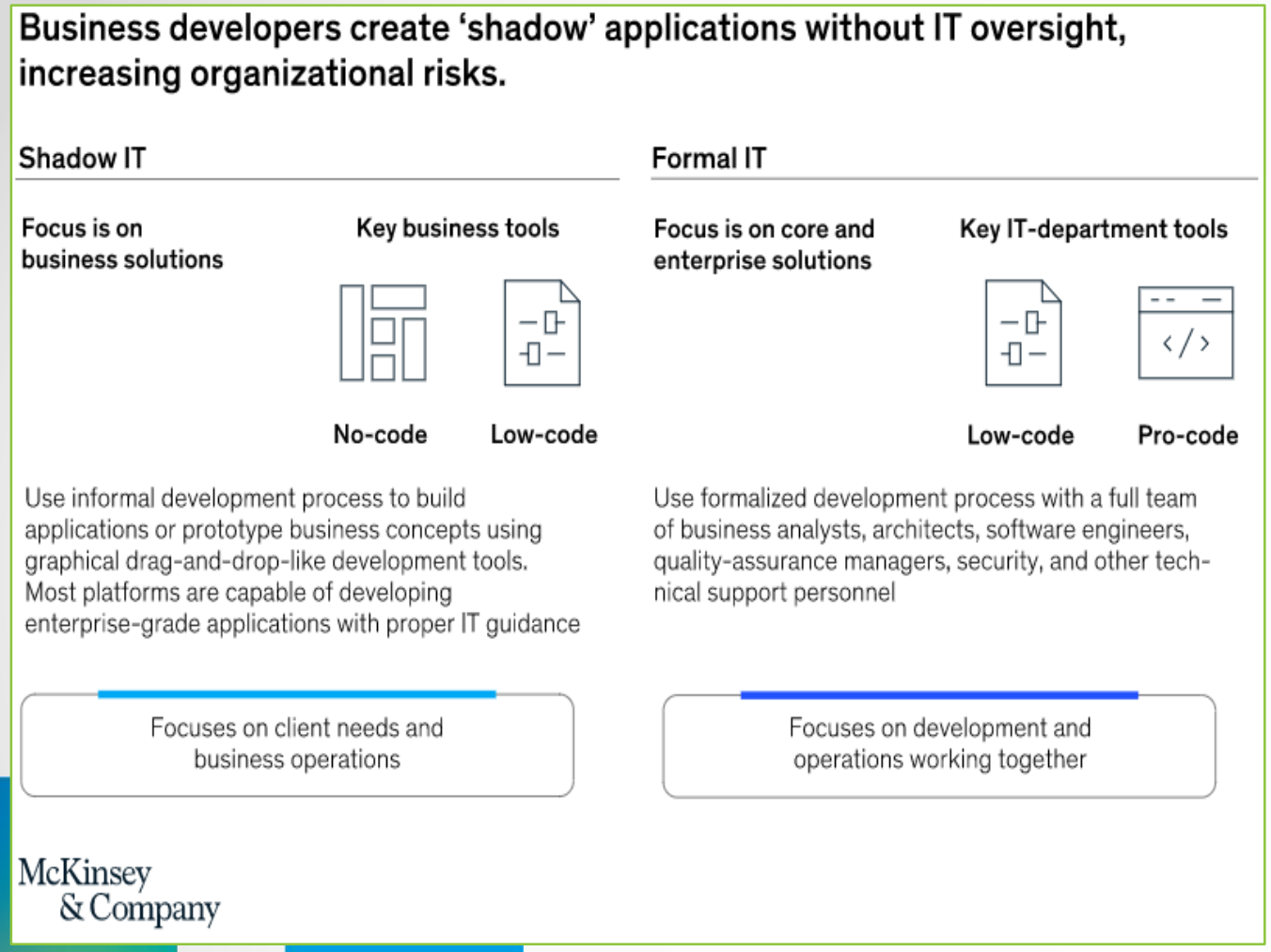
Recommendations

To incorporate business-led IT and “shadow IT” into the I&T operating model, CIOs must:

- Adopt differentiated approaches to stewarding and managing business-led and “shadow IT” by identifying the different kinds and their varying needs and risks.
- Redefine ownership and accountability of business-led IT-developed and -acquired solutions by engaging with the executive team.
- Define a set of I&T operating model design principles that guides the integration of business-led IT into the I&T operating model by addressing the issues of owner accountability, transparency, governance controls and quality.
- Define boundaries to “shadow IT” by using mission criticality and complexity as criteria.
- Identify opportunities for alignment and convergence between the I&T operating models of the different stakeholder groups by using Gartner’s I&T operating model framework.
- Create a set of services relevant to IT’s role as steward and in supporting business-led IT.

https://www.gartner.com/doc/3957146=lavfer&ydobhtua=fer?3886073

Shadow IT

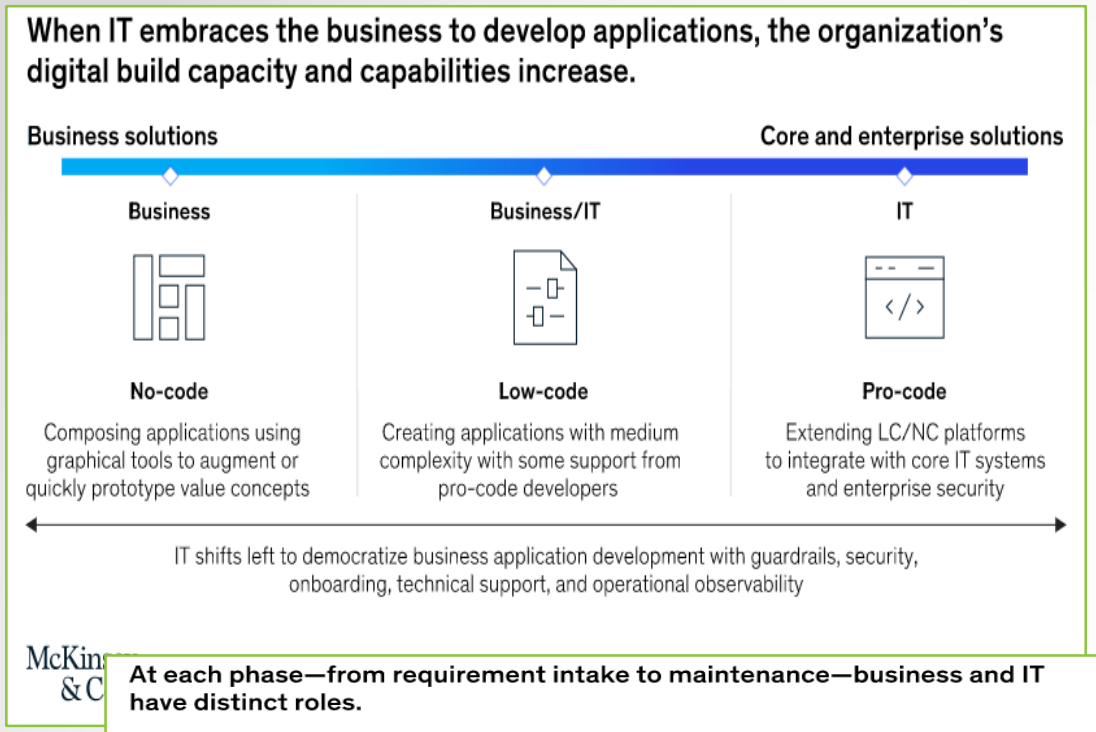


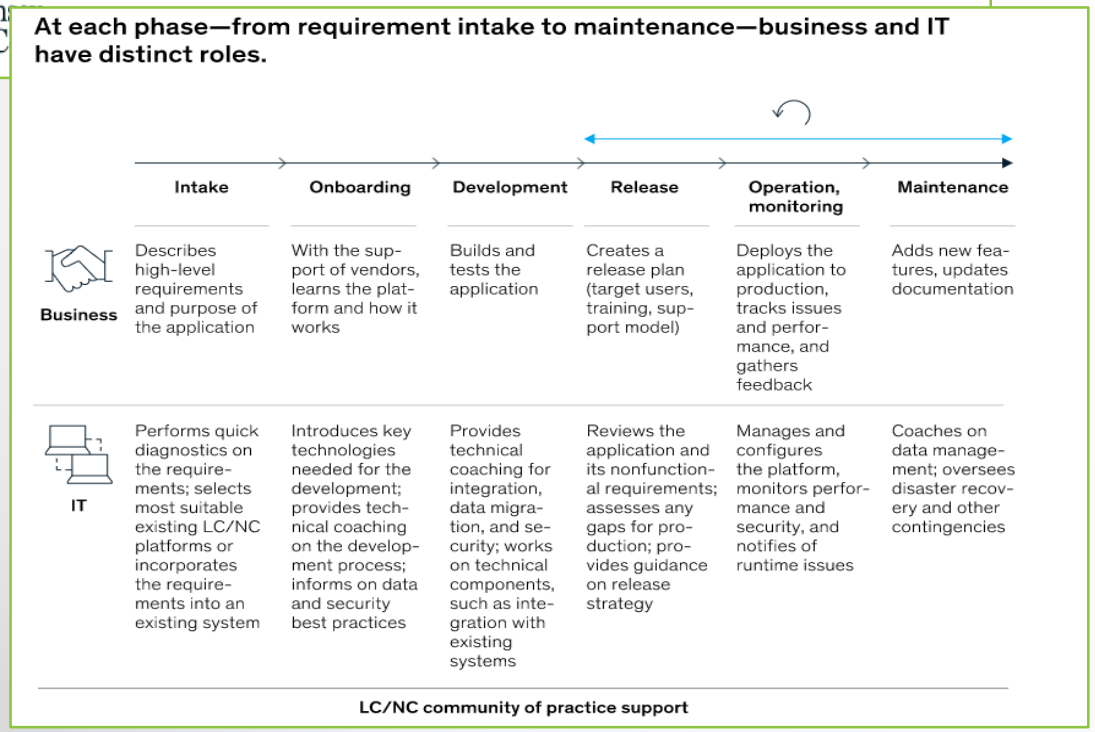
- פתרונות ניהול המידע/מערכות ללא שיתוף אגף הטד"מ
- מהווה **סיכון רציני בשל חוסר ניהול של המידע**, מחסור ב-"אמת אחת", קושי בהמשכיות עסקית, מידע שנשמר במקומות מקומיים ולא מנוהלים ועוד
- המסע מתחיל בביצוע מלאי של "יישומי צל" ולאחר מכן בחירת פלטפורמות LowCode/NoCode שמתאימות לצרכים שאפליקציות הצללים ממלאות
- בשלב הבא, אגף טד"מ יספק למפתחים עסקיים מסלולים למינוף הפלטפורמות החדשות
- מודל תפעול מקצה לקצה כדי להפחית סיכונים, לשמור על זריזות ולהגביר את היכולות הדיגיטליות של הארגון

לנצל את המעבר לענן להסדרת פתרונות לא מנוהלים

Shadow IT

- בתפיסה זו אגף טד"מ של ארגון מרחיבה את הידע בפיתוח תוכנה ל"צד הצל" על ידי אספקת פלטפורמות NoCode/LowCode מקצועיות ואימוץ מפתחים עסקיים.
- לאגף טד"מ יש תפקיד משמעותי בבניית אקו-סיסטם הארגוני ומרחיב את התכולה לפתרונות שנוהלו באופן עצמאי על ידי יחידות עסקיות.





https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/low-code-no-code-a-way-to-transform-shadow-it-into-a-next-gen-technology-asset

Low Code

Gartner predicts that by 2026, developers outside formal IT departments will account for at least 80% of the user base for low-code development tools, up from 60% in 2021.

היכולות לפתח יישום שלם

- תמיכה בפיתוח אפליקציות המורכבות ממשקי משתמש
- לוגיקה עסקית
- זרימת עבודה ושירותי נתונים (work flow)
- בדיקה
- פריסה וניהול פשוטים של יישומים

- פיתוח יישומים מהיר הוא קל מכיוון שדרישות הקוד הנמוכות מאפשרות להפעיל מערכת אלו כמעט באופן מיידי ללא צורך בהתמחות או ניסיון בתכנות , היכרות בשפת תוכנה מסוימת.
- סביבת העבודה של מוצרים אלו פותחו במטרה להיות קלים וזמינים לשימוש

Low code is the evolution of Rapid Application Development to cloud and SaaS models.

שלושה נושאים במיקוד - סיכום



Business Led IT

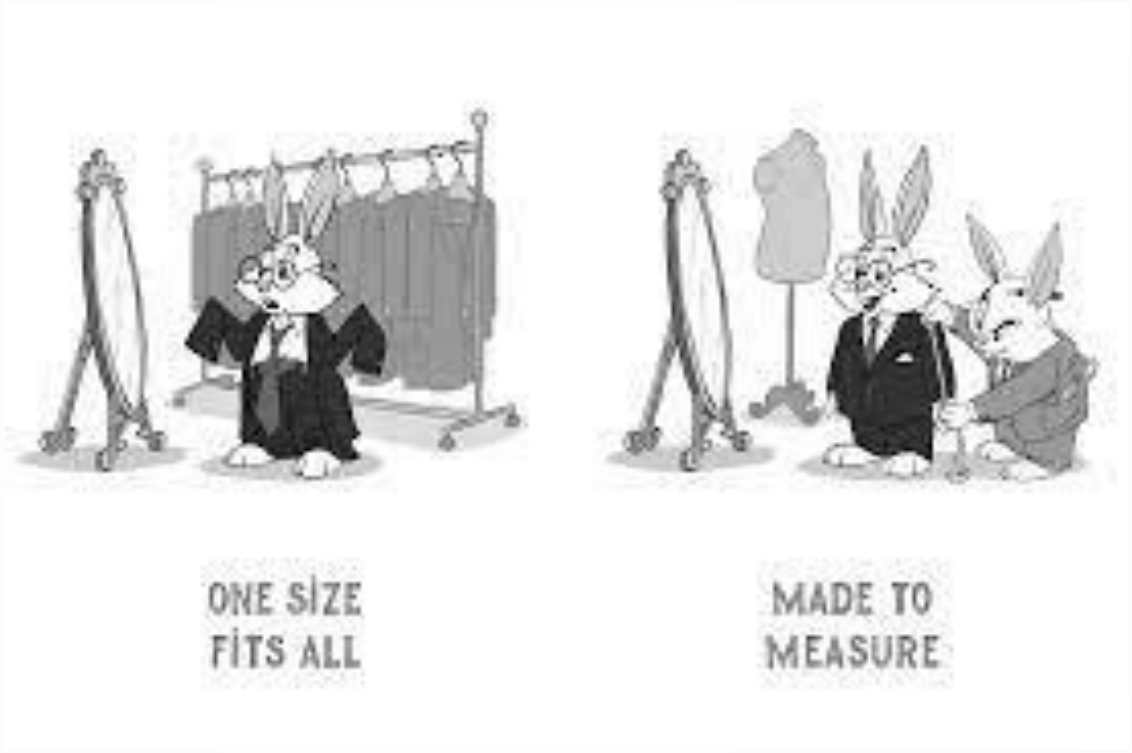


Shadow IT



Low Code/
No Code

אין פתרון בית ספר



יתפרסמו הנחיות ומסמכים המכוונים ל Best Practices נושאים אלו

משרד משתף

נדב שרייבמן

FinOps – תוכנית מערך הדיגיטל למעבר לענן



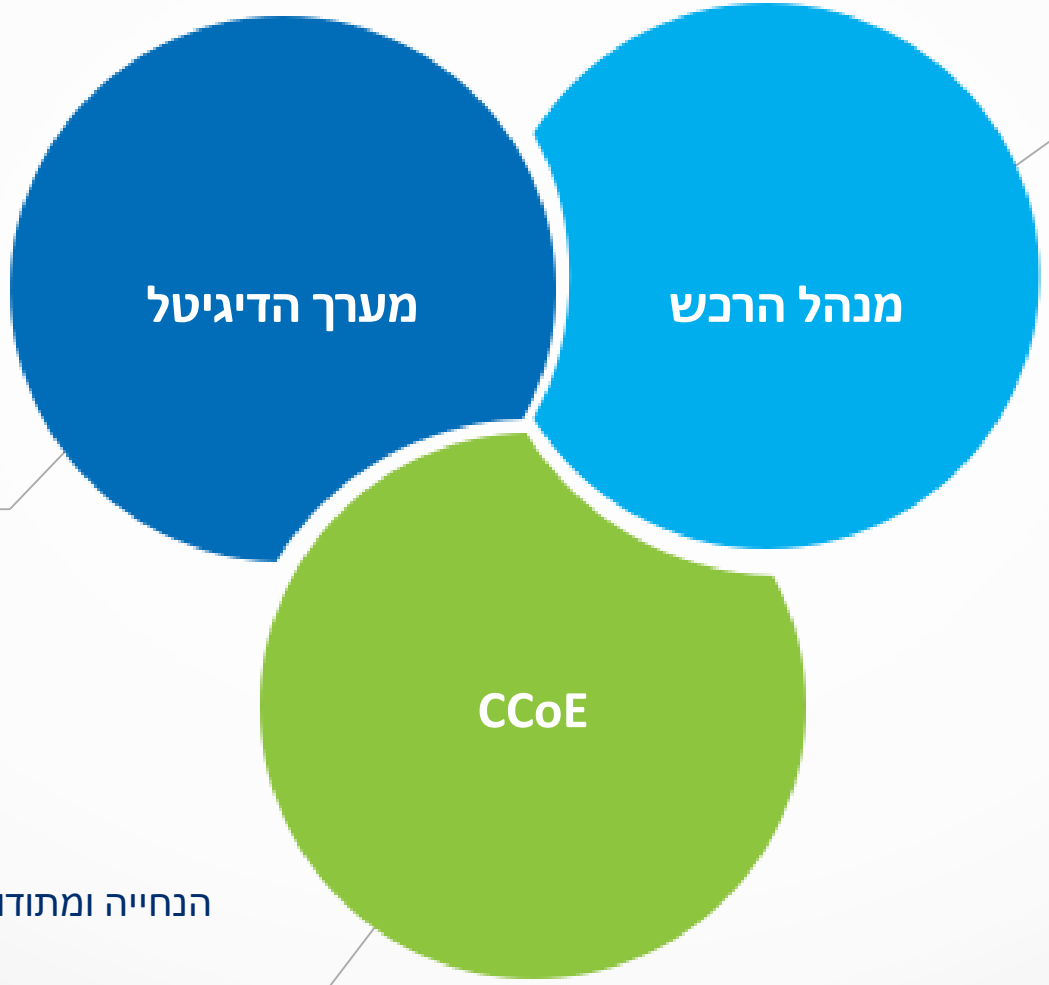
מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

מצב קיים

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

גופים מעורבים

מנהל מכרז נימבוס



הנחייה ומתודולוגיה, מנהל את ה-LZ המרכזי

הנחייה ומתודולוגיה

שלב 1 - התארגנות: רמת המשרד

הגדרה ואיוש תפקידים (צוות ניהול תקציבי לעולמות הענן)



הגדרת תהליכי עבודה ותוכנית עבודה



הכשרות וידע



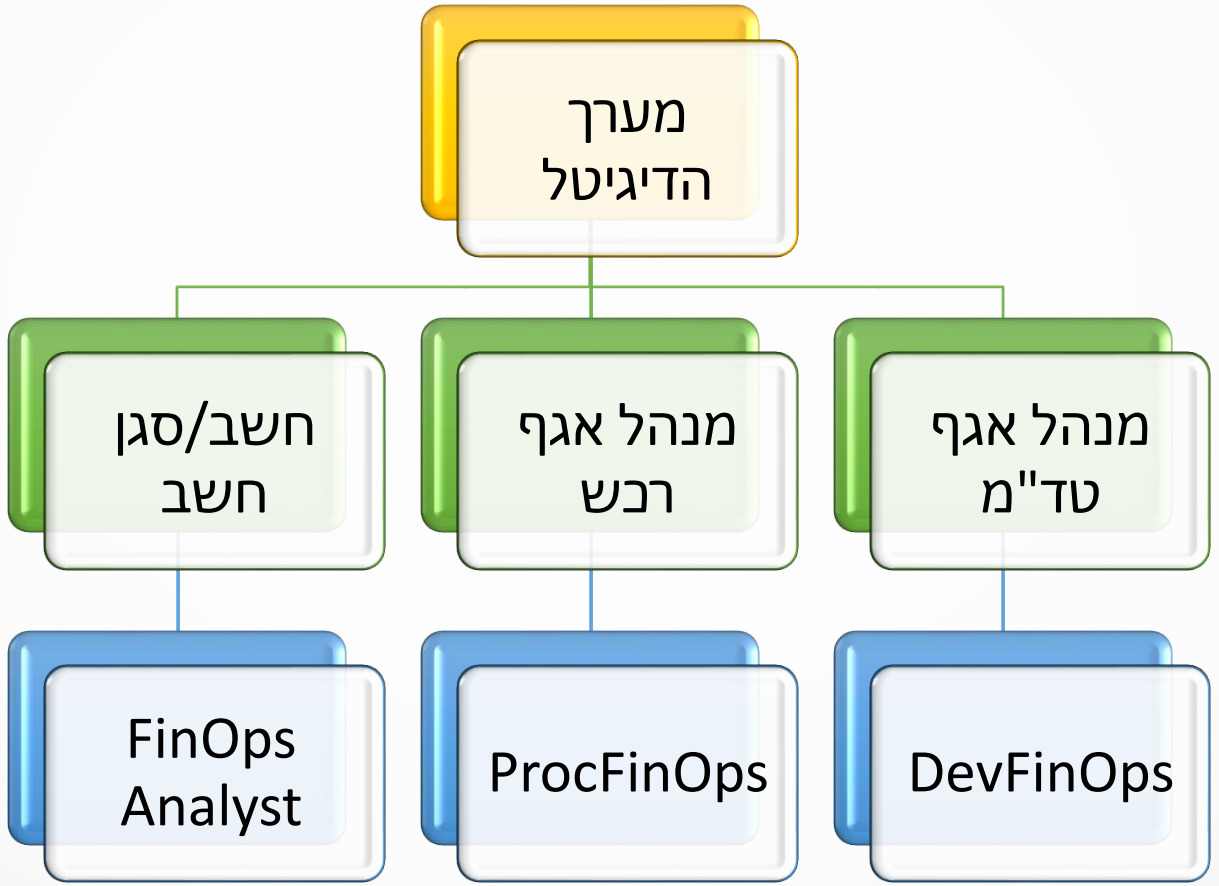
הזמנה ותקציב



סיוע ומרכז ידע

מבנה צוות פינאופס

FinOps Analyst.5.5.4 , ה- ProcFinOps וה- DevFinOps צוות ה-FinOps הם תפקידי הליבה של תהליך הניהול הכלכלי בענן בארגון והם אלו שאמורים להביא למימוש התהליך בפועל ולרתום את הצוותים בארגון.



