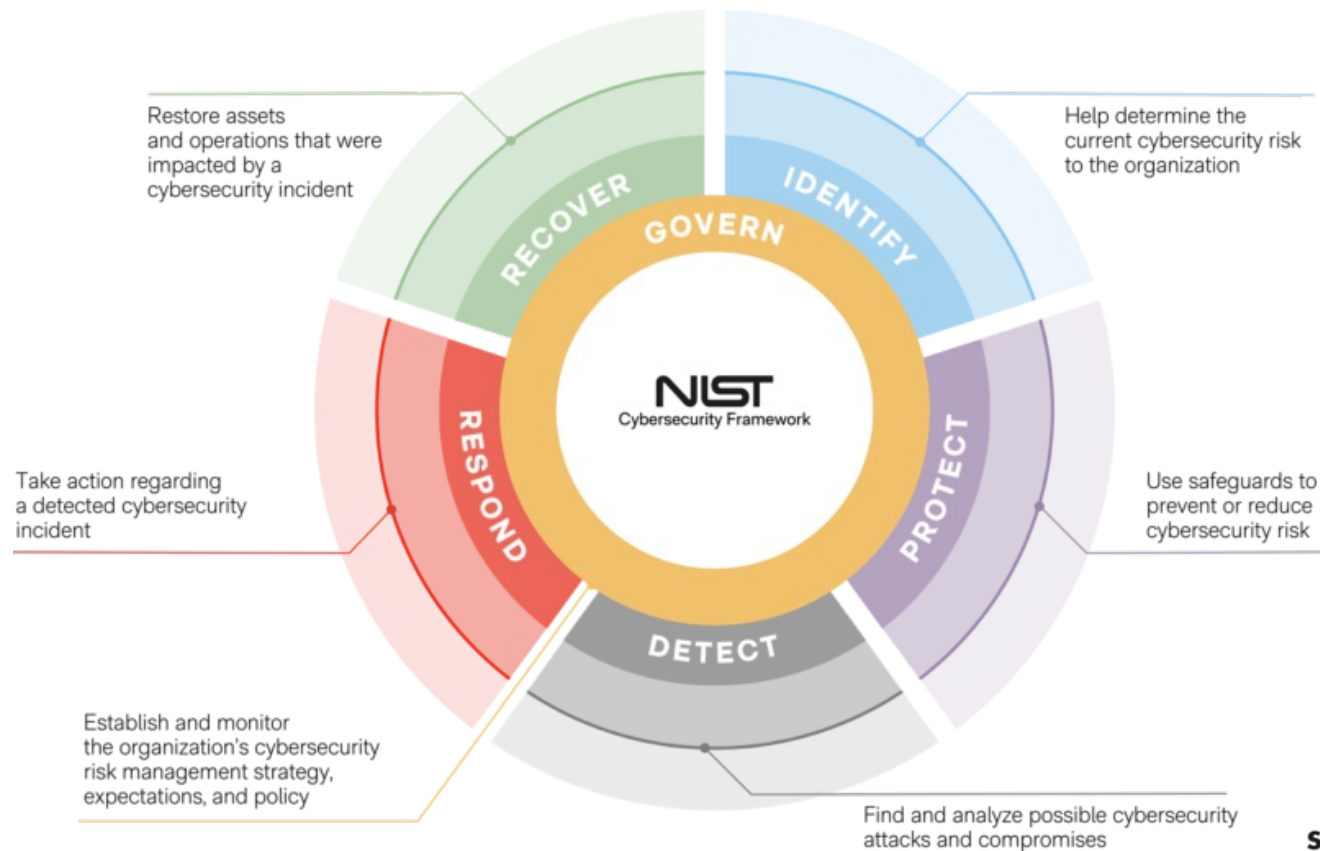


שיעור 3

NIST Cybersecurity Framework

NIST Cybersecurity Framework (2.0)



מטרת השיעור

שיעור שלם על NIST CSF, השתגעתם?

כן.. לכן מטרת השיעור הן:

- להכיר את התכנית, כיצד נוצרה ולמה נועדה.
- להבין כיצד ליישם את התכנית בארגונים השונים.
- לפתח גישה ביקורתית ויישומית למדיניות סייבר בארגונים!

