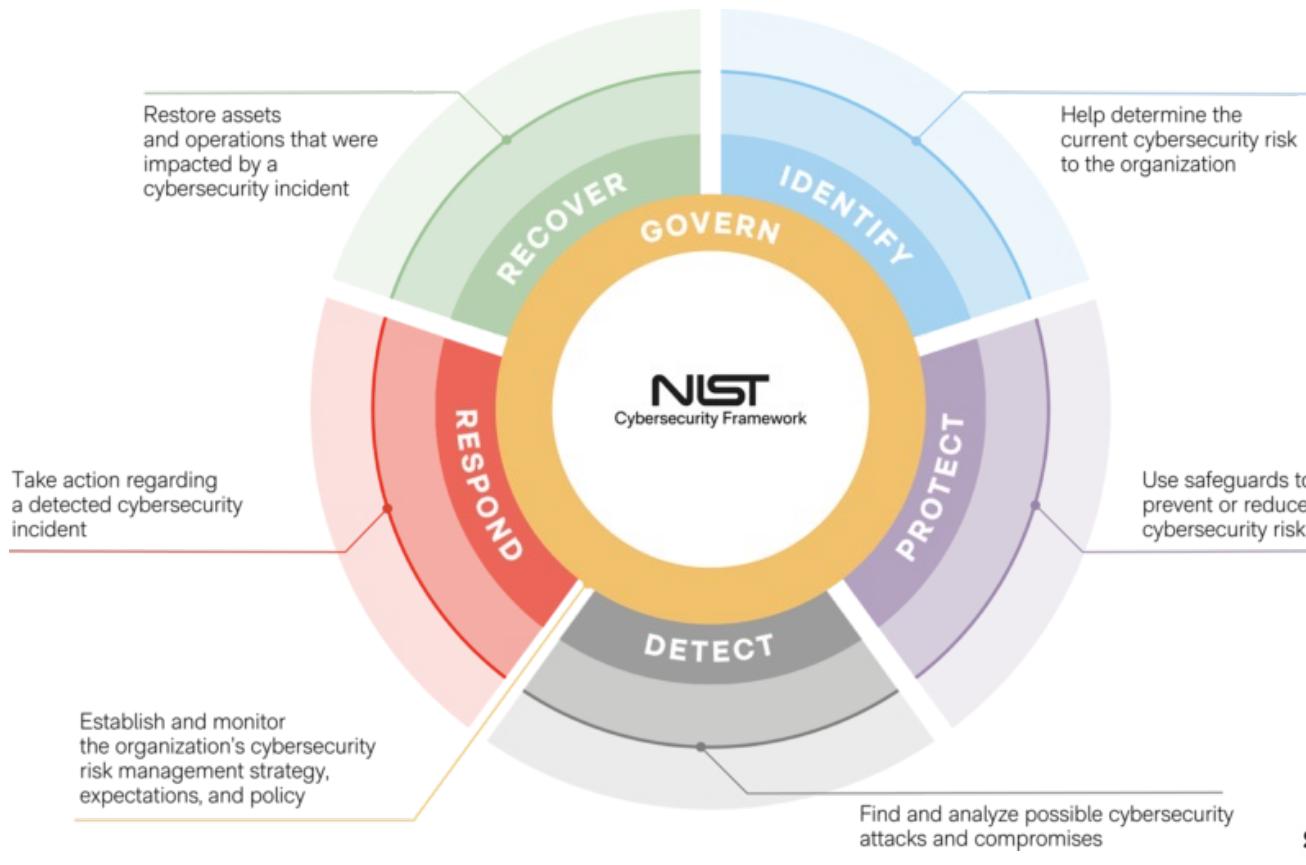


# שיעור 3

NIST Cybersecurity Framework

# NIST Cybersecurity Framework (2.0)



## מטרת השיעור

שיעור שלם על CSF NIST, השתגעתם?  
כן.. לכן מטרות השיעור הן:



- להכיר את התכנית, כיצד נוצרה ולמה נועדה.
- להבין כיצד לישם את התכנית בארגונים השונים.
- לפתח גישה ביקורתית וишומית למדייניות סייבר בארגונים!