כלת ענן - מדיניות והסדרת תהליכי עבודה – נוסח להפצה

איוש צוות פינאופס במערך הדיגיטל

Egov - מערך השירותים הדיגטליים

- ProcFinops, Analyst FinOps – נדב שרייבמן (מטה –רכש)
- ProcFinops (הזמנות, מרכבה) דקלה טובול (מטה –רכש)
- DevFinops – לא מאויש

LandingZone

- ProcFinops– רונית תורג'מן (אזור נחיתה)
- DevFinops – לא מאויש

CCoE

- ProcFinops– לא מאויש
- DevFinops – ירון אמיר (חלקית)

תהליכי עבודה ותכנית הכשרות – צוות פינאופס במערך הדיגיטל (רמת "המשרד"

- הגדרת נוהל עבודה והגירה ותפעול בענן לפי תפקידים על בסיס מסמכי החובה
  - ProcFinops, Analyst FinOps
  - מנהל מוצר
  - ארכיטקטים
  - צוותי פיתוח

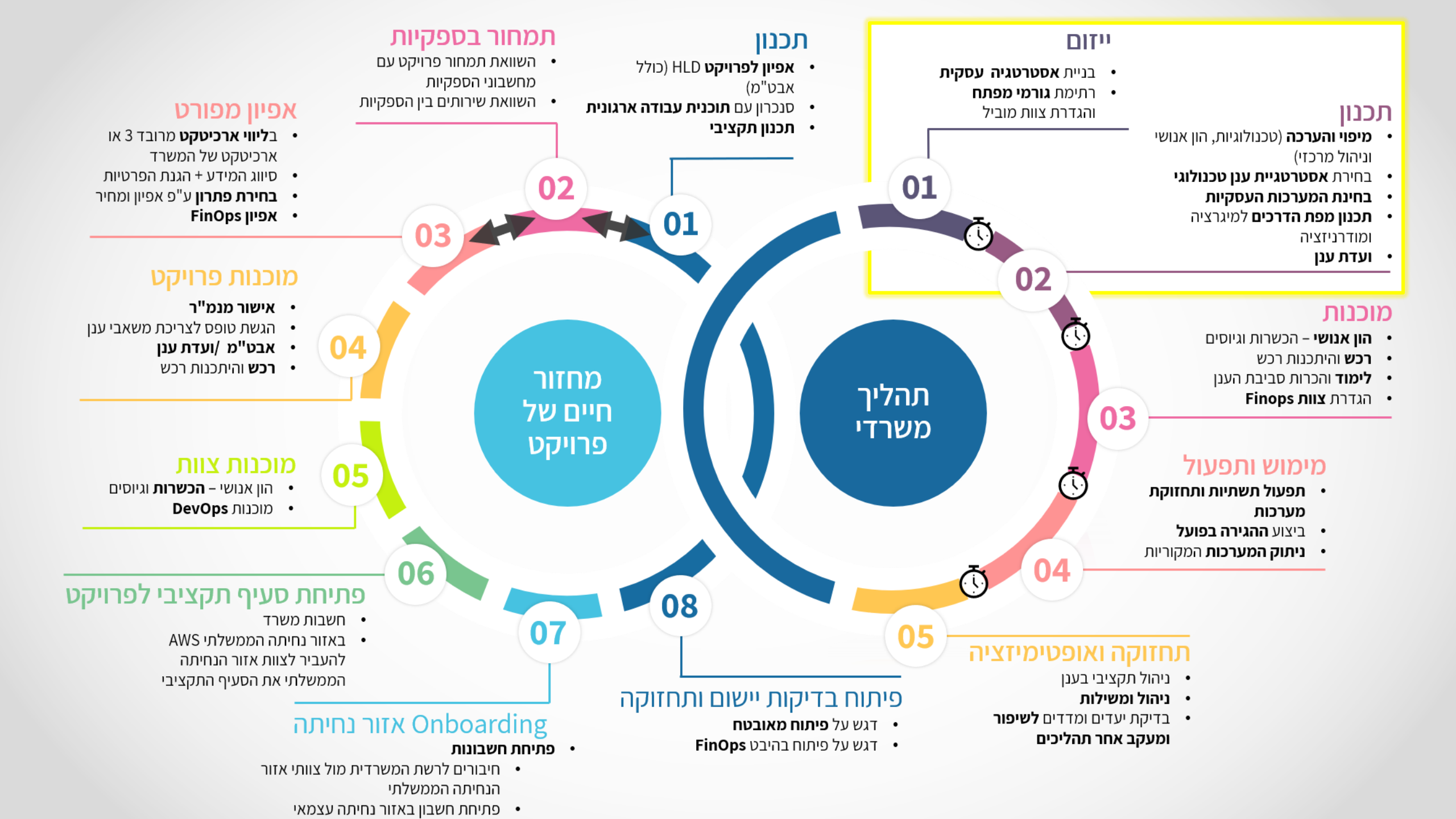
- הגדרת תכנית הכשרות לפי תפקידים בשיתוף הספקים הזוכים
  - קורסים לפי רמות ידע
  - ימי עיון והעשרה

מסמכים לקריאת חובה !

1. מסמך אסטרטגיה ממשלתית
2. מודל ההפעלה הממשלתי בענן – פן טכנולוגי
3. אתר נימבוס – Cloud Me In
4. היערכות משרדית למיגרציה בענן
5. הודעת מכרז מרכזי 16.2.2 – נימבוס – אספת שירותי ענן ציבורי
6. כלכלת ענן – מדיניות והסדרת תהליכי עבודה (טרם הופץ)

"התוכנית" מעבר ותפעול בענן

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

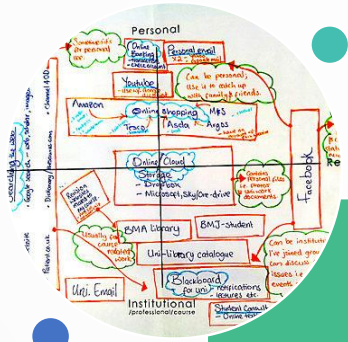

מחזור חיים של פרויקט
תהליך משרדי
01
02
03
04
05
06
07
08
ייזום
בניית אסטרטגיה עסקית
רתימת גורמי מפתח והגדרת צוות מוביל
תכנון
מיפוי והערכה (טכנולוגיות, הון אנושי וניהול מרכזי)
בחירת אסטרטגיית ענן טכנולוגי
בחינת המערכות העסקיות
תכנון מפת הדרכים למיגרציה ומודרניזציה
ועדת ענן
מוכנות
הון אנושי – הכשרות וגיוסים
רכש והיתכנות רכש
לימוד והכרות סביבת הענן
הגדרת צוות Finops
מימוש ותפעול
תפעול תשתיות ותחזוקת מערכות
ביצוע ההגירה בפועל
ניתוק המערכות המקוריות
תחזוקה ואופטימיזציה
ניהול תקציבי בענן
ניהול ומשילות
בדיקת יעדים ומדדים לשיפור ומעקב אחר תהליכים
פיתוח בדיקות יישום ותחזוקה
דגש על פיתוח מאובטח
דגש על פיתוח בהיבט FinOps
Onboarding אזור נחיתה
פתיחת חשבונות
חיבורים לרשת המשרדית מול צוותי אזור הנחיתה הממשלתי
פתיחת חשבון באזור נחיתה עצמאי
פתיחת סעיף תקציבי לפרויקט
חשבות משרד
באזור נחיתה הממשלתי AWS להעביר לצוות אזור הנחיתה הממשלתי את הסעיף התקציבי
מוכנות צוות
הון אנושי – הכשרות וגיוסים
מוכנות DevOps
מוכנות פרויקט
אישור מנמ"ר
הגשת טופס לצריכת משאבי ענן
אבט"מ /ועדת ענן
רכש והיתכנות רכש
אפיון מפורט
בליווי ארכיטקט מרובד 3 או ארכיטקט של המשרד
סיווג המידע + הגנת הפרטיות
בחירת פתרון ע"פ אפיון ומחיר
אפיון FinOps
תמחור בספקיות
השוואת תמחור פרויקט עם מחשבוני הספקיות
השוואת שירותים בין הספקיות
תכנון
אפיון לפרויקט HLD (כולל אבט"מ)
סנכרון עם תוכנית עבודה ארגונית
תכנון תקציבי

אז איך מתחילים?



התארגנות

- גיבוש צוות מטה לתכנית
- הקמת גופי ניהול ומנהלת
- הקמת CCOE משרדי



מיפוי תמונת מודיעין

- מיפוי כל הפעולות שנעשו עד כה
- מיפוי ה- On prem עם כלים של הספקים
- גיבוש תמונה אחת, דיון ותיקוף



הקפאת מצב

- מוצרים
- IT
- סייבר
- אישור חריגים

איך ממשיכים? נערכים להמשך

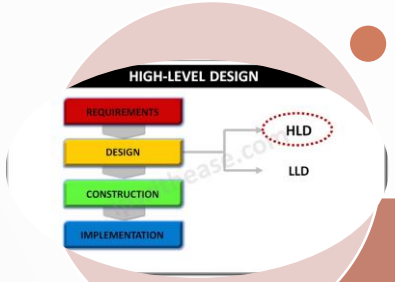


לכל המאוחר סוף Q2/23

תחילת מימוש וישום



1. מיפוי קבוצות יישומים ומוצרים ויחסי גומלין
2. קביעת מדיניות לגבי העברת מוצרים דיגיטליים
3. מיפוי הדרכות, הכשרות והסמכות נדרשות
4. תכנון וקביעת משאבים נדרשים
5. הכנת לוז ותכנית שלדית כולל ציוות גורמים אחראיים



חודשיים

פיצול לשולחנות עבודה לניתוח ובניית תכנית ומשמעויות (HLD)



חודש

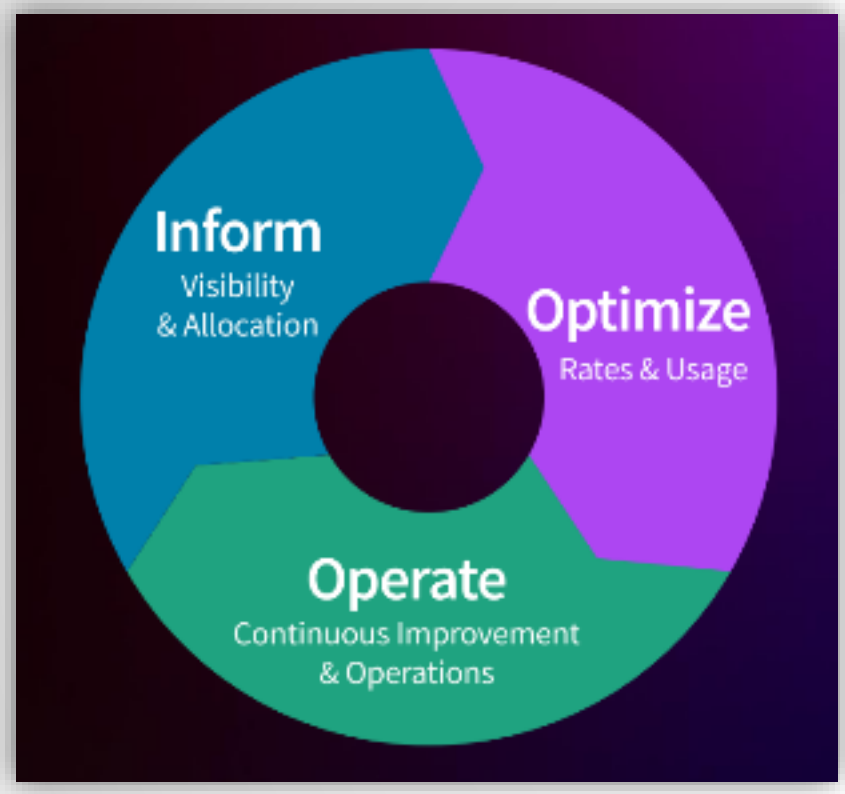
גיבוש תכנית אב

1. תכולת תכנית אב, עקרונות היסוד במעבר לענן:
   - א- Multi Cloud, Single Cloud
   - ב- מדיניות הגירה (6 R's) – קוים מנחים להחלטה
   - ג- קביעת מדיניות הכשרות וכח אדם חיצוני
2. ארכיטקטורת המשרד (עץ חשבונות)
3. מבנה ארגוני – DevSecOpsFin

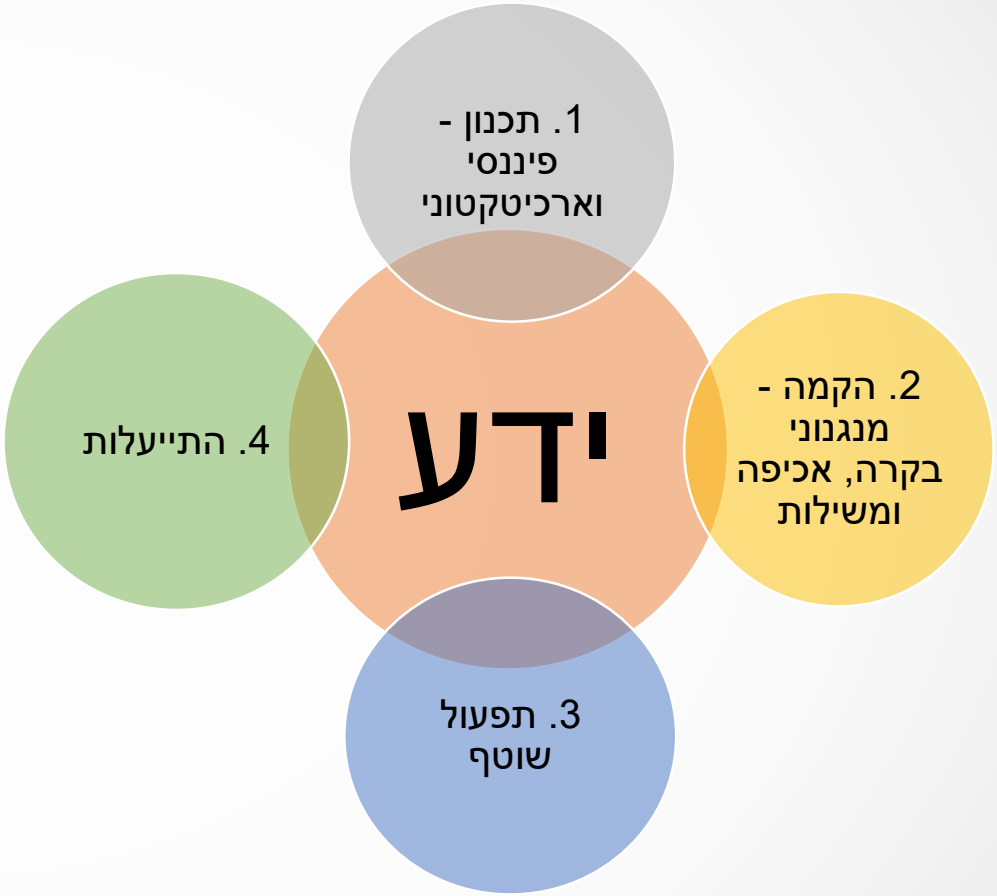
תהליך העבודה

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

תהליך העבודה FinOps רמת המשרד והמוצר





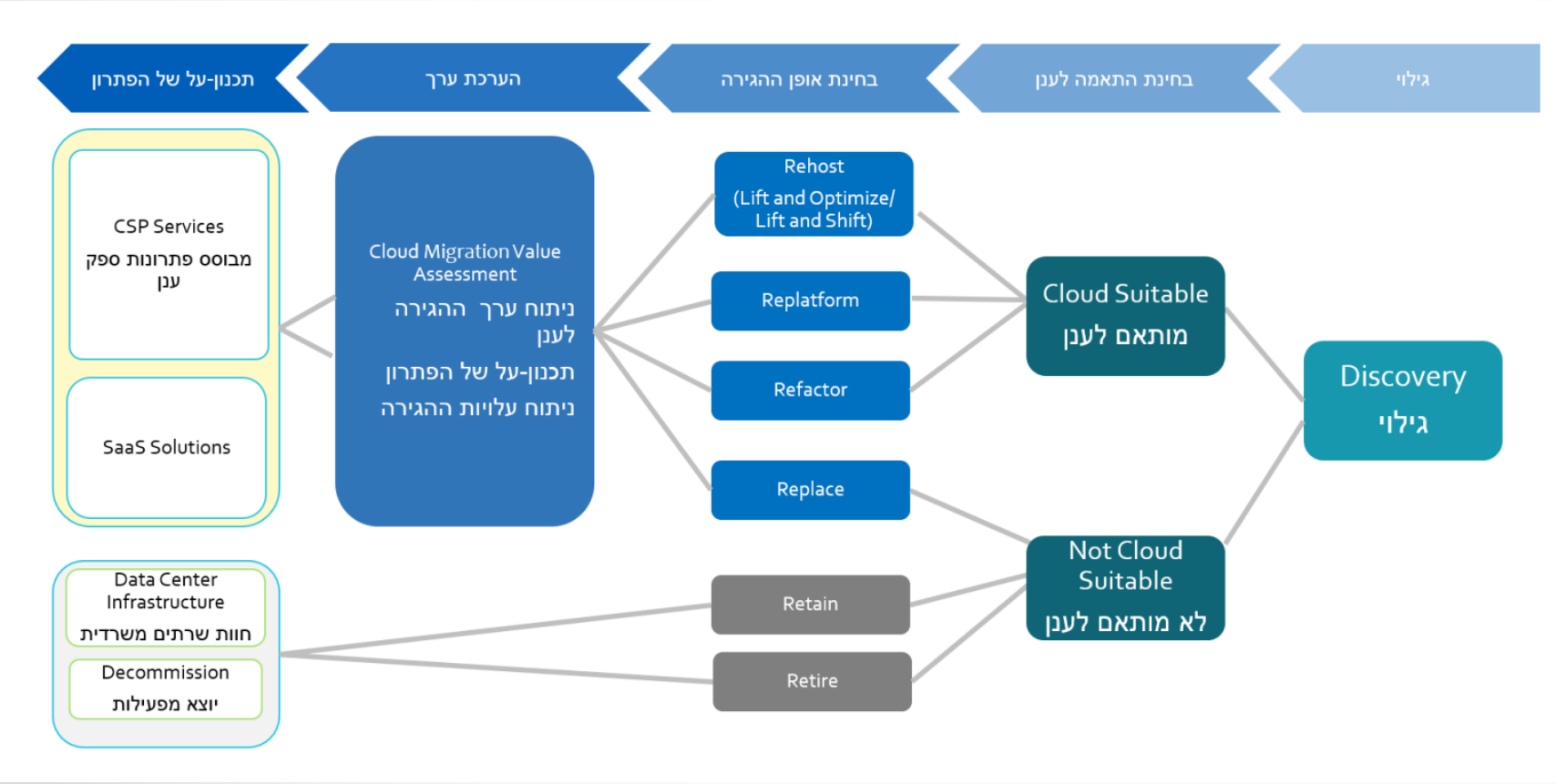


מקור: מסמך כלכלת ענן - מדיניות והסדרת תהליכי עבודה – נוסח להפצה

שלב 1 - תכנון הגירה לענן פיננסי וארכיטקטוני

אחריות: מנהל "התוכנית" רמת משרד/ מנהל מוצר (רמת המוצר/פרויקט)