היסטוריה וסיבות הקמה

תכנית ה-NIST Cybersecurity Framework הוקמה בעקבות צו נשיאותי 13636, שפורסם ב-12 בפברואר 2013. הצו יזם שיתוף במידע על איומי סייבר ופיתוח מסגרת להקטנת סיכונים בתשתיות קריטיות. NIST נבחרה בשל היותה סוכנות לא-רגולטורית עם היסטוריה של שיתוף פעולה עם התעשייה והאקדמיה. פיתוח המסגרת כלל בקשות למידע, תגובות ציבוריות וחמישה סדנאות שנערכו בארצות הברית, בהם זוהו פערים והוכנו תוכניות פעולה.

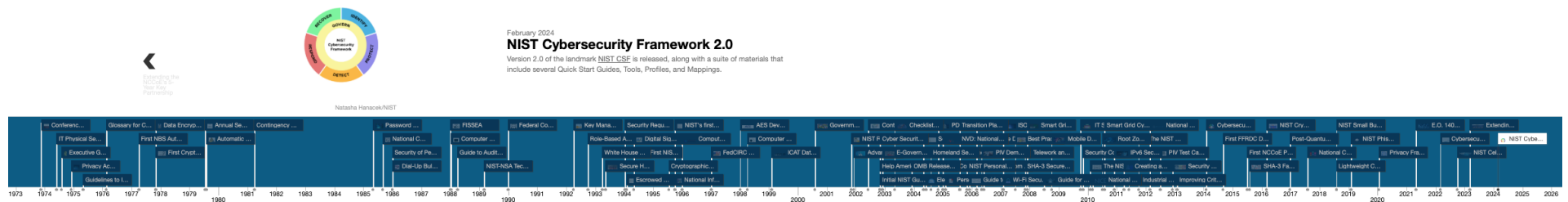
לקריאה נוספת: <https://www.nist.gov/cyberframework/history-and-creation-framework>

היסטוריה וסיבות הקמה

הסיבות העיקריות לפיתוח תכנית ה-NIST Cybersecurity Framework היו:

- עלייה דרמטית באיומי הסייבר.
- הצורך בהגנה טובה יותר על תשתיות קריטיות.
- הצורך בתכנית גובש כדי להגדיר מתודולוגיה אחידה לניהול סיכוני סייבר
- לחזק את הגנת המערכות קריטיות במגזר הפרטי והציבורי.
- לשפר את שיתוף הפעולה בין הממשל הפדרלי לבין גורמים בתעשייה.

היסטוריה אינטראקטיבית



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

תכנית ה-NIST Cybersecurity Framework היא **מסגרת** לניהול סיכוני סייבר, שפותחה על ידי המכון הלאומי לתקנים וטכנולוגיה בארצות הברית. התכנית נועדה לעזור לארגונים לזהות, להגן, לזהות, להגיב ולהתאושש מאיומי סייבר. היא מציעה גישה שיטתית ומתודולוגיה מובנית לשיפור אבטחת המידע והתמודדות עם סיכונים, ומתאימה למגוון רחב של ארגונים בכל הגדלים. המסגרת כוללת עקרונות, תהליכים וכלים שנועדו לשפר את מוכנות הארגון ולהפחית את הסיכון לפגיעות סייבר.