## ההיסטוריה וסיבת הקמה

תכנית ה-Cybersecurity Framework NIST הוקמה בעקבות צו נשיאותי 13636, שפורסם ב-12 בפברואר 2013. הצו יזם שיתוף במידע על איום סייבר ופיתוח מסגרת להקטנת סיכוןם בתשתיות קritisיות. NIST נבחרה בשל היotta סוכנות לא-רגולטורית עם היסטוריה של שיתוף פעולה עם התעשייה והאקדמיה. פיתוח הממסגרת כלל בקשות מידע, תגבות ציבוריות וחמשה סדנאות שנערכו בארצות הברית, בהם זוהו פערים והוכנו תוכניות פעולה.

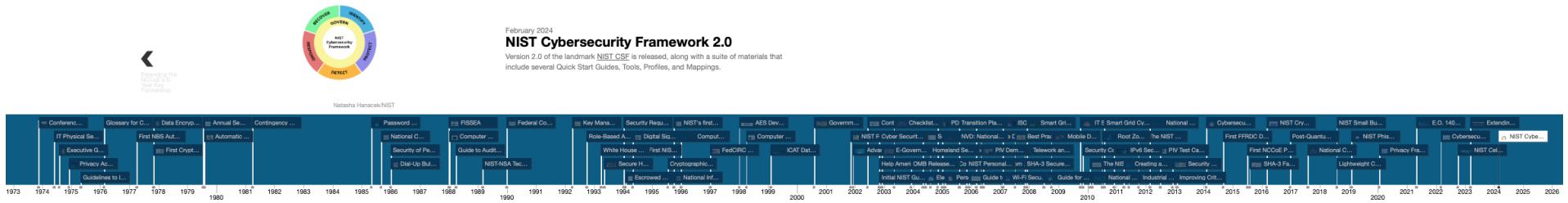
לקריאה נוספת: <https://www.nist.gov/cyberframework/history-and-creation-framework>

## ההיסטוריה וסיבות הקמה

הסיבות העיקריות לפיתוח תכנית ה-NIST Cybersecurity Framework היו:

- עליה דרמטית באירועי הסייבר.
- הצורך בהגנה טובה יותר על תשתיות קritisיות.
- הצורך בתכנית גובש כדי להגדיר מתודולוגיה אחידה לניהול סיכון סייבר.
- לחזק את הגנת המתקנים קritisיות במגזר הפרטי והציבורי.
- לשפר את שיתוף הפעולה בין הממשלה הפדרלי לבין גורמים בתעשייה.

# ההיסטוריה אינטראקטיבית



נא ליעין ב: <https://csrc.nist.gov/nist-cyber-history>

## תמצית התכנית

תכנית ה-Cybersecurity Framework NIST היא **מסגרת לניהול סיוכני סיבר**, שפותחה על ידי המכוון הלאומי לתקנים וטכנולוגיה בארצות הברית. התכנית נועדה לעזור לארגונים **לזהות, להגן, להגיב ולהתאושש** מאירועי סיבר. היא מציעה גישה שיטתית וمتודולוגית מבנית לשיפור אבטחת המידע והتمודדות עם סיוכנים, ומתאימה למגוון רחב של ארגונים בכל הגודלים. המסגרת כוללת עקרונות, תהליכיים וכליים שנועדו לשפר את מוכנות הארגון ולהפחית את הסיכון לפגיעות סיבר.

## **תמצית התכנית: כפי שכתוב במסמך עצמו**

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks. It is useful **regardless** of the maturity level and technical sophistication of an organization's cybersecurity programs. Nevertheless, the CSF does not embrace a one-size-fits-all approach. **Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions.** By necessity, the way organizations implement the CSF will vary.