בקרה: פינאופס



מקור: הנחיית מערך הדיגיטל - היערכות משרדית למיגרציה לענן

שלב 1 – תכנון הגירה לענן ברמת המוצר

מנהל "מוצר" (פרויקט, מחלקה)



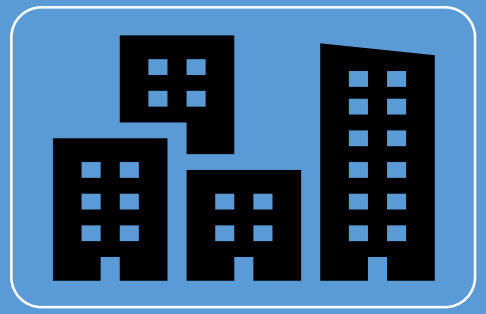
- איפיון וניתוח מצב קיים – הגדרת BaseLine, אופן ההגירה (R's), השוואה בין הספקים ותהליך הבחירה, ניתוח עלויות המיגרציה לענן
- ביצוע תמחיר מוצר ענן בהתאם לארכיטקטורה וקונפיגורציה לכל הסביבות
- הגדרת תהליכי עבודה

ProcFinOps



- בחינת תמחיר
- תקציב והזמנה
- תיוגים ו-KPI's

DevFinOps



- בחינת תכנון ארכיטקטורה

שלב 1 – תכנון הגירה לענן ברמת המוצר

בסיס העבודה תיוגים

הגדרת KPI's טכנולוגיים אופציונליים

- בשירותי מחשוב מבוססי מעבדים בארכיטקטורת arm עבור כל שירות עם אפשרות זו.
- בעת שימוש בטכנולוגיות קונטיינרים - גובה ההזדמנות לחיסכון על ידי התאמת המשאבים ברמת קונטיינרים לשימוש בפועל.

הגדרת KPI's אופרטיביים אופציונליים

- אחוז שימוש בשירותים מוזלים (כמה מסך השימוש בשירותי המחשוב רץ על שרתי Spot או שירותים בהתחייבות).
- אחוז ניצול ההתחייבויות עבור כל התחייבות שרכשנו
- פילוח עלויות כל פרויקט לפי תיוגים נבחרים.

הגדרת KPI's חובה

- עמידה בתקציב – אופן ניצול התקציב עד לנקודת הזמן הנוכחית.
- צפי לעמידה בתקציב לאורך חיי הפרויקט וזיהוי פרויקטים החורגים או מועמדים לחריגה.
- עלות 'יחידה' (Unit Cost).
- הזדמנויות להתייעלות כלכלית בכל פרויקט ביחס לכלל עלויות הענן של הפרויקט.

שלב 2: הקמה תשתית ענן - eGov

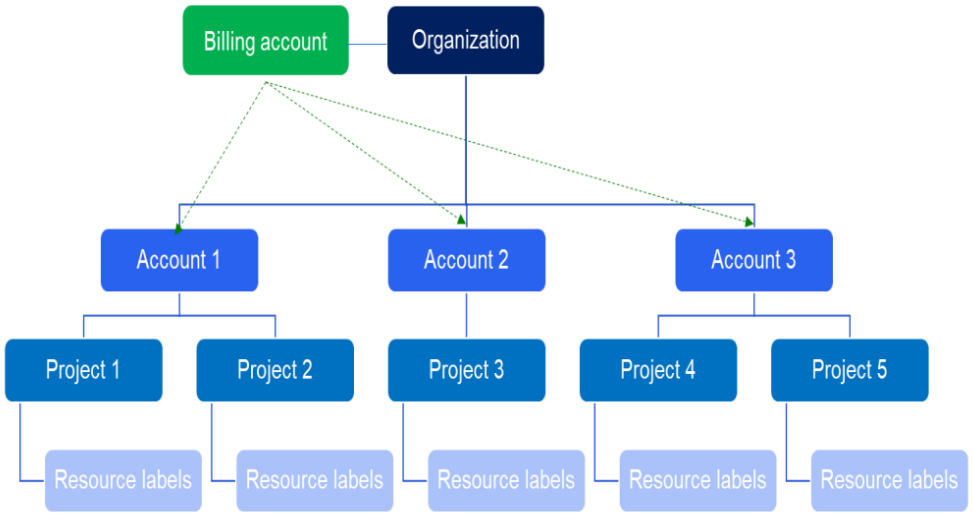
1. קביעת מבנה החשבונות והחיוב
2. קביעת אופן חיוב שירותים משותפים
3. תיוג שירותים
4. KPI’s ודשבורד'ס

בקרה, אכיפה ומשילות – לאחר שלב בחינת התכנון, יתעמק צוות ה- FinOps במנגנוני הבקרה, האכיפה והמשילות שהוגדרו והוטמעו עבור כל פרויקט ויציג תכנית עבודה לייעול במידת האפשר והצורך. עם בניית תכנית העבודה יעבוד צוות ה- FinOpsעם צוותי העבודה השונים כדי לקדם את הטמעת תכנית ההמלצות שהציג במטרה לקיים סביבת עבודה המאפשרת מקסימום גמישות בשימוש בשירותי הענן תוך קיום מנגנוני אכיפה כדוגמת מנגנוני תזמון (Scheduling) של סביבות, התראה על משאבים שלא בשימוש, מניעת שימוש בשירותים לא מאושרים לשימוש, אכיפת תקציב ועוד.

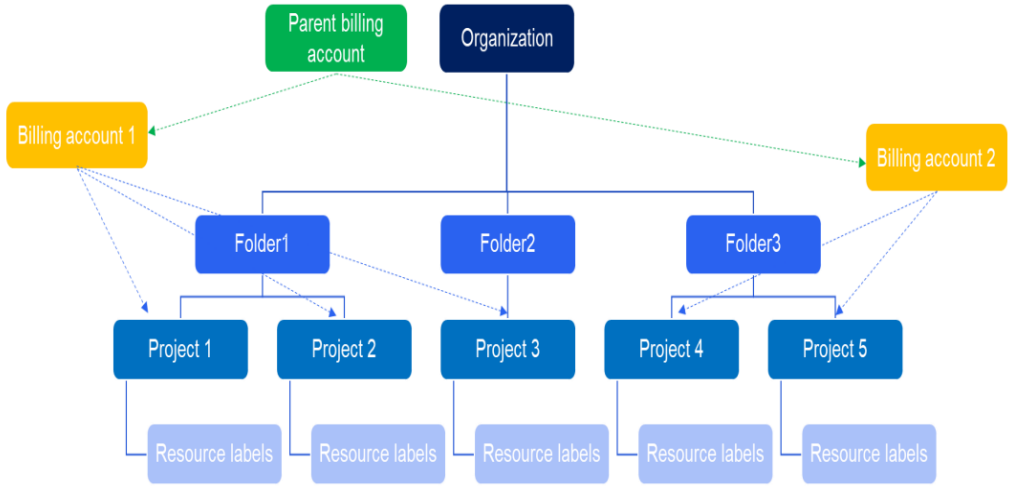
שלב 2 – הקמה: הכנת תשתית ענן - eGov

קביעת מבנה החשבונות / ארכיטקטורת חשבונות ותיוגים

AWS



GCP



Billing accounts

The relationship between a GCP project and a billing account is many-to-one, meaning that multiple GCP projects are attached to one billing account for the entire organization.[7]

Best practice

Use a single billing account for simplicity. Devise internal chargeback mechanisms to allocate costs amongst departments.

מקור: היערכות לסליקה ובילינג בפרויקט נימבוס

שלב 2 – הקמה: משימות

קביעת מבנה הבילינג / הגדרת מבנה חשבונות

- מס' החשבונות הנדרשים עבור הפרויקט (פיתוח, בדיקות וייצור)
- הגדרת Shared services וכן מרווח

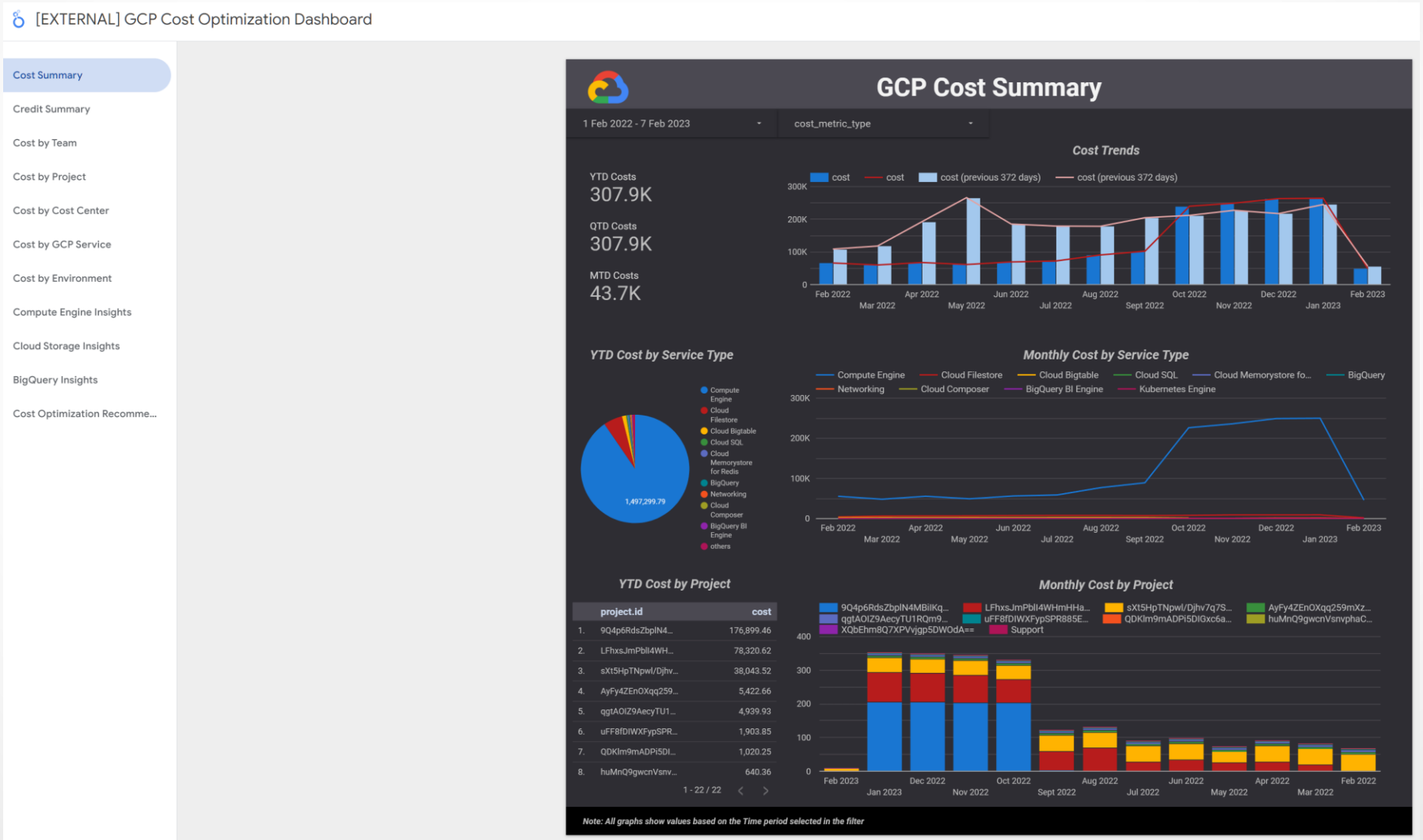
קביעת תיוג ותיוג הפרויקטים

הקמת דשבורדס / דיווחים

- קביעת כלים לניטור עליות ענן ולמעקב יומי אחר עלויות כל פרויקט

שלב 2 – אביפה: הכנת תשתית ענן - eGov

KPI's , דשבורד'ס ודוחות



https://lookerstudio.google.com/reporting/0c1364a4-9c94-4c1d-becd-b9c77dee7aaw2xw/egap/2

שלב 3 - תפעול שוטף (Day 2)

- מעקב אחר **עלויות השימוש השוטפות** של כל פרויקט,
- **אופן ניצול תקציב** הפרויקט,
- **רכישת התחייבויות** עבור השימוש הקבוע בשירותים שונים
- ביצוע **מעקב אחר אופן ניצולן**,
- ביצוע **מעקב אחר ה- KPIs** שהוגדרו לכל פרויקט כולל מדדים חדשים שהגדיר ועוד.

תפעול שוטף – שלב הבקרה והתפעול השוטף הוא מהותי בתהליך העבודה.
בשלב זה, ובהובלת ה- ProcFinOps, ה- FinOps Analyst וה- DevFinOps מבוצעים תהליכי בקרה ומעקב על בסיס יומי/חודשי/רבעוני/חציוני, כפי שמפורט במסמך הנחיות.

מקור: מסמך כלכלת ענן - מדיניות והסדרת תהליכי עבודה – נוסח להפצה

שלב 4 – התייעלות

שלב ההתייעלות הוא שלב מרכזי בתהליך שמאפשר למצות את ההשקעה של המשרד למקסם את הערך לכל שקל.

- התייעלות טכנית - Rightsizing, Refactoring
- התייעלות פיננסית – CUD, סוגי מכונות (Custom), סוגי חוזים
- בקרות – תקציב, התרעות, מגבלות (Capping)...

מעקב אחר המלצות להתייעלות – ישנם מס' כלי המלצות שזמינים למשתמשים:

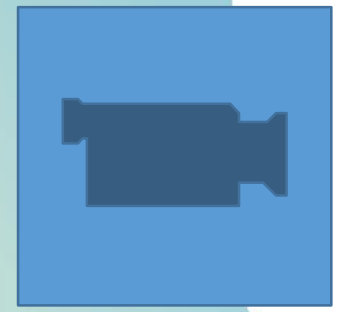
AWS: Trusted Advisor; Cost Recommendations; Compute Optimizer; AWS Rightsizing.
GCP: Cost Recommender; VM Rightsizing; Idle VM Recommender Assist; Active Assist.

מקור: מסמך כלכלת ענן - מדיניות והסדרת תהליכי עבודה – נוסח להפצה

הגשר לענן

Why cloud makes agile and DevOps more important

ויקטור חזנוב
ארכיטקט ענן, CCoE



סרטון קצר

חשיבות Agile ו-DevOps במעבר לענן

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

מעבר לענן- יתרונות



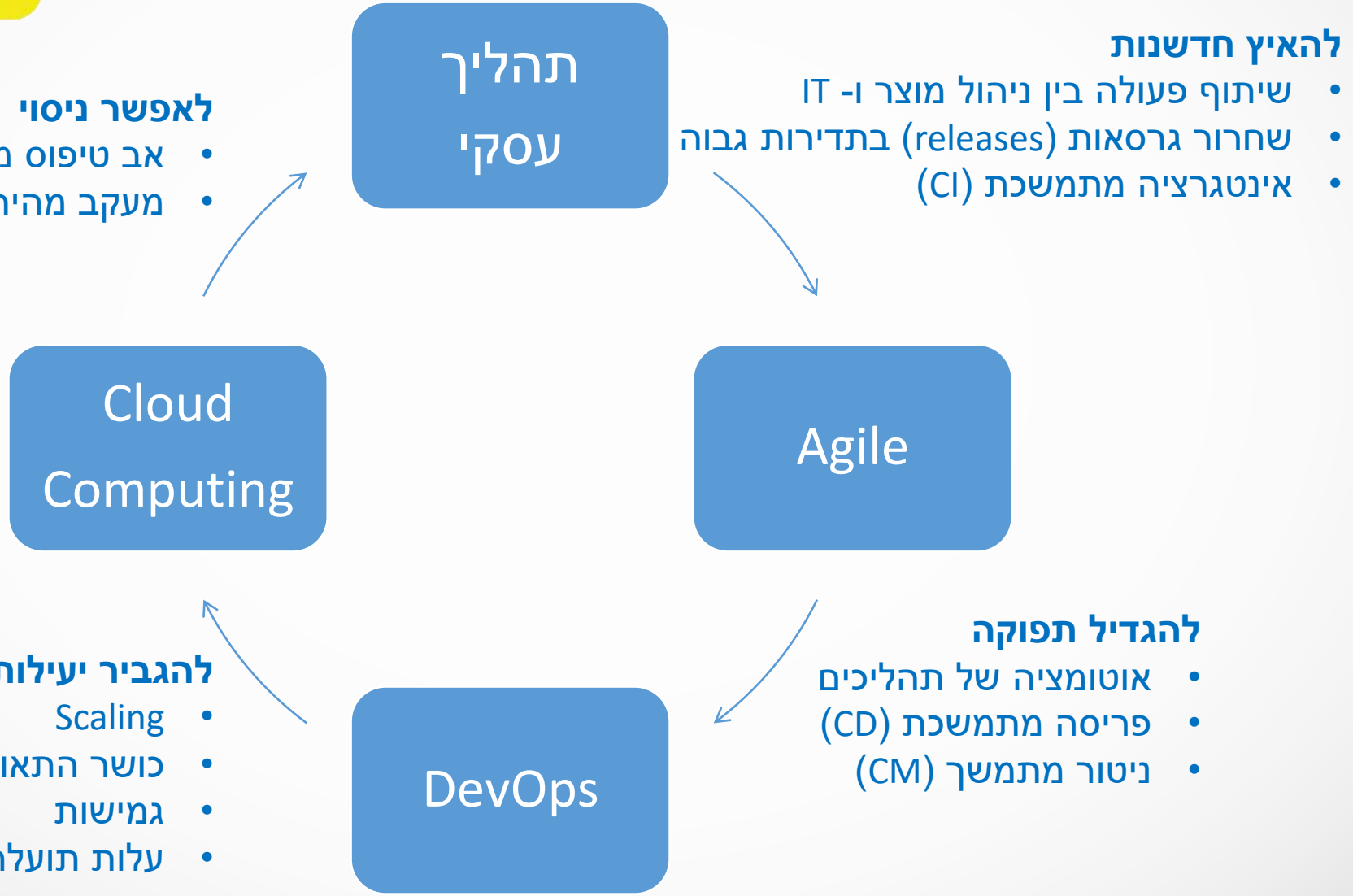
- זריזות
- גמישות
- ביצועים
- חדשנות
- הפחתה בעלויות
- גיבוי יעיל יותר
- אבטחת מידע
- שיתוף משאבים