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 מתוך התכנית עצמה

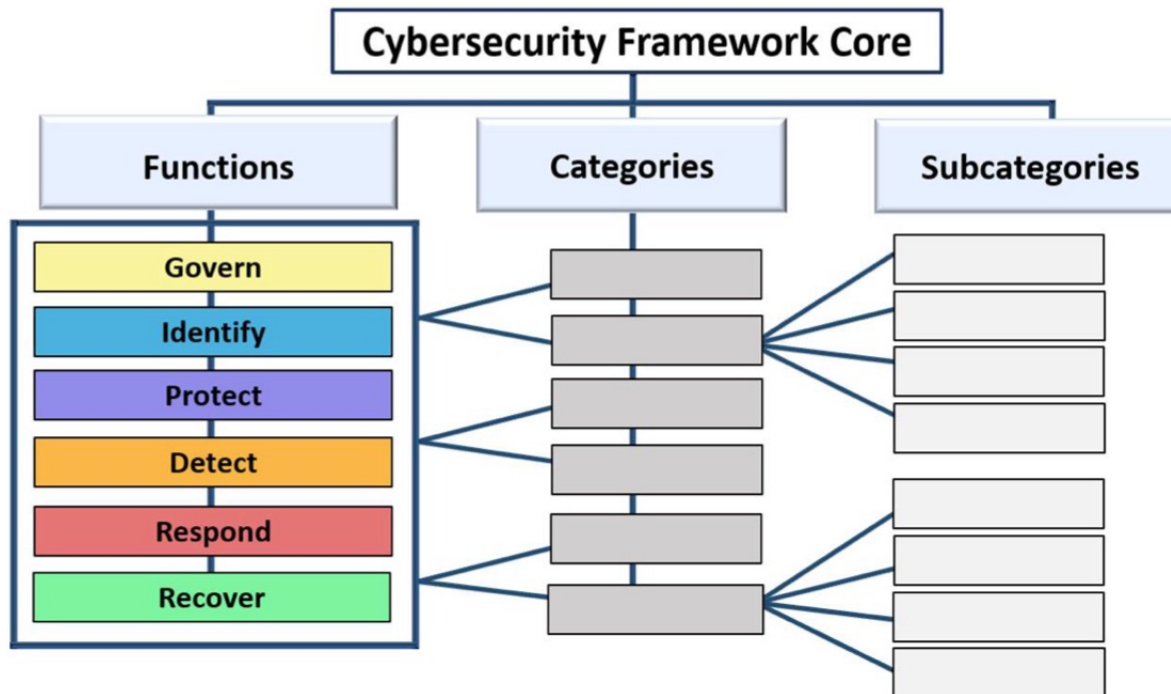
מקור: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

עמודים 3-6, 15.

NIST

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

פונקציות, קטגוריות, תת-קטגוריות



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

Fig. 1. CSF Core structure


פונקציות, קטגוריות, תת-קטגוריות

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

Function	Category	Category Identifier
Govern (GV)	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
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	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
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



פונקציות, קטגוריות, תת-קטגוריות + הפניות חיצוניות



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, תת-קטגוריות + הפניות חיצוניות

*מהמסמך הישן

Function	Category	ID
Identify	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
Protect	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
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