מקור: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

## קריאה מຕור התכנית עצמה

מקור: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

.15, עמודים 3-6



## פונקציות, קטגוריות, תת-קטגוריות

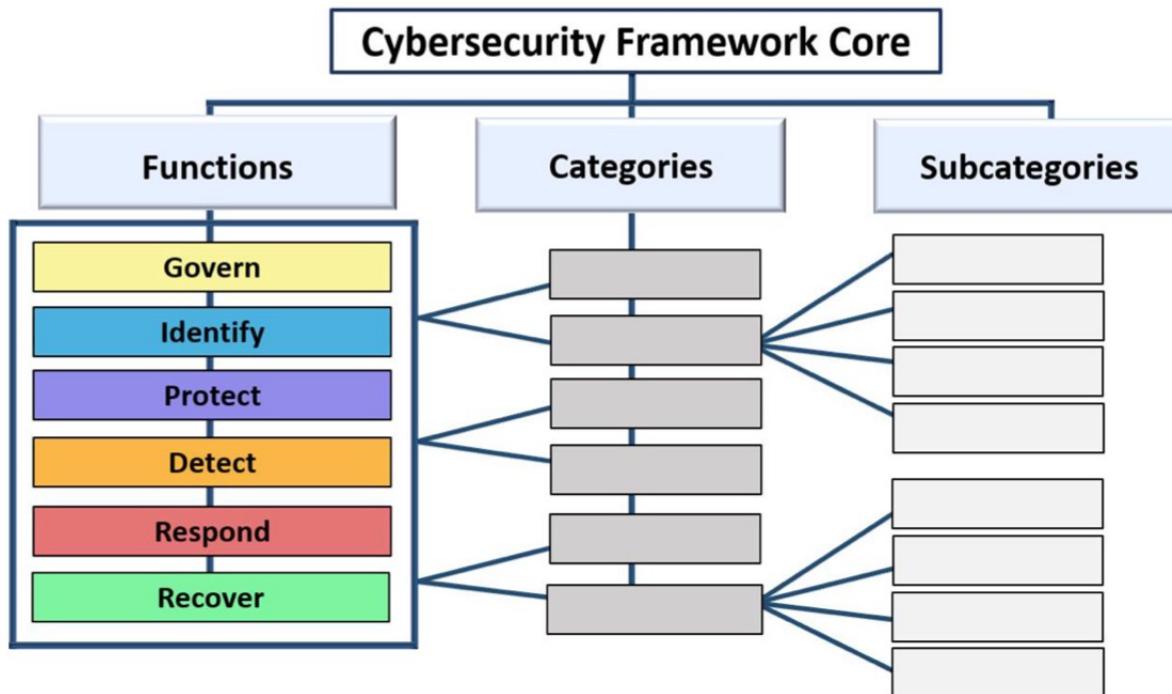


Fig. 1. CSF Core structure

# פונקציות, קטגוריות, נת-קטגוריות

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
<b>Govern (GV)</b>	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
<b>Identify (ID)</b>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<b>Protect (PR)</b>	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
<b>Detect (DE)</b>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<b>Respond (RS)</b>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<b>Recover (RC)</b>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



# פונקציות, קטגוריות, נת-קטגוריות + הנקודות חיצונית

NIST

Search NIST

Menu

CYBERSECURITY FRAMEWORK

[ Helping organizations to better understand and improve their management of cybersecurity risk ]

CSF 2.0 Resource Center +

- News and Events
- Related Programs
- Ways to Engage
- Cybersecurity @ NIST
- CSF 1.1 Archive +

CONNECT WITH US

See even more new [NIST CSF 2.0 resources](#) as we celebrate [Cybersecurity Awareness Month!](#)

**CSF 2.0**

For industry, government, and organizations to reduce cybersecurity risks

[Read the Document](#)



**CSF 2.0 Profiles**

Templates and useful resources for creating and using both CSF profiles

[See the Profiles](#)



**Quick Start Guides**

For users with specific common goals

[View the Quick Start Guides](#)