צווארי בקבוק במחזור החיים של המוצר בענן



- צוות תשתיות IT
- צוותי פיתוח
- צוותי תפעול ואפליקציות

מחזור החיים של המוצר בענן



מתודולוגיה Agile – לקראת השינוי

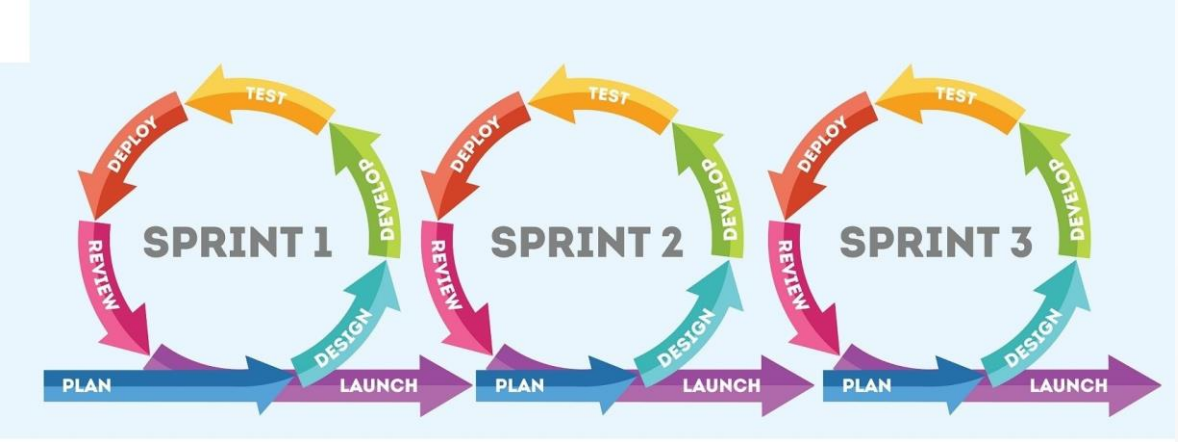


שינויים נדרשים :

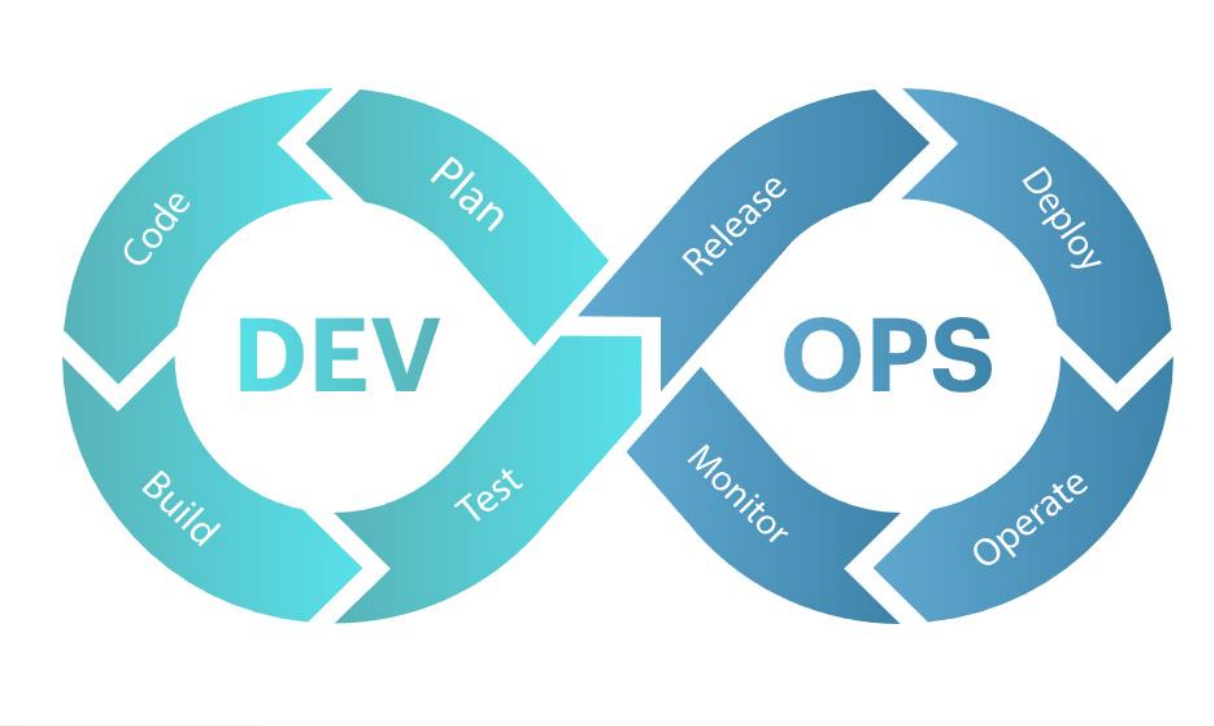
- שינוי תהליכים
- שינוי כלים
- שילוב לקוח עסקי
- אוטומציה של תהליכים
- הכשרת הצוותים

פרקטיקות (תכנון, ישום, הפקת לקחים):

- תכנון ספרינט
- פגישות סטנד-אפ יומיות
- סקירת ספרינט
- הפקת לקחים של ספרינט



מה זה DevOps ?



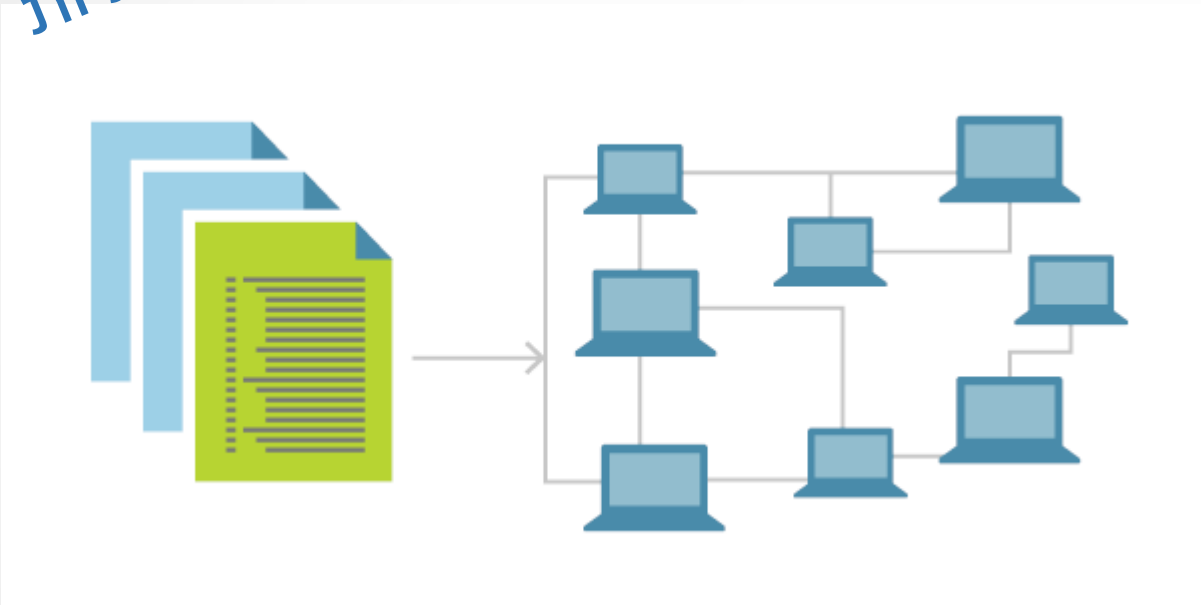
DevOps - אוסף של שיטות עבודה, כלים ופילוסופיה המאפשרת אוטומציה ומשלבת את התהליכים בין פיתוח תוכנה וצוותי IT.
DevOps - תקשורת ושיתוף פעולה בין צוותים ואוטומציה טכנולוגית.

פרקטיקות מקובלות של DevOps:

1. infrastructure as code (IaC)
2. Continuous Development
3. Continuous Integration
4. Continuous Delivery
5. Continuous Deployment
6. Continuous Monitoring
7. Continuous Operations

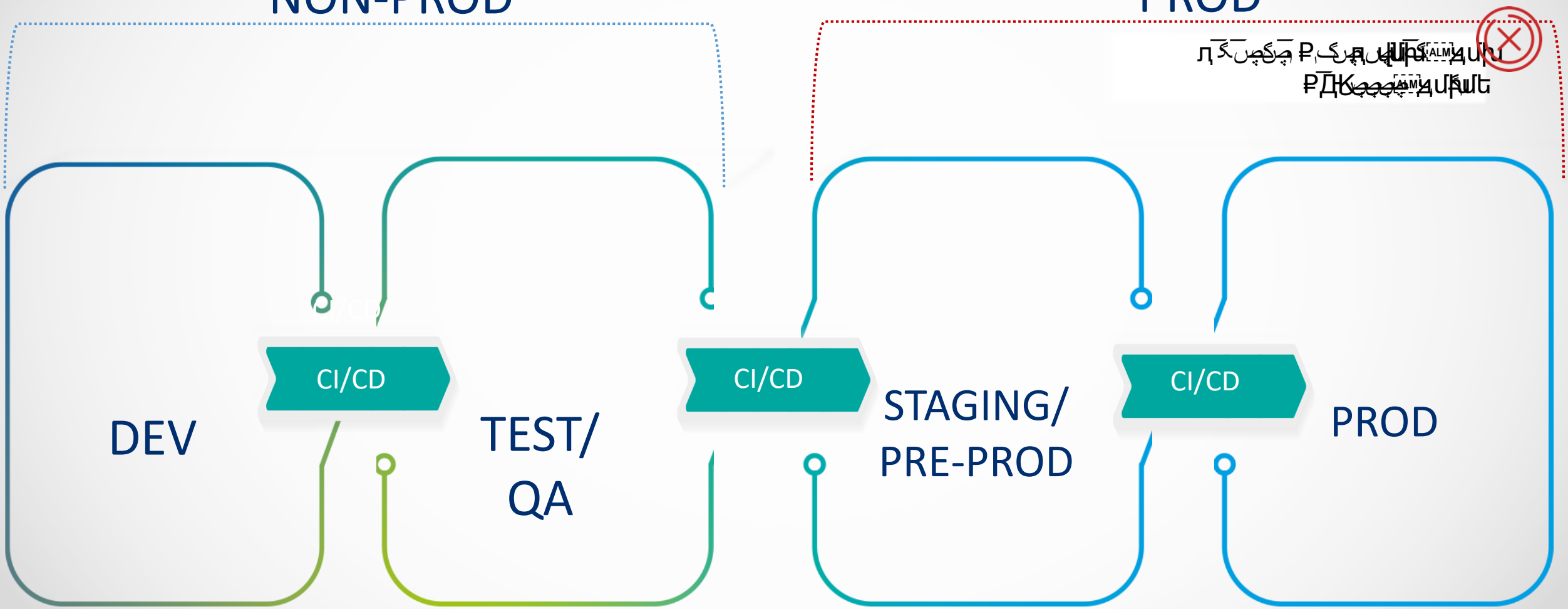
Infrastructure as code (IaC)

יעוד – צוותי תשתיות



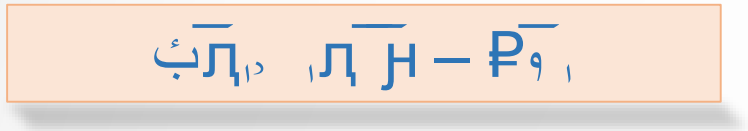
- מקור יחיד של אמת (Single Source of Truth)
  - שמירת הכל ב- source control
    - קוד
    - סקריפטים
    - תבניות תשתית
- בניית תבניות IaC
- שפות JSON או YAML
- שימוש בקבצי הגדרה הצהרתית (declarative)
- אוטומציה קלה
- סטנדרטיזציה סביבות
- סטנדרטיזציה אבטחת מידע
- מדיניות ורגולציה
- חזור לתצורה קודמת מהירה (roll back)

הפרדת סביבות ענן לפי סביבת הנתונים



העברת גרסאות תתבצע ללא מגע יד אדם ועל ידי תהליכי אוטומציה בלבד

- Continuous Development
מקידוד עד איחוד עם ענף ראשי (merge with master)



- כלים לניהול גרסאות של קוד (Git repository)
- בקרת איכות הקוד (code review)
- מדיניות אישורי קוד (code approving)
- זיהוי התנגשויות בקוד
- זיהוי אי התאמה עם הקוד הקודם
- מתן משוב מידי למפתחים על שינויים
- זיהוי vulnerabilities, שגיאות ופגמים בשלב מוקדם בפיתוח

Continuous Integration

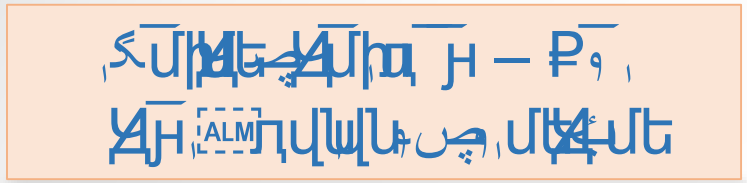
- ריצה אחרי כל commit
  - אוטומציה של הבניית קוד (build)
  - אוטומציה של טסטים
    - בדיקות יחידה
    - בדיקות אינטגרציה
    - בדיקות e2e
  - בדיקת ביסוי קוד בטסטים
  - סריקת קוד לחולשות (vulnerabilities)

Continuous Delivery

QA- [illegible]

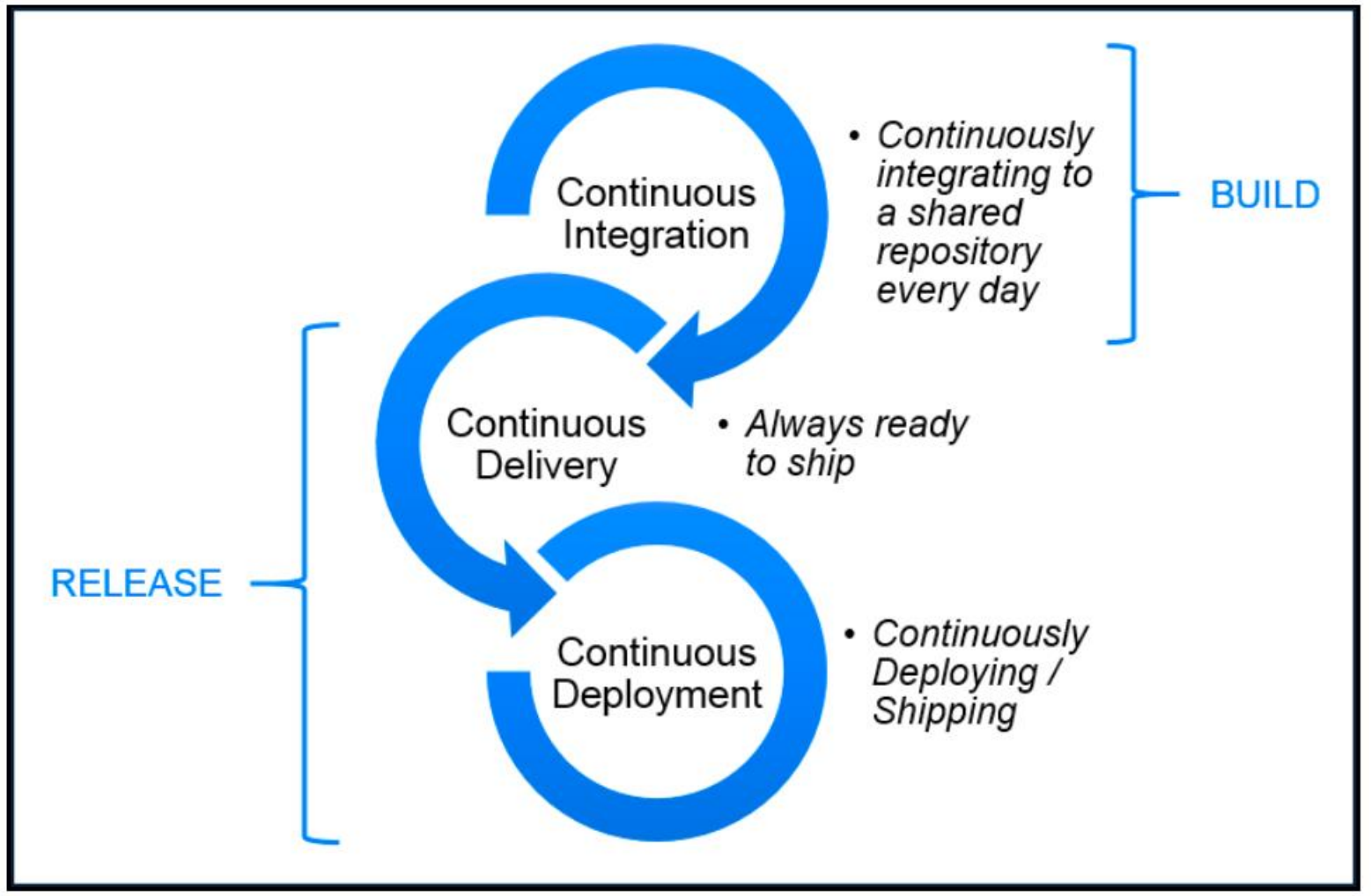
- יעוד – צוותי פיתוח ו- QA
- ריצה אחרי CI
- אוטומציה של הבניית קוד (build)
  - אוטומציה של טסטים על סביבת זהות ליצור
    - בדיקות אינטגרציה
    - בדיקות UI
    - בדיקות API
    - בדיקות e2e
    - בדיקות עומס
    - בדיקות רגרסיה
- בניית חבילה (artifact/image) מוכנה לפריסה ליצור
- סריקת חבילה / אימג׳ לפגיעות

Continuous Deployment

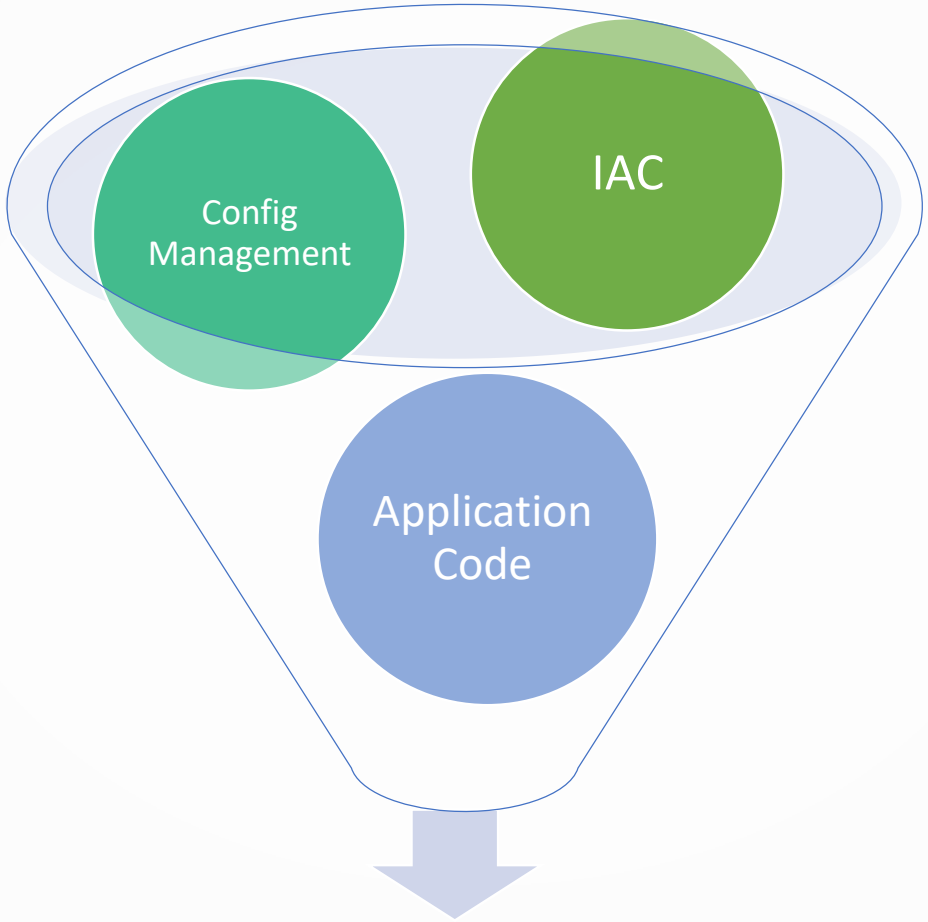


- המשך של Continuous Delivery
- ניהול קונפיגורציות (Configuration management)
- Feature Toggles
- הגדרות סוגי פריסה
  - אוטומטית אחרי כל check-in
  - סלקטיבי
  - blue/green
  - canary
- מהירות להגיב לפריסה
- מדיניות ההפצה ליצור מוכתבת ע''י המשרד (יומי \
- שבועי או הפצה אוטומטית)