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

עיונים במסמך ההכנות

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



ללומדים בבית – נא לעיין בקובץ מהאתר: csf2.xlsx

פרופילים ורמות



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

עיונים במסמך הפרופילים:
CSF 2.0 Organizational
Profile Template Draft

https://youtu.be/n7tnEo_22Do?si=6bjfSIEt-G87eJ98&t=79

פרופילים ורמות

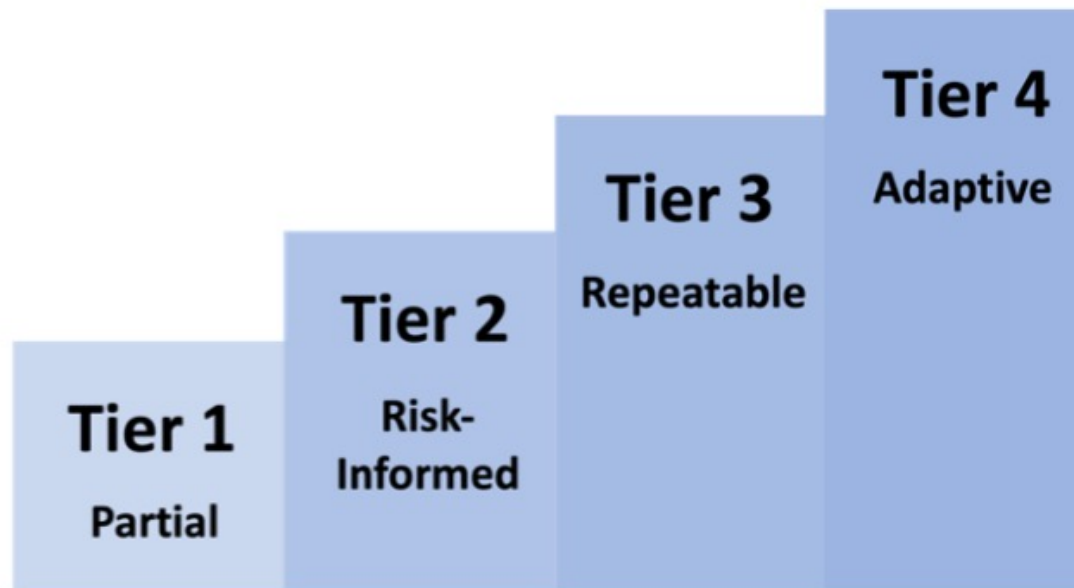
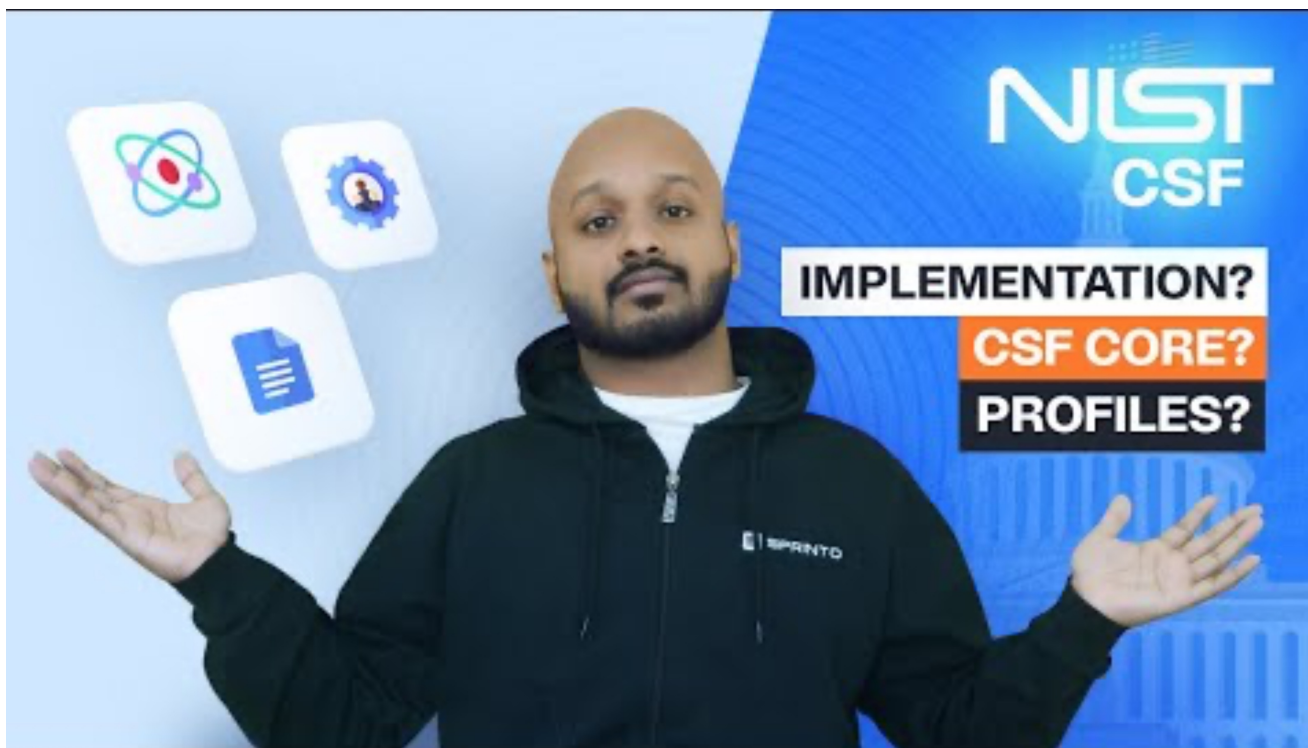


Fig. 4. CSF Tiers for cybersecurity risk governance and management

פרופילים ורמות