**Informative References (Mappings)**

See how NIST's resources overlap and share themes

[See the Mappings](#)

## פונקציות, קטגוריות, נת-קטגוריות + הנקודות חיצונית

\* מהמסמך הישן

<b>Function</b>	<b>Category</b>	<b>ID</b>
<b>Identify</b>	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
<b>Protect</b>	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
<b>Detect</b>	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
<b>Respond</b>	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
<b>Recover</b>	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

<b>Subcategory</b>	<b>Informative References</b>
<b>ID.BE-1:</b> The organization's role in the supply chain is identified and communicated	<b>COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05</b> <b>ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2</b> <b>NIST SP 800-53 Rev. 4 CP-2, SA-12</b>
<b>ID.BE-2:</b> The organization's place in critical infrastructure and its industry sector is identified and communicated	<b>COBIT 5 APO02.06, APO03.01</b> <b>ISO/IEC 27001:2013 Clause 4.1</b> <b>NIST SP 800-53 Rev. 4 PM-8</b>
<b>ID.BE-3:</b> Priorities for organizational mission, objectives, and activities are established and communicated	<b>COBIT 5 APO02.01, APO02.06, APO03.01</b> <b>ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6</b> <b>NIST SP 800-53 Rev. 4 PM-11, SA-14</b>
<b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established	<b>COBIT 5 APO10.01, BAI04.02, BAI09.02</b> <b>ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3</b> <b>NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14</b>
<b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<b>COBIT 5 DSS04.02</b> <b>ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1</b> <b>NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14</b>