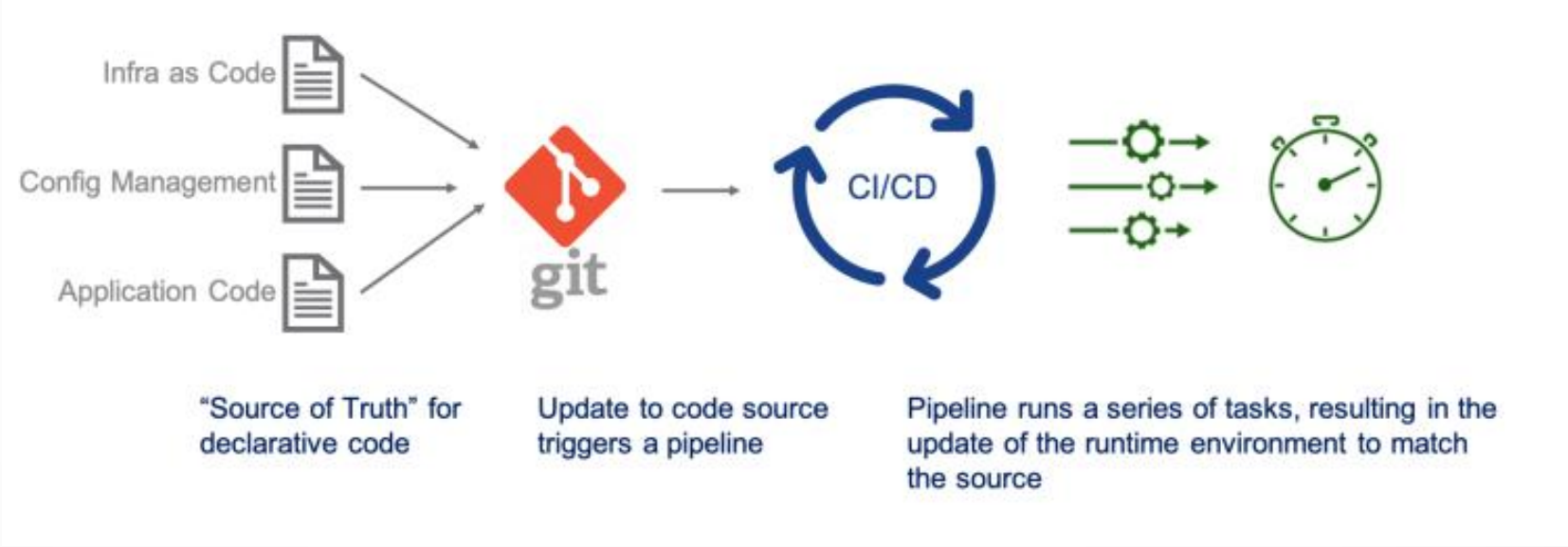
DevOps CI/CD - סיכום ביניים



סיכום ביניים - DevOps CI/CD



סיכום ביניים - DevOps CI/CD



שינויים בענן - DevOps CI/CD



מקור ליישום ותשתית באותו מקום - Git repository



הגדרה הצהרתית (declarative) של תשתיות



IaC – תשתיות דרך קוד



Git as a single source of truth



פריסה לסבית יצור – אוטומטי ,ללא מגע אדם (מפחיות טעויות אנוש)

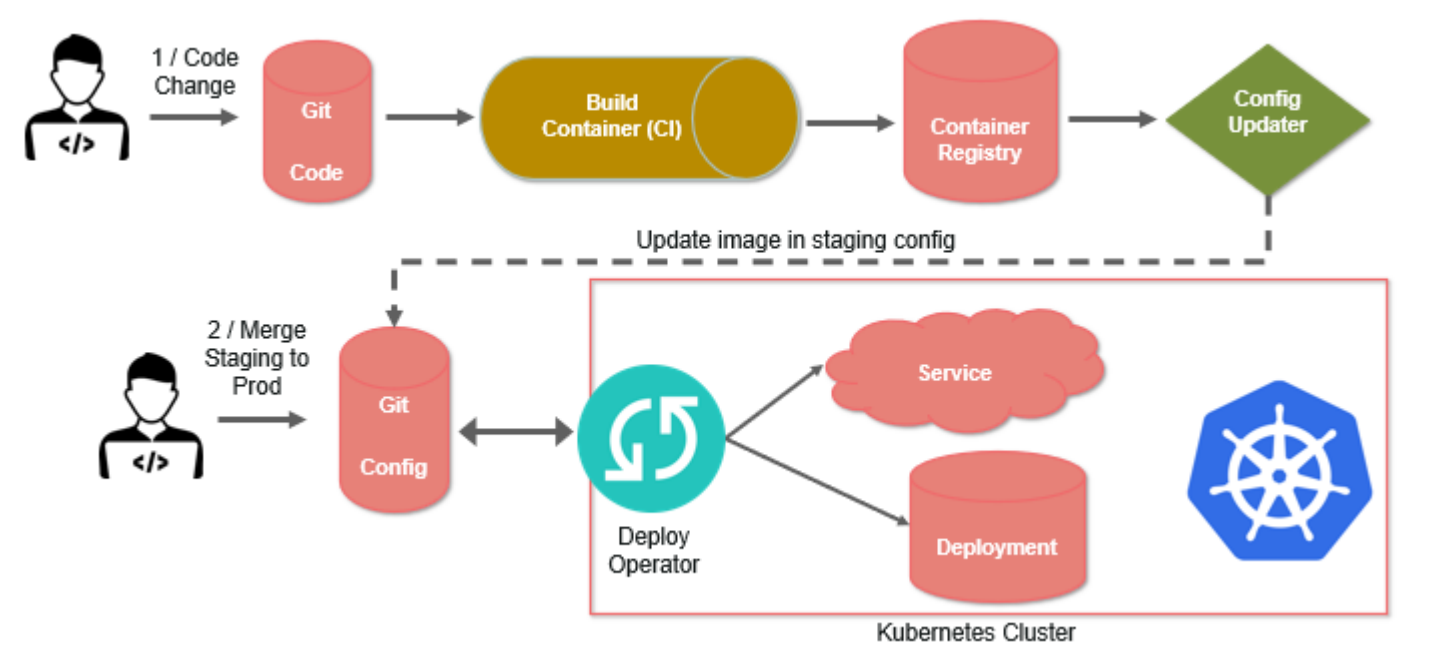


CI/CD pipelines אחראים על build,test & deploy



merge רק אחרי אישור code review/approve)

השינוי בענן
GitOps - pull במקום push



- Current state <> Desired state
- מותאם ל K8s , אבל יש בלים ל- VMs

Continuous Monitoring

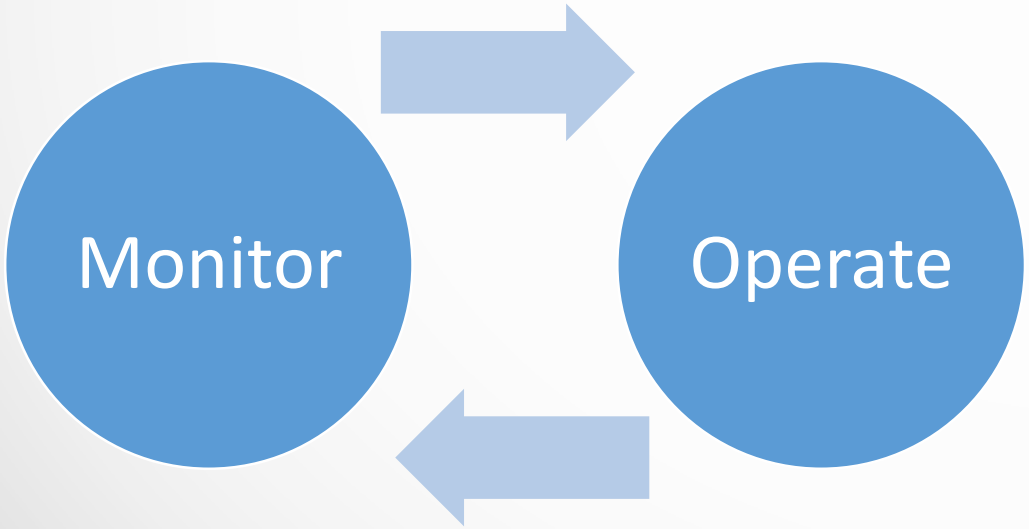
יעוד – צוותי תפעול ו- IT

- זיהוי סיכוני אבטחה
- זיהוי בעיות עמידה בתקנות (compliance)
- הגדרות סוגי ניטור וסיכונים
  - אפליקציות
  - שירותים
  - עומסים
  - רשת
  - מסד נתונים
  - אבטחת מידע
- הגדרת התראות
- תרשימי מדדים
- שאילתות לוגים

Continuous Operations(Day 2)

יעוד – צוותי תפעול

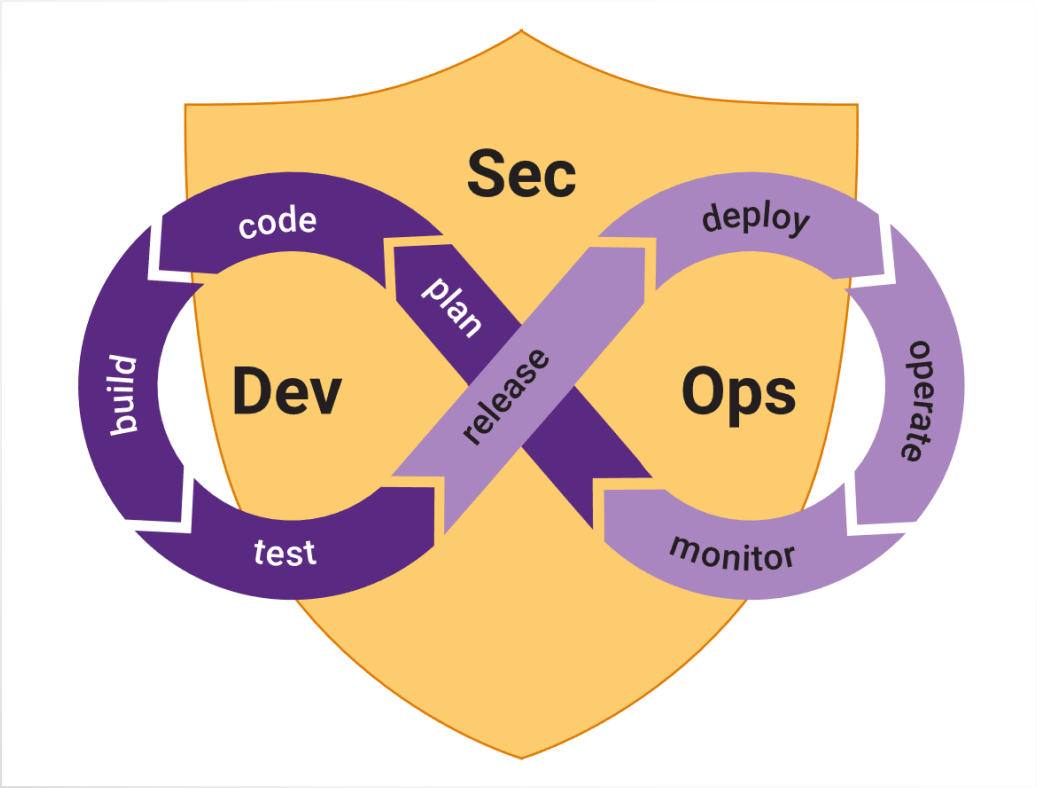
- זמינות
- ביצועים
- ניטור
- שדרוגים
- אבטחת מידע
- FinOps



DevSecOps

Secure by design

יעוד – כולם



- העתקת האבטחה "שמאלה"
- הטמעת פיתוח מאובטח
- זיהוי חולשות
- זיהוי קוד פרוץ
- למזער את שטח ההתקפה הפוטנציאלי
- עקרון ה- Least-Privilege
- הימנע חילוץ מידע
- מתקפת מניעת שירות (DoS)
- עמידה ברגולציה (Compliance)
- זיהוי סודות (secrets)

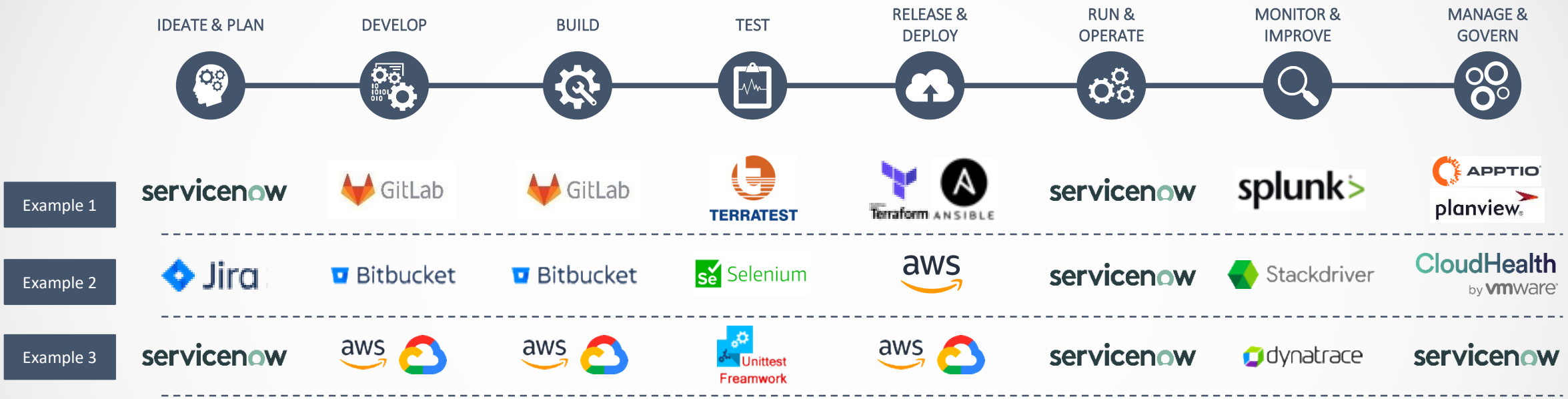
Shift Left

איך מתחילים?



כלים DevOps

דוגמאות של כלים לפי שלבי יישום מערכות



Google Cloud

aws



כלים ברובד 1

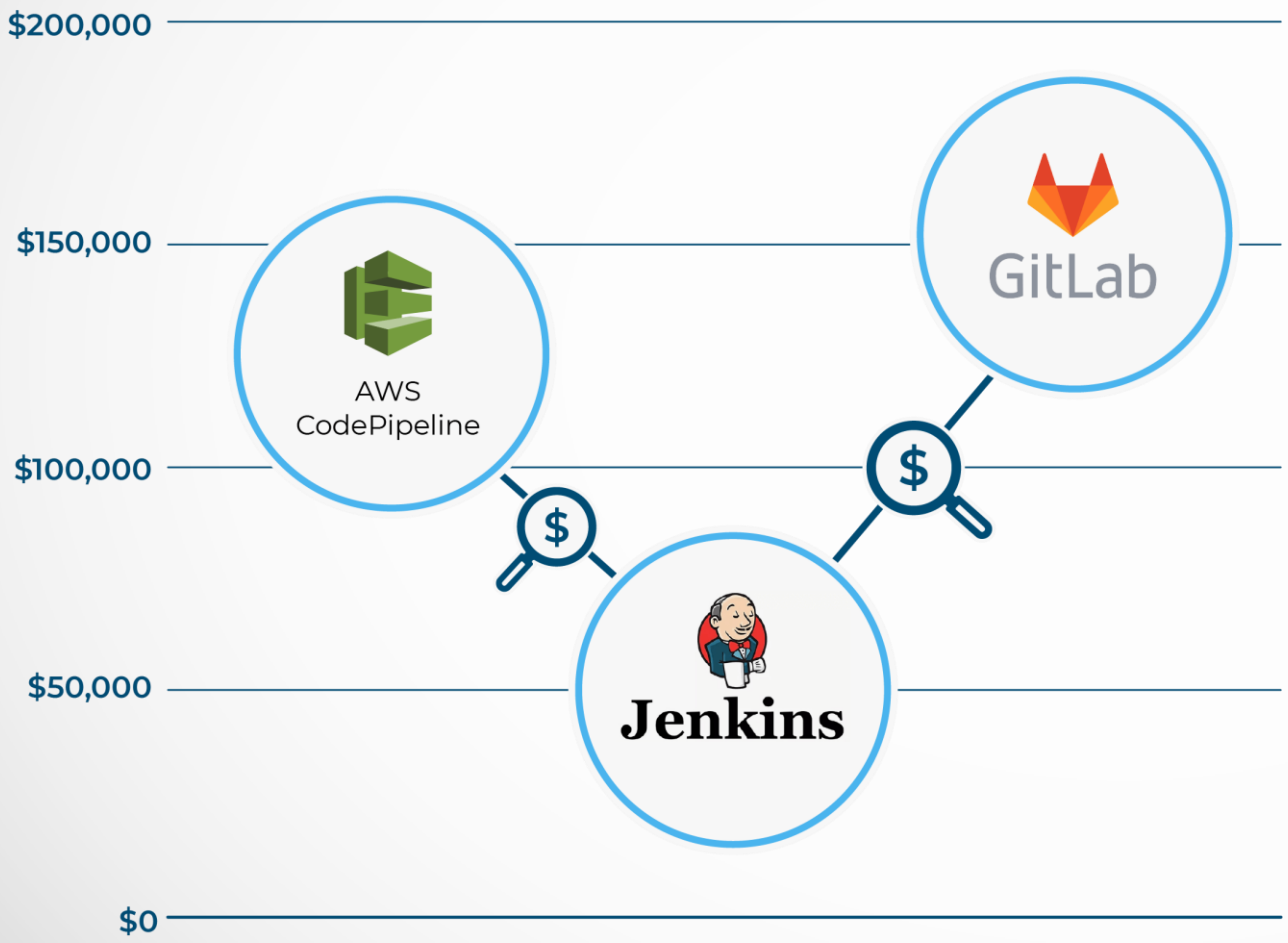
Tool	Description	Develop	Build	Test	Deploy	Operate	Monitor	Govern
AWS Config	Assess, audit and evaluate resource configurations based upon rules.				✔		✔	✔
AWS Cloud9	Preconfigures the development environment ready for serverless development.	✔						
AWS CloudFormation	Provision and management of resources using templates and stacks.		✔		✔			✔
AWS CodeBuild	Compiles and test code, creates software packages for deployment.		✔	✔				
AWS CodePipeline	Automates infrastructure and application code releases for continuous delivery.		✔		✔			
AWS CloudTrail	Tracks Management Console, SDKs and command line tool activities.						✔	
AWS CloudWatch	Unified view of AWS resources, applications, and service based on logs/events.						✔	
AWS Guard Duty	Threat detection monitoring.						✔	
AWS Control Tower	Automated setup of new landing zones using best-practices blueprints.							✔
AWS Beanstalk	Orchestrates deployment of various AWS services, like EC2, S3, SNS and ELB.		✔		✔	✔	✔	
AWS Code Commit	Code repository and version control.	✔						
AWS Code Deploy	Provisions and manages code to EC2 and Lambda.		✔		✔	✔	✔	
AWS X-RAY	Traces and reports application request and response calls.			✔		✔		
AWS System Manager	Update, manage, and configure server resources.					✔	✔	
AWS STS	Security Token Service provides temporary credentials for user authentication.					✔		
AWS Resource Groups	Resource groups helps manage/automate tasks on many resources at one time.					✔		✔
AWS Security Hub	Single view of priority security alerts and compliance across AWS accounts.						✔	
AWS Instance Scheduler	Automates the starting and stopping of EC2 and RDS instances.					✔		
AWS RDS Perf Insight	Monitor, analyze and troubleshoot RDS database performance.					✔	✔	
AWS API Gateway	Creates, publishes maintains, monitors and secures APIs at scale.	✔	✔	✔	✔		✔	
AWS Service Catalog	Create and manage catalogs of IT services that are approved for use on AWS.				✔	✔		
AWS Lambda	Event-driven, serverless computing platform.	✔	✔	✔	✔	✔		



כלים ברובד 1

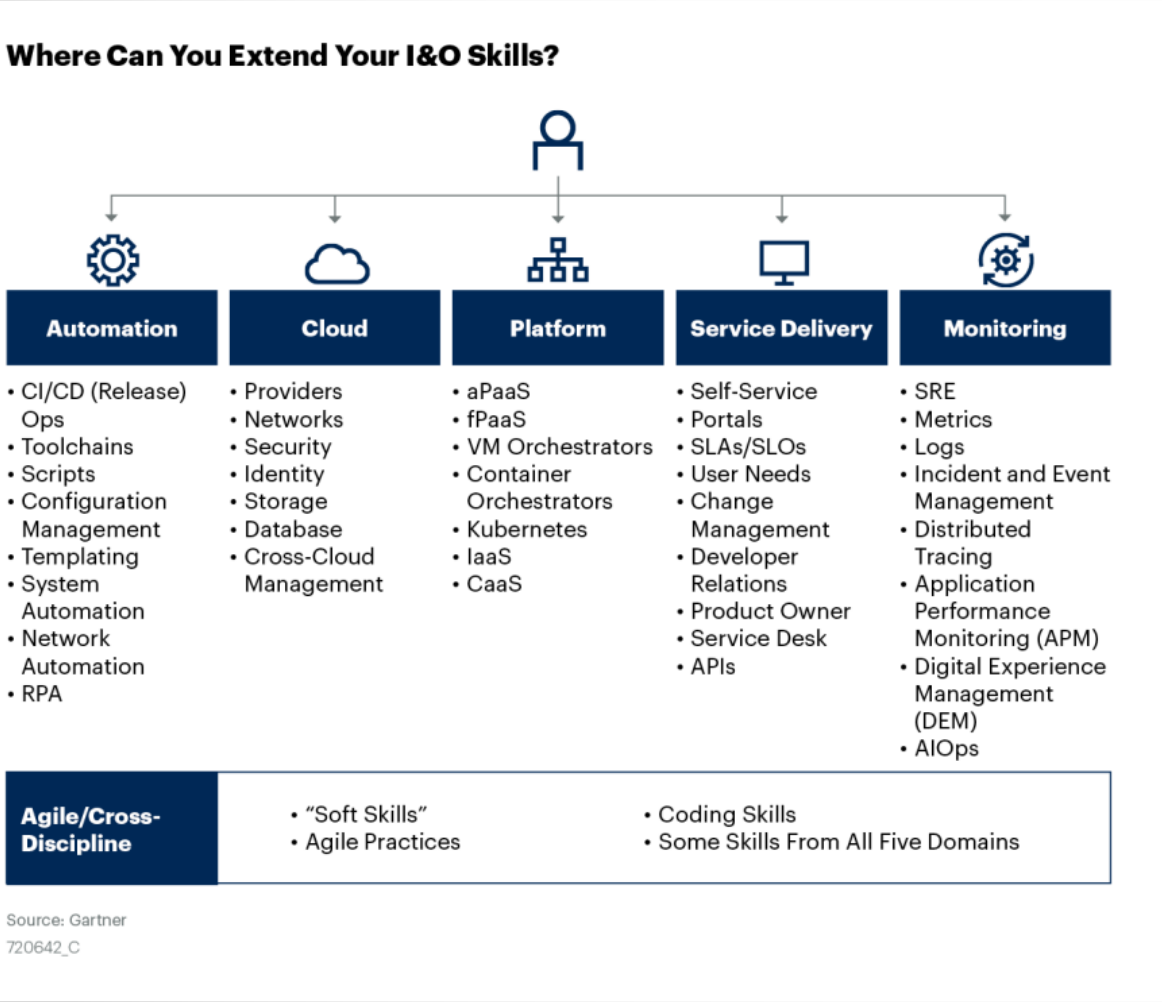
Tool	Description	Develop	Build	Test	Deploy	Operate	Monitor	Govern
GCP Apigee API Management Platform	Design, secure, analyze, and scale APIs anywhere with visibility and control.	✓	✓	✓	✓			
GCP Certificate Authority Service	Simplify the deployment and management of private certificate authorities without managing infrastructure.	✓	✓	✓	✓	✓	✓	
GCP Cloud Build	Build, test, and deploy on Google Cloud serverless CI/CD platform	✓	✓	✓				
GCP Cloud Build Triggers	Automatically starts a build whenever you make any changes to your source code. You can configure the trigger to build your code on any changes to the source repository or only changes that match certain criteria.				✓	✓		
GCP Cloud Deployment Manager	Create and manage cloud resources with simple templates.					✓	✓	✓
GCP Cloud Functions	Run your code with zero server management with this scalable, pay-as-you-go functions-as-a-service (FaaS) offering.	✓	✓	✓	✓	✓		
GCP Cloud Operations	Google's operations suite for monitoring, logging, error reporting, and application performance management.					✓	✓	
GCP Cloud Run	Develop and deploy highly scalable containerized applications on a fully managed serverless platform.			✓	✓	✓	✓	✓
GCP Cloud Scheduler	Fully managed enterprise-grade cron job scheduler. It allows you to schedule virtually any job, including batch, big data jobs, cloudinfrastructure operations, and more.		✓	✓	✓	✓	✓	✓
GCP Cloud SDK	Tools and libraries for interacting with Google Cloud products and services.	✓	✓					
GCP Cost Management	Tools for monitoring, controlling, and optimizing your Google Cloud costs.							✓
GCP Event Threat Detection	A built-in service for the Security Command Center Premium tier that continuously monitors your organization and identifies threats within your systems in near-real time.						✓	
GCP Google Account	Users get access to Google Cloud services by setting up a Google Account.							✓
GCP Google Analytics	Make informed decisions regarding application marketing and performance optimizations by understanding user behavior. Unlimited reporting for up to 500 distinct events that you can define using the Firebase SDK and integrate into the Google ecosystem (BigQuery, Data Studio, Play, AdMob, Ads, and Firebase).					✓	✓	
GCP Identity Platform	Add identity and access management functionality to your applications, help protect user accounts, and scale with confidence using this customer identity and access management (CIAM) platform.						✓	✓
GCP Resource Manager	Hierarchically manage resources by project, folder, and organization.		✓	✓	✓	✓	✓	✓
GCP Role Based Access Control (RBAC)	A built-in RBAC mechanism enables configuring of fine-grained and specific sets of permissions that define how a given Google Cloud user, or group of users, can interact with any Kubernetes object in your cluster, or in a specific Namespace of your cluster.							✓

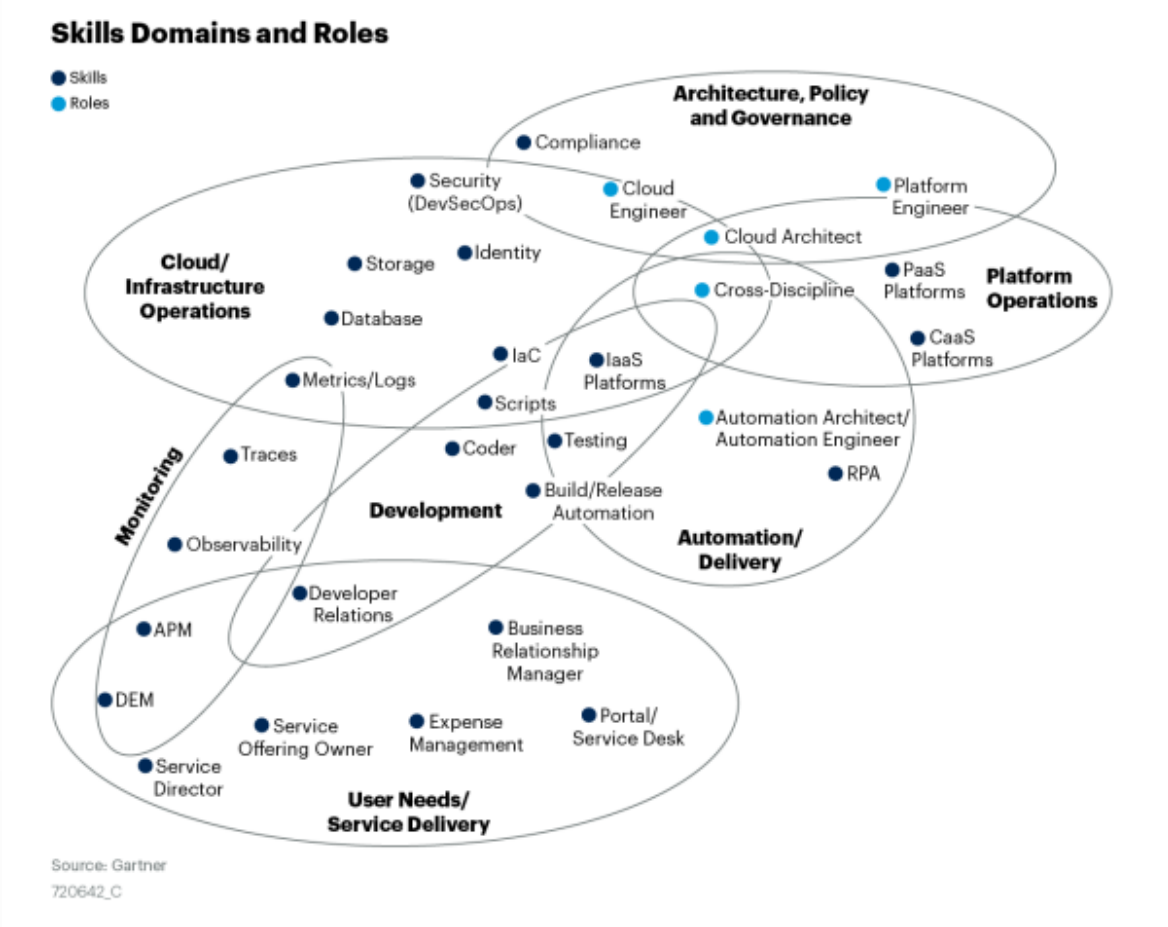
לזכור תמיד לכל שירות ענן יש מחיר



- הבנה של הרכב העלויות
- ניהול עלויות
- יכולת חיזוי
- אופטימיזציה
- הכשרת FinOps

השקעה בהון אנושי והרחבת היכולות





מקור –גרטנר. מאמר New Roles and Skills for I&O Professionals in DevOps

מכרז הדיגיטל טק' (רובד 3) להכנסת ידע לארגון

אשכול תשתיות והגירה לענן



https://govextra.gov.il/offices/cicdxops/

המלצה לצאת לדרך













שינוי תפיסה

Thus, DevOps is not a single role, but rather, an approach that requires closer collaboration between roles.



מודל ההפעלה בענן שינוי תפיסת הניהול התקציבי

ירון אמיר

בין הוירטואלי לפיננסי
השינוי בהיבט ניהול התקציב



מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

What is FinOps



https://www.finops.org/introduction/what-is-finops/



What is FinOps

Google Cloud

- FinOps enables enterprises to drive financial accountability and maximize business value
- FinOps helps understand the complexity and challenges to traditional IT financial management
- FinOps helps to identify the building blocks and key success metrics for business value realization

Value of cloud FinOps

1. Accelerate business value realization and innovation
2. Drive financial accountability and visibility
3. Optimize cloud usage and cost efficiency
4. Enable cross-organizational trust and collaboration
5. Prevent sprawl of cloud spend



https://cloud.google.com/learn/what-is-finops

What is FinOps – Cost Management

Plan

- Define Requirements
- Architect With Cost in Mind
- Choose Pricing Models
- Forecast Consumption
- Deploy Pilot Application
- Establish Budget

Track

- Design Native Hierarchy
- Implement Tagging Strategy
- Allocate Costs of Shared Resources
- Define Metrics to Track
- Alert on Anomalies
- Implement Chargeback and Show back

Reduce

- Dispose of Unused Resources
- Schedule Services
- Rightsized Allocation-Based Services
- Leverage Discount Models
- Upgrade Instance Generation
- Establish a DevOps Feedback Loop

Optimize

- Use Preemptible Instances
- Setup Data Storage Life-Cycle Policies
- Implement Horizontal Autoscaling
- Balance Usage of Consumption-Based Services
- Use Serverless Technologies
- Modernize your Application for PaaS

Evolve

- Adopt Tooling
- Onboard New Providers
- Broker Cloud Services
- Shift Budget Accountability
- Incentivize Financial Responsibility
- Correlate Costs to Business Value

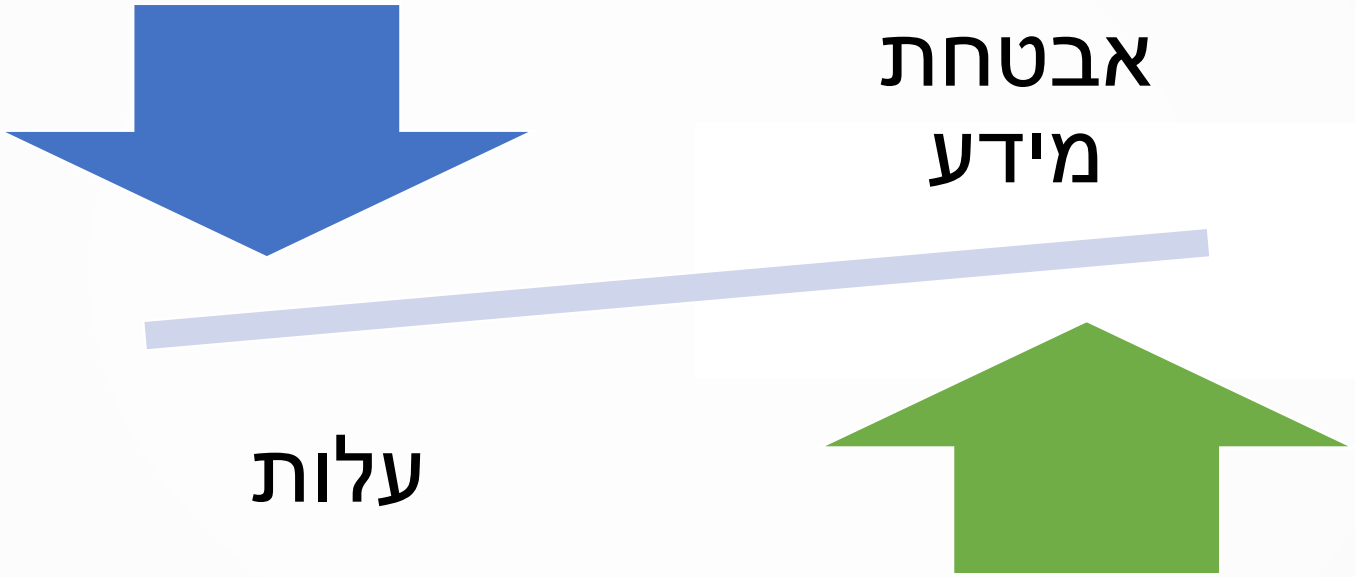


המפתח לפאזל הביליניג הינה ההבנה שכאשר מדברים על FinOps ו- Billing מדברים על

ארכיטקטורה

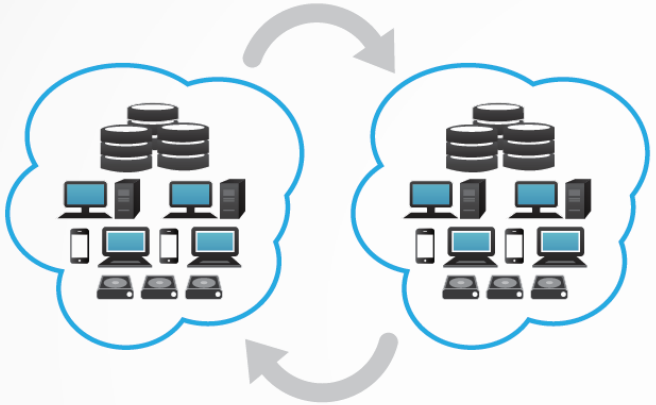
FinOps– כלכלת ענן

ארכיטקטורה בענן מושפעת בעיקר משני גורמים עיקריים



FinOps- בלבלת ענן

DR As Automation



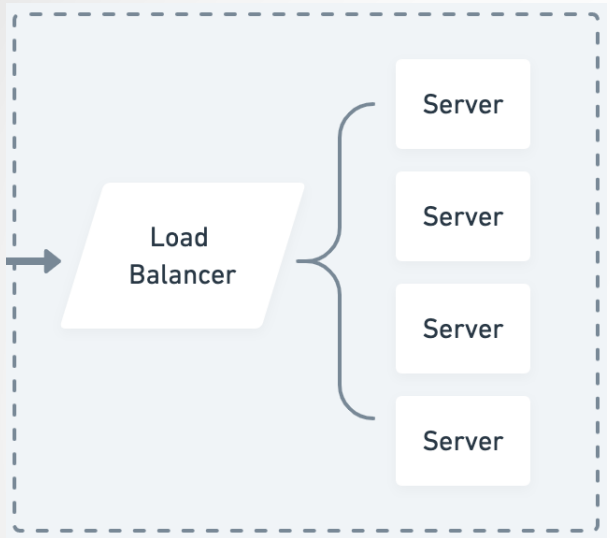
Amazon Relational Database Service (Amazon RDS)

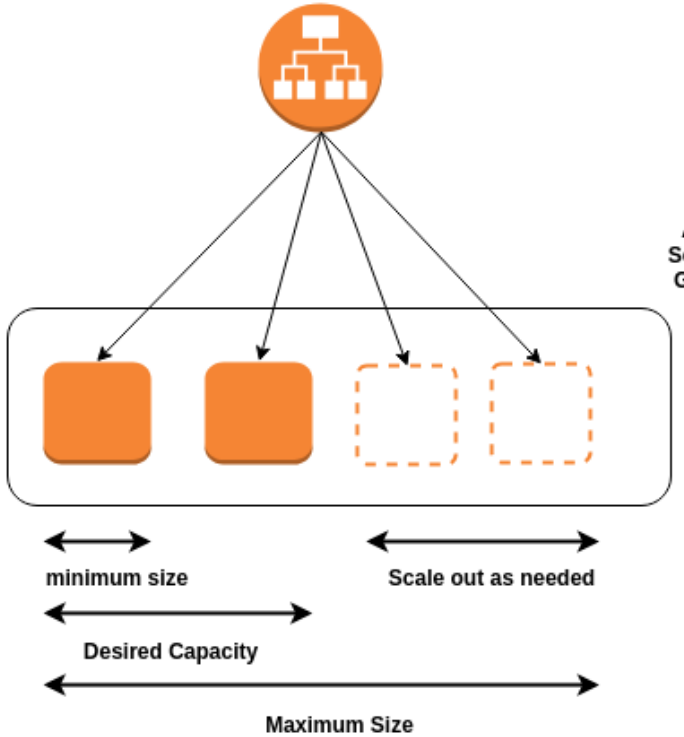
Cloud SQL

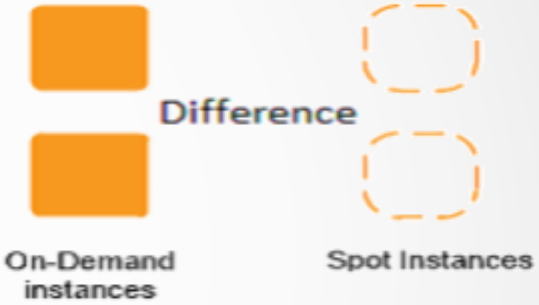
- בסיסי נתונים מנוהלים
  - גיבויים שעתיים
  - Snapshots
  - Cloud storage/s3 backup-restore
  - cluster / multi AZ - HA
- ניהול סביבות prod/non-prod DB