**יעוניים במסמך ההכנות**

**מקור:** <https://www.nist.gov/informative-references>



**לומדים בבית – נא לעין בקובץ מהאתר: csf2.xls**

## פרופילים ורמות

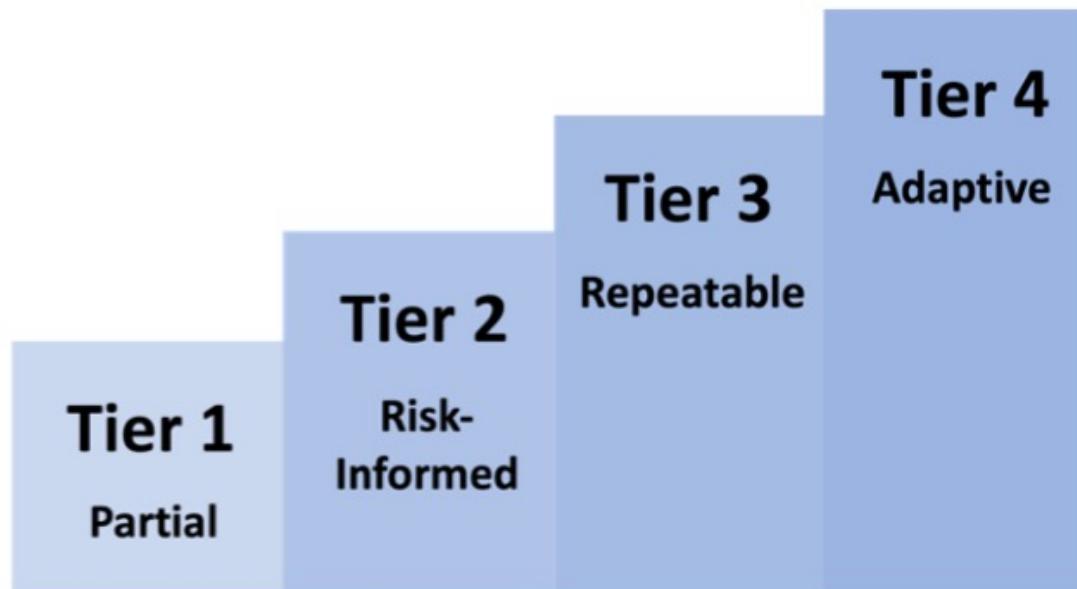


Fig. 3. Steps for creating and using a CSF Organizational Profile

עוניים במסמך הפרופילים:  
CSF 2.0 Organizational  
Profile Template Draft

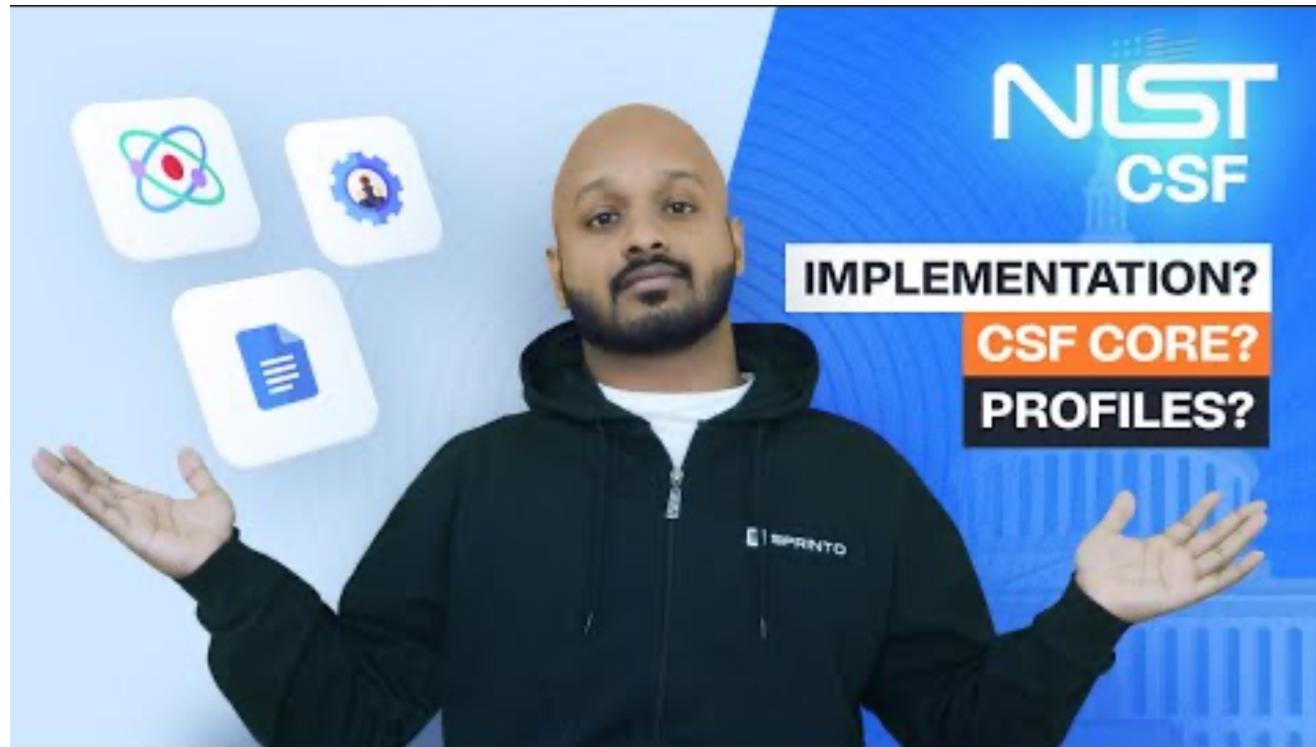
## פרופילים ורמות

[https://youtu.be/n7tnEo\\_22Do?si=6bjfSIEt-G87eJ98&t=79](https://youtu.be/n7tnEo_22Do?si=6bjfSIEt-G87eJ98&t=79)