Application layer from ci/cd IAC

FinOps- בלבלת ענן - דוגמאות למיגרציה









Cloud Financial Management

FinOps- בלבלת ענן



Savings Plans



Reserved Instance (RI) Reporting



AWS Cost & Usage Report



Committed Use Discounts and Flat Rate Purchases



Reservations and Savings Plans

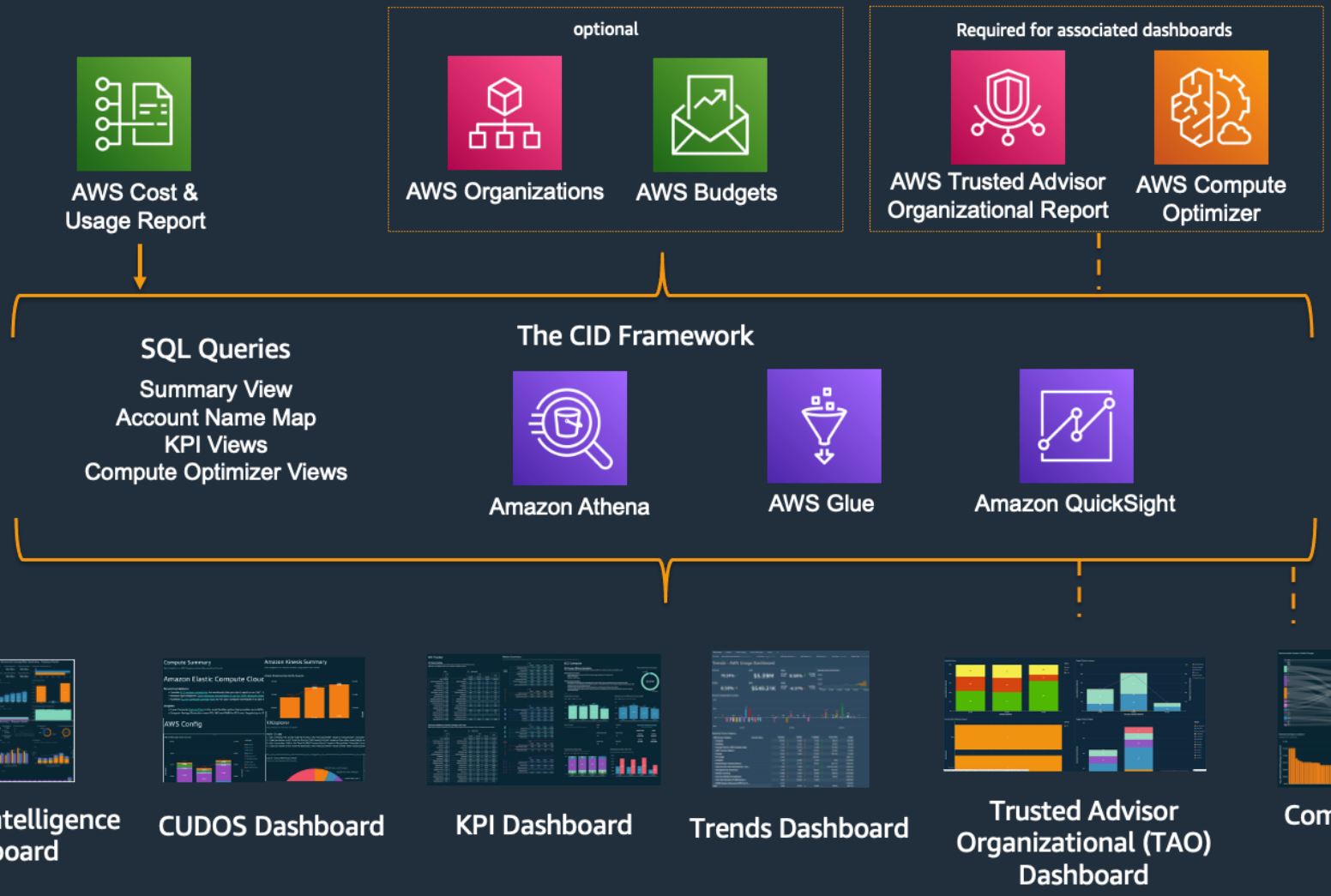
Dashboards

The Cloud Intelligence Dashboards Framework

1. Start with your Cost and Usage Reports

2. Setup the framework

3. Access your dashboards



https://www.wellarchitectedlabs.com/cost/

https://www.wellarchitectedlabs.com/cost//sdraobhsad-troper-egasu-tsoc/ecnegilletni_duolc_200/sbal_200

[EXTERNAL] GCP Cost Optimization Dashboard

Reset

- Cost Summary
- Credit Summary
- Cost by Team
- Cost by Project
- Cost by Cost Center
- Cost by GCP Service
- Cost by Environment
- Compute Engine Insights
- Cloud Storage Insights
- BigQuery Insights
- Cost Optimization Recomme...

Looker

BigQuery

GCP Cost Summary

1 Mar 2022 - 15 Mar 2023

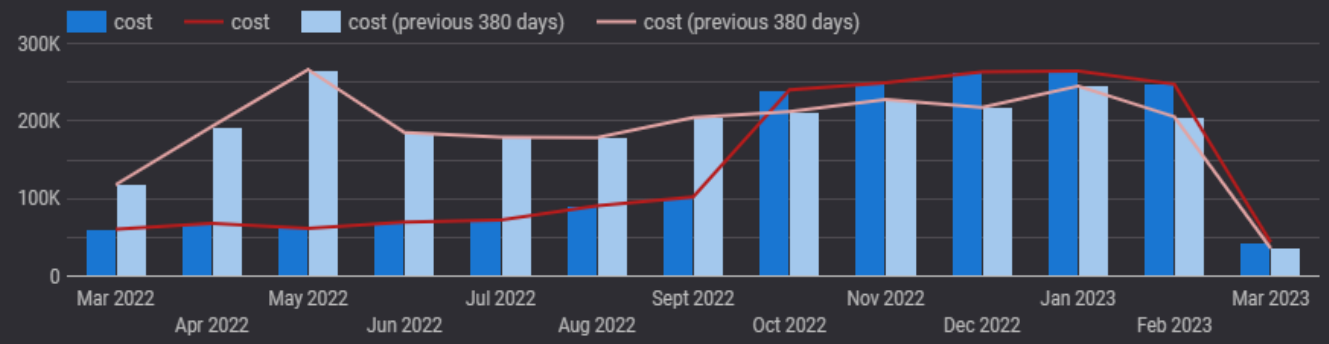
cost_metric_type

YTD Costs
555.0K

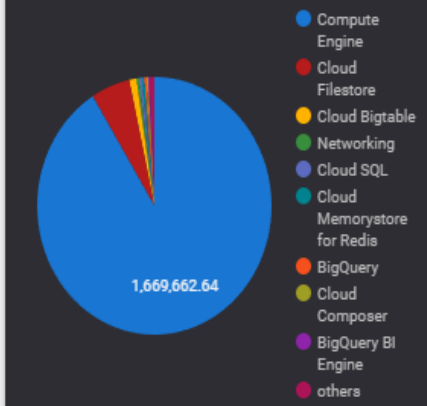
QTD Costs
555.0K

MTD Costs
43.4K

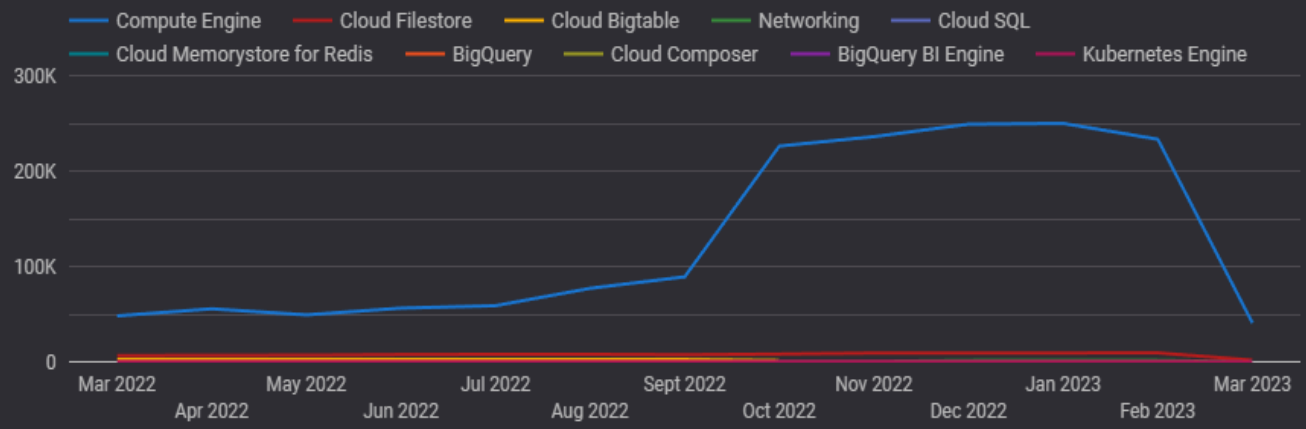
Cost Trends



YTD Cost by Service Type



Monthly Cost by Service Type



https://lookerstudio.google.com/u/0/reporting/6cf564a4-9c94-4cfd-becd-b9c770ee7aa2/page/WXzW

הון אנושי

FinOps- כלכלת ענן תפקידים



גורם	בעלי תפקידים	פירוט	רמת מעורבות
הנהלה	מנכ"ל המשרד, סמנכ"ל תכנון ותקציבים	ביסוס חסות ארגונית על התהליך, הגדרתו כמשימת ליבה והקצאת המשאבים הנדרשים	בינונית-גבוהה
כספים ותקציב	חשבים וסגניהם, מנהלי מחלקות תשלומים, מנהלי מחלקות התחייבויות, חשבונאי ראשי, מנהל אגף תקציבים במשרד	בקרה עליונה ושימוש בכלי ה-FinOps לצורך הקצאת משאבים, ביסוס תהליכי בקרה ובניית תחזיות וניהול סיכונים פיננסיים	גבוהה מאוד
רכש	מנהלי אגפי רכש, מנהלי רכש IT	בעלי עניין מהותיים אשר נוטלים חלק מרכזי בתהליך ניהול כלכלת הענן בארגון ואמונים על זיהוי ומינוף הזדמנויות לאופטימיזציית עלויות	גבוהה מאוד
טכנולוגיה	מנהלי מערכות מידע (CIO), מובילי טכנולוגיות (CTO), צוותי פיתוח, תפעול, הנדסה וארכיטקטורה	בעלי עניין מהותיים אשר נוטלים חלק מרכזי בתהליך ניהול כלכלת הענן בארגון ואמונים על הבנייה הארכיטקטונית והבקרה התפעולית של הפרויקטים	גבוהה מאוד
יחידות עסקיות	מנהלי יחידות עסקיות, דורשים טכניים ביחידות העסקיות ואחראי התקציב ביחידות העסקיות	מעורבים במקרים בהם המימוש הטכני מבוצע בהובלת היחידה העסקית עצמה וכן כאשר תקציב הפעילות הרלוונטית מנוהל באופן ישיר על ידי היחידה העסקית	נמוכה
ספקי הענן	שירותי מומחים, תמיכה וארכיטקטורה	סיוע לארגון במשימות ספציפיות להתאמה ולשיפור פעולותיו בענן	בינונית
ספקים חיצוניים אחרים	יועצים/שותפים/ספקי טכנולוגיה רלוונטית	ייעוץ שוטף לארגון בתחום ה-FinOps, סיוע בתהליכי אופטימיזציית עומק ושימוש בכלים רלוונטיים לצורך כך.	בינונית

FinOps- בלבלת ענן תפקידים



Day 2

Plan

- Define Requirements
- Architect With Cost in Mind
- Choose Pricing Models
- Forecast Consumption
- Deploy Pilot Application
- Establish Budget

Track

- Design Native Hierarchy
- Implement Tagging Strategy
- Allocate Costs of Shared Resources
- Define Metrics to Track
- Alert on Anomalies
- Implement Chargeback and Show back

Reduce

- Dispose of Unused Resources
- Schedule Services
- Rightsized Allocation-Based Services
- Leverage Discount Models
- Upgrade Instance Generation
- Establish a DevOps Feedback Loop

Optimize

- Use Preemptible Instances
- Setup Data Storage Life-Cycle Policies
- Implement Horizontal Autoscaling
- Balance Usage of Consumption-Based Services
- Use Serverless Technologies
- Modernize your Application for PaaS

Evolve

- Adopt Tooling
- Onboard New Providers
- Broker Cloud Services
- Shift Budget Accountability
- Incentivize Financial Responsibility
- Correlate Costs to Business Value

חומרי הדרכה/לימוד

skillbuilder.aws

Optimizing your FinOps Strategy with AWS
FREE
EN | 1h 00m ★ 5.0
Digital training

AWS Billing and Cost Management
FREE
EN | 06m 00s ★ 5.0
Digital training

Deep Dive: Amazon Elastic Block Store (Amazon EBS) Cost Optimization
FREE
EN | 30m 00s ★ 5.0
Digital training

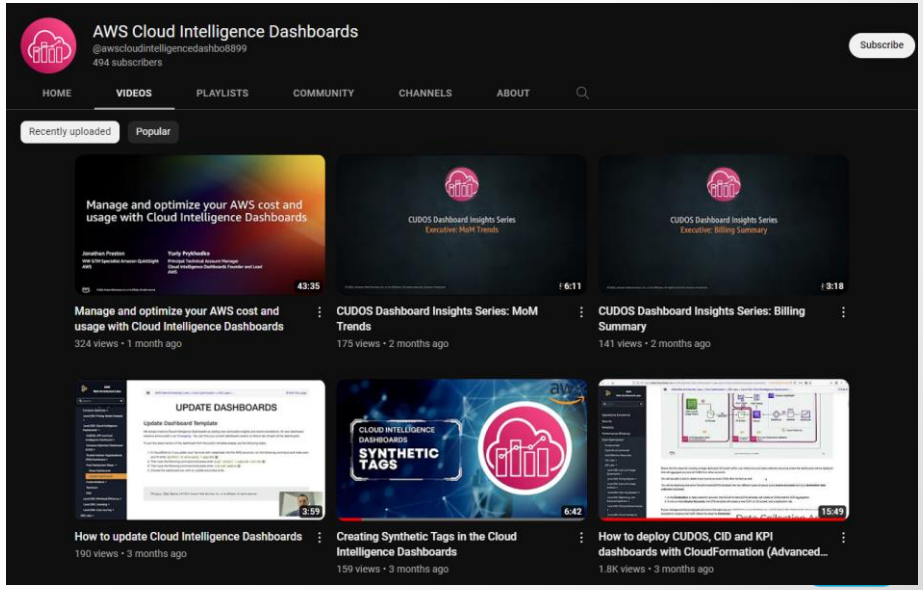
AWS Cloud Practitioner Essentials
FREE
EN | 6h 00m ★ 5.0
Digital training

AWS Cloud for Finance Professionals
FREE
EN | 17h 00m ★ 5.0
Digital training

AWS Cloud Essentials for Business Leaders (Financial Services)
FREE
EN | 2h 00m ★ 5.0
Digital training

AWS Cloud Essentials for Business Leaders
FREE
EN | 2h 00m ★ 5.0
Digital training

https://www.youtube.com/@awscloudintelligencedashbosoediv/8899



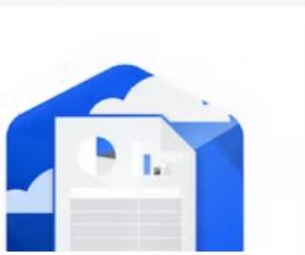
https://explore.skillbuilder.aws/learn/course/external/view/elearning/slanoisseforp-ecnanfi-rof-duolc-swa/10803

https://explore.skillbuilder.aws/learn/course/external/view/elearning/notiazimtipo-tsoc-sbe-nozama-erots-kcolb-ctisale-nozama-evid-peed/10143

https://explore.skillbuilder.aws/learn/course/external/view/elearning/13231/optimizing-your-finops-strategy-with-aws

חומרי הדרכה/לימוד

coursera.org



Google Cloud

Understanding Your Google Cloud Costs

Skills you'll gain: Cloud Computing, Billing & Invoicing, Finance

4.6 (75 reviews)

Beginner · Course · 1-4 Weeks



Google Cloud

Google Cloud Digital Leader Training

Skills you'll gain: Cloud Computing, Cloud Infrastructure, Cloud Platforms, Google Cloud…

4.7 (3.1k reviews)

Beginner · Professional Certificate · 3-6 Months



Google Cloud

Google Cloud Digital Leader Training בעברית

Skills you'll gain: Cloud Computing

4.6 (8 reviews)

Beginner · Specialization · 3-6 Months



Google Cloud

Optimizing Your Google Cloud Costs

Skills you'll gain: Cloud Computing, Accounting, Billing & Invoicing, Cost Accounting, Finance,…

4.5 (26 reviews)

Intermediate · Course · 1-4 Weeks



Google Cloud

Optimizing Cost with Google Cloud Storage

Skills you'll gain: Cloud API, Google Cloud Platform

Intermediate · Project · Less Than 2 Hours



Google Cloud

Exploring Cost-optimization for GKE Virtual Machines

Skills you'll gain: Kubernetes, Network Architecture

Intermediate · Project · Less Than 2 Hours



Google Cloud

Setting Up Cost Control with Quota

Skills you'll gain: Data Analysis, Google Cloud Platform

Intermediate · Project · Less Than 2 Hours



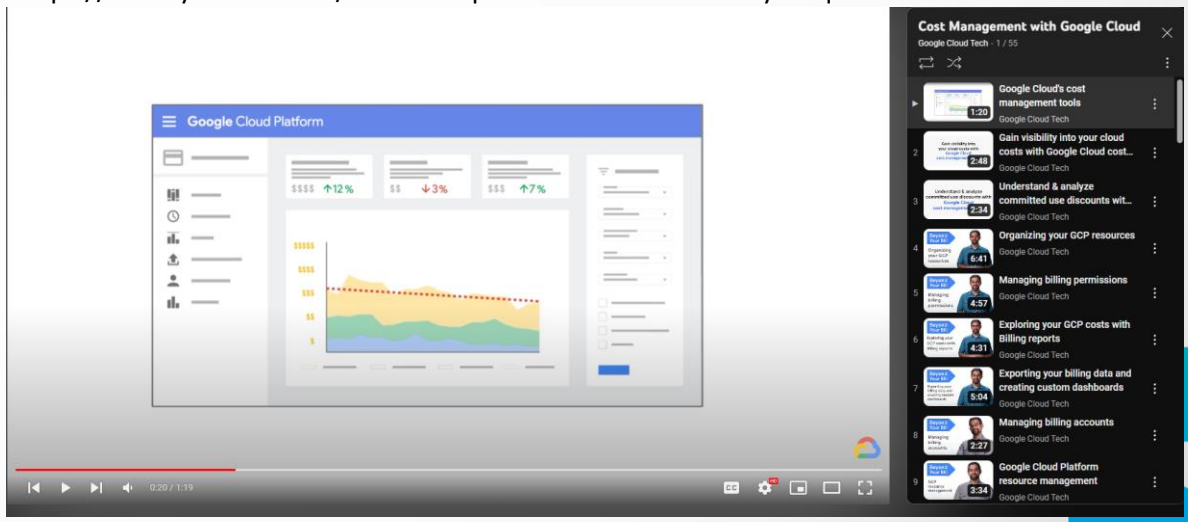
Google Cloud

Understanding and Analyzing Your Costs with Google Cloud Billing Reports

Skills you'll gain: Cloud Computing, Google Cloud Platform

Beginner · Project · Less Than 2 Hours

https://www.youtube.com/watch?v=rplhJdUI-Lo&list=PLIivdWyY5sqKeXavu1XuBNBDLBO31kzM0



https://www.coursera.org/search?query=understanding%20your%20google%20cloud%20costs&index=prod_all_launched_products_term_optimization&allLanguages=English