**Fig. 4. CSF Tiers for cybersecurity risk governance and management**

## פרופילים ורמות

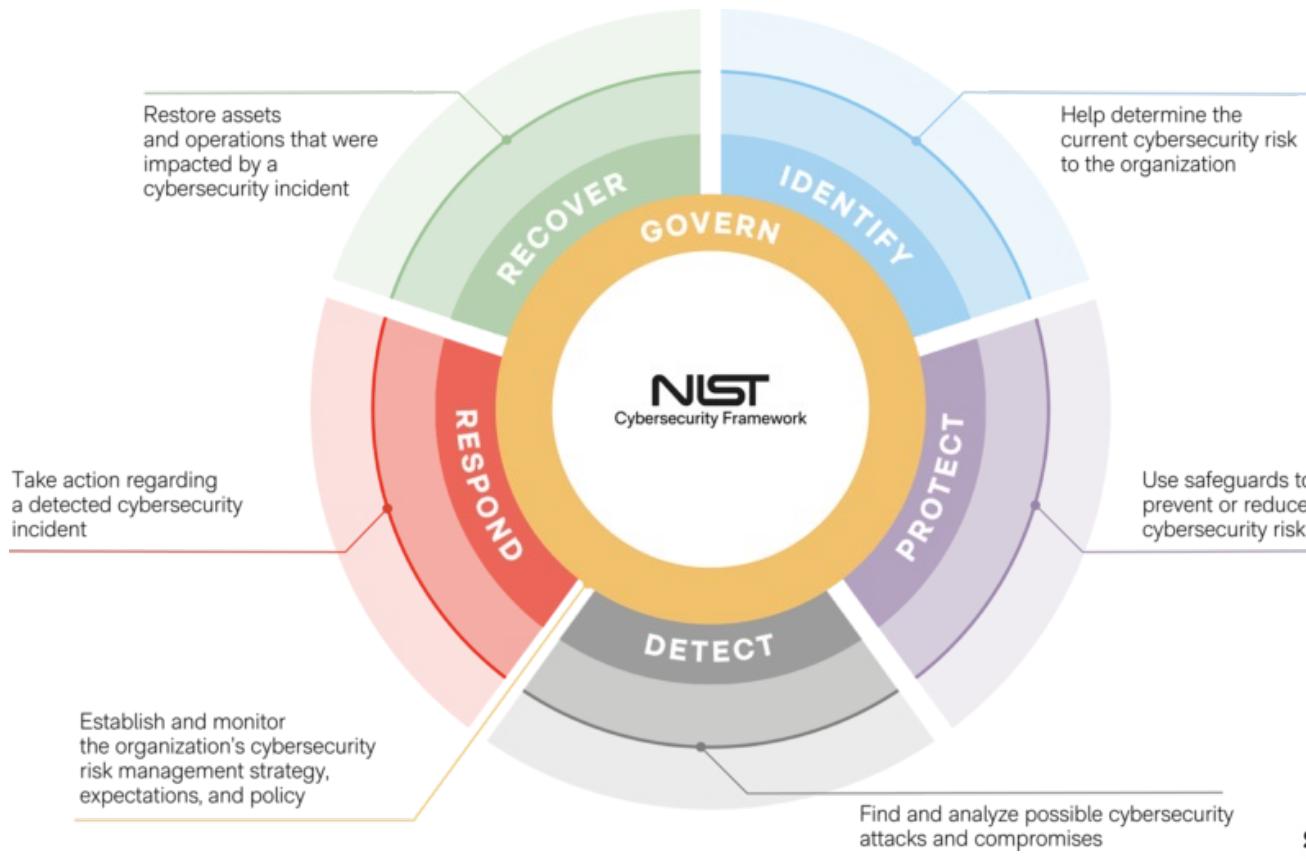


01:20-03:05

[https://youtu.be/n7tnEo\\_22Do?si=6bjfSIEt-G87eJ98&t=79](https://youtu.be/n7tnEo_22Do?si=6bjfSIEt-G87eJ98&t=79)

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# NIST Cybersecurity Framework (2.0)



## סיכום ושאלות



# שיעור 4

תורת ההגנה בסיביר 2.0 של מערך הסיביר הישראלי.  
עינויים במסגרת אבטחת הסיביר של ENISA.