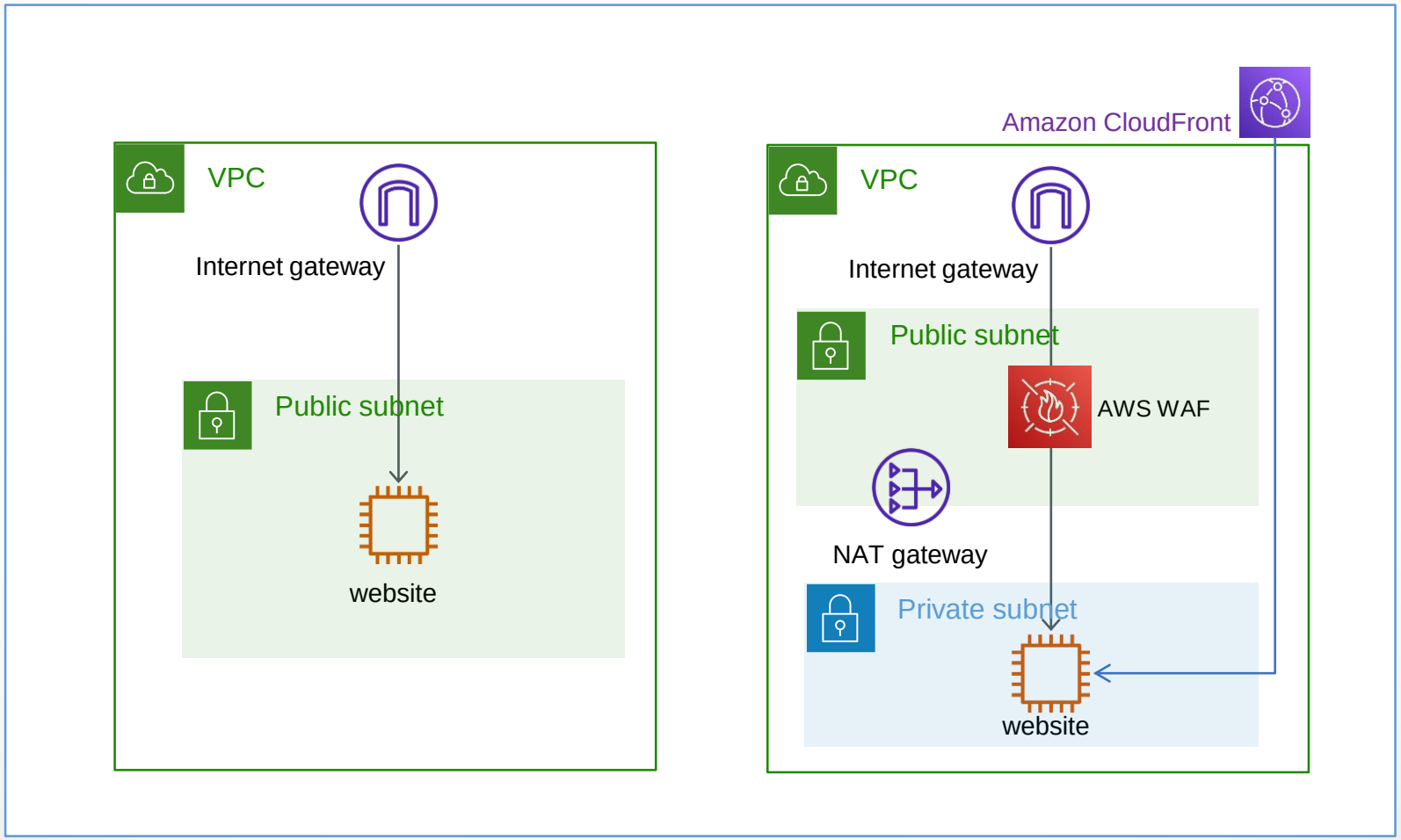
המפתח לפאזל הביליניג הינה ההבנה שכאשר מדברים על FinOps ו- Billing מדברים על

ארכיטקטורה

FinOps- ארכיטקטורה בענן

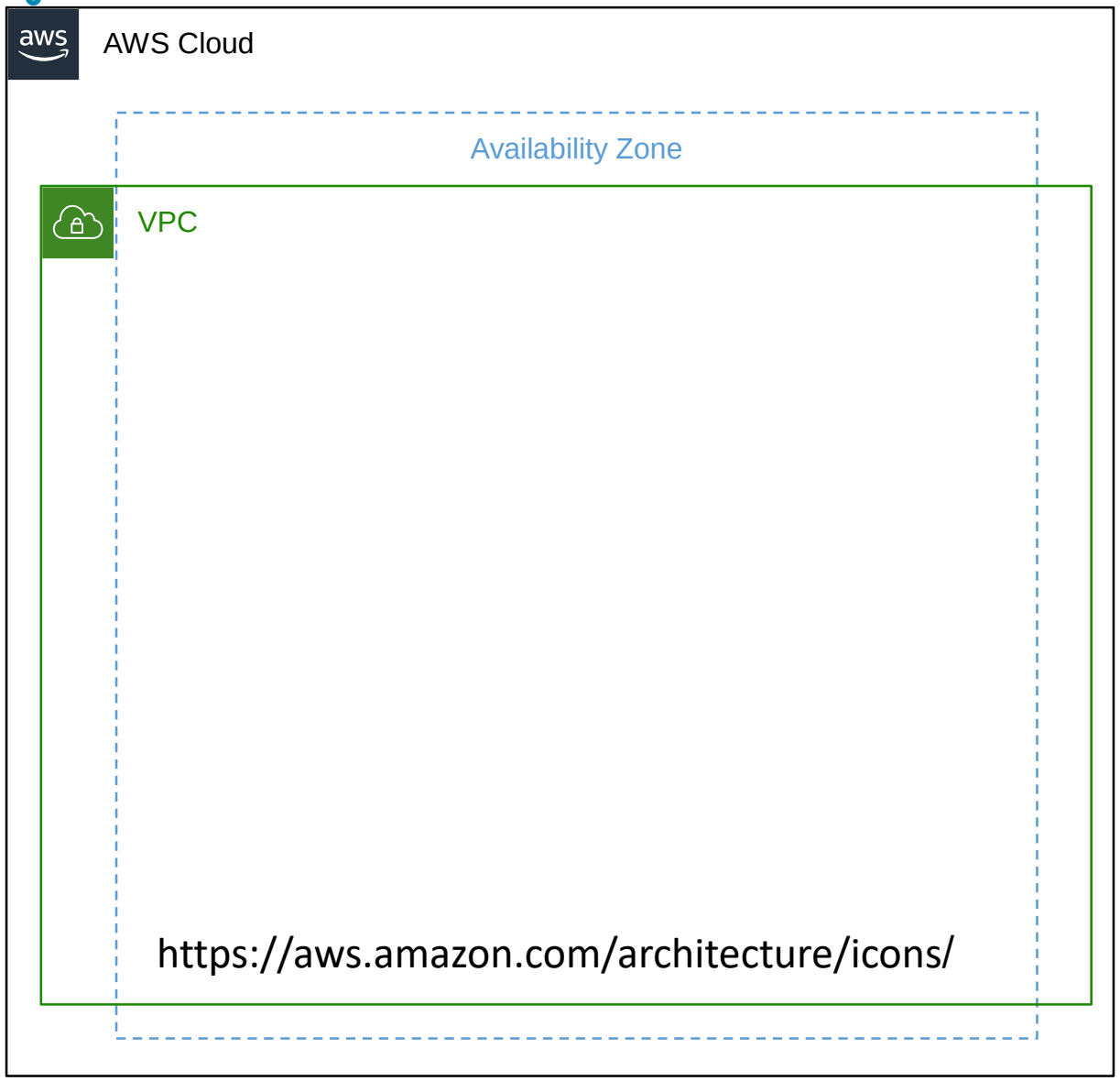
ארכיטקטורה בענן מושפעת בעיקר משני גורמים עיקריים

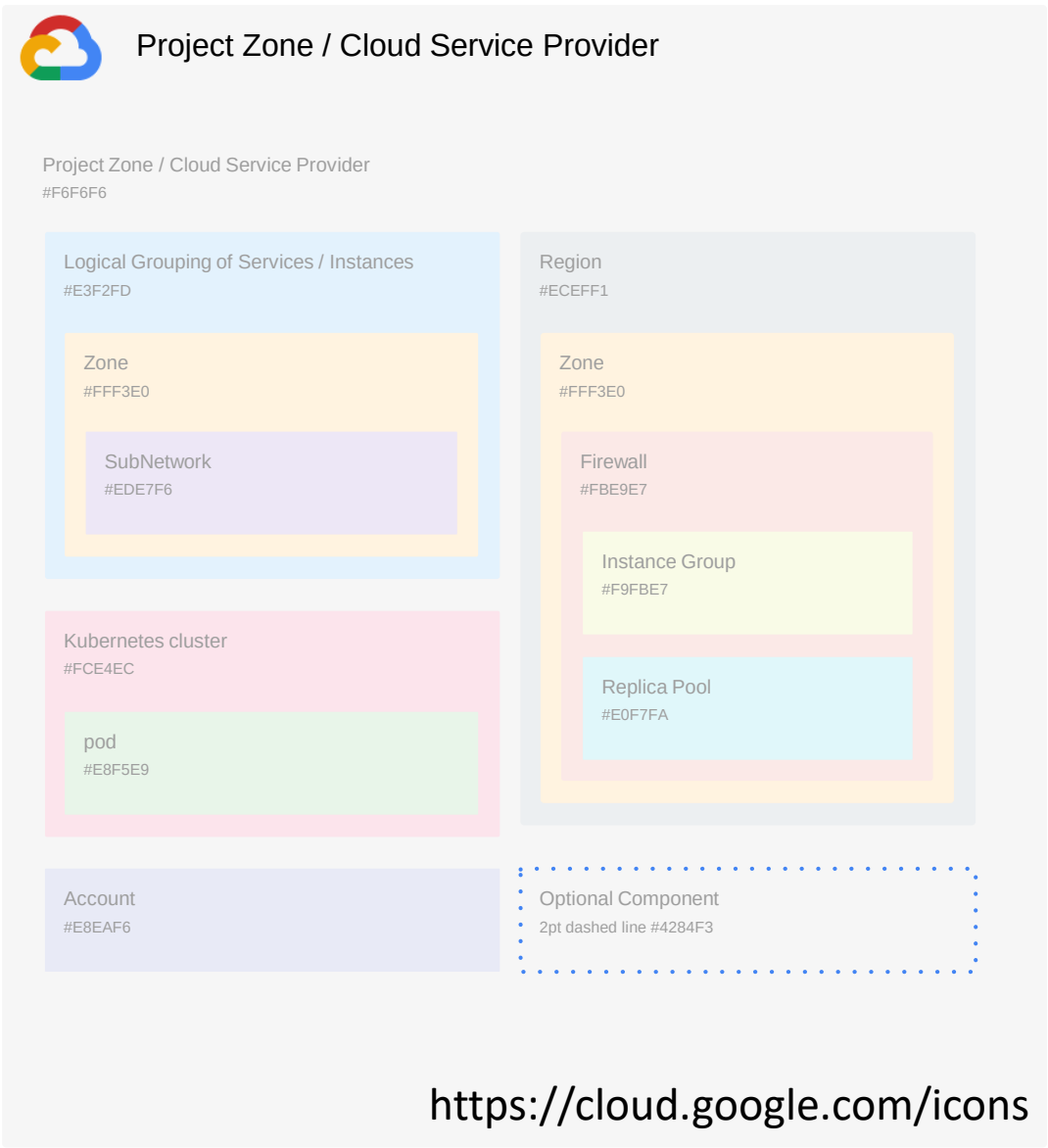
- אבטחת מידע
- עלות



Google

FinOps - ארכיטקטורה בענן





FinOps - ארכיטקטורה בענן

aws

Contact Us | Support | English | My Account | Sign In to the Console

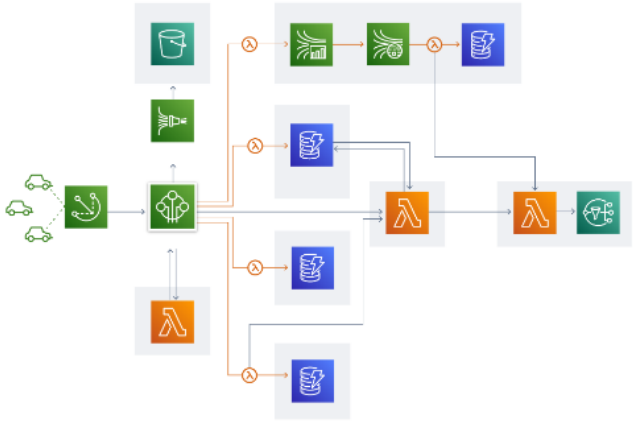
Products | Solutions | Pricing | Documentation | Learn | Partner Network | AWS Marketplace | Customer Enablement | Events | Explore More

AWS Architecture Center | Technology Categories | Video Series | AWS Well-Architected | Libraries | More Resources

Explore Our Architecture Diagrams

Browse AWS reference architecture diagrams and learn how to architect more efficiently and effectively on AWS with our expert guidance and best practices in the AWS Architecture Center.

AWS Architecture Center



Toolkits

Get started with one of our toolkits.

Microsoft PowerPoint
Compatible with Microsoft PowerPoint 2013 and newer (.pptx format).
Download PPTx for Dark Backgrounds
Download PPTx for Light Backgrounds

Sketch
Download Sketch toolkit

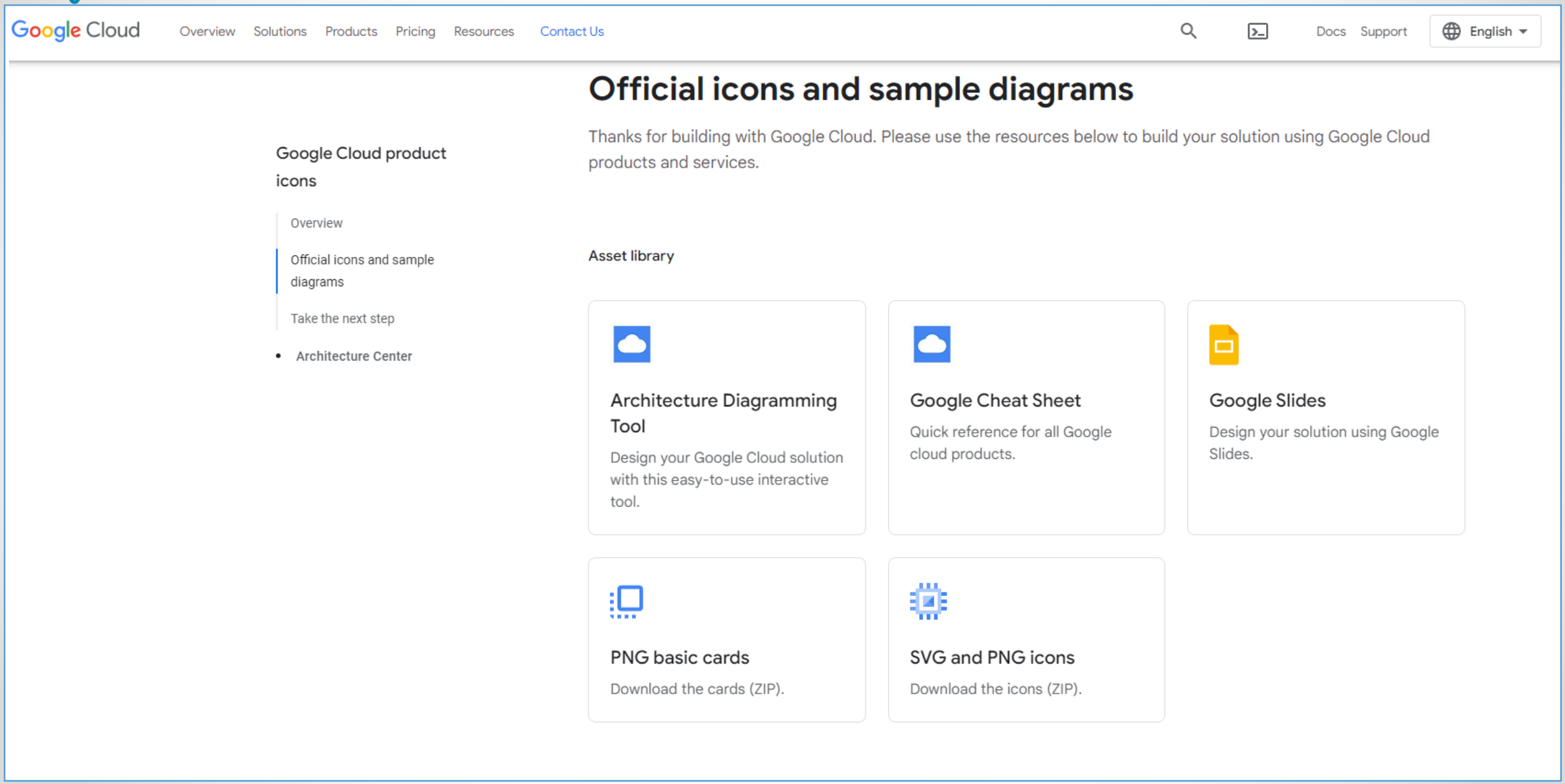
Assets

Import an asset package into your favorite diagramming tool. Package contains sets for both dark and light backgrounds in both PNG and SVG file formats.

Asset Package

Drawing and diagramming tools

FinOps - ארכיטקטורה בענן



סיכום
יום

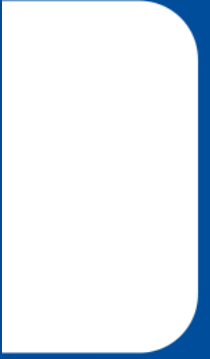
Cloud Me In

קרן הציגה את מודל ההפעלה בפן התהליכים ושינוי ארגוני

ויקטור הציג את תפיסת ה DevOps כגשר לענן

נדב הציג את במסע המשרדי בהקמת צוות ניהול תקציבי לענן עבור מערך השירותים הדיגיטליים

ירון הציג את השינוי בניהול התקציבי בהתייחס לארכיטקטורה













ניימבוס
Cloud Me In

תודה רבה!



מנהלי הקהילה

ירון אמיר
ארכיטקט ענן ראשי
yarona@digital.gov.il

קרן בר-לב
CTO ממשלתי ומנהלת יחידת ה- CCoE
karenb@digital.gov.il



צוות אזור הנחיתה ממשלתי

יוסי אבגי
שלומי ארונוביץ שקד
קובי הירש
אורית אלימלך- זוסמן
שייע כגנוביץ
אלון גלעד
אלכסי נקרסקוב



משתתפים בהכנת המפגש

נדב שרייבמן
nadav@digital.gov.il
052-2324420

ויקטור חזנוב
VictorK@digital.gov.il

חדווה בן חיים
Chedvab@digital.gov.il



צוות Let's Gov

יעל בראל
ענת קוסיאק
שולמית זריהן

מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

let's gov

ניימבוס
Cloud Me In

אתר נימבוס
Cloud Me In

מייל NimbusCCoE@Digital.gov.il

נימבוס
Cloud Me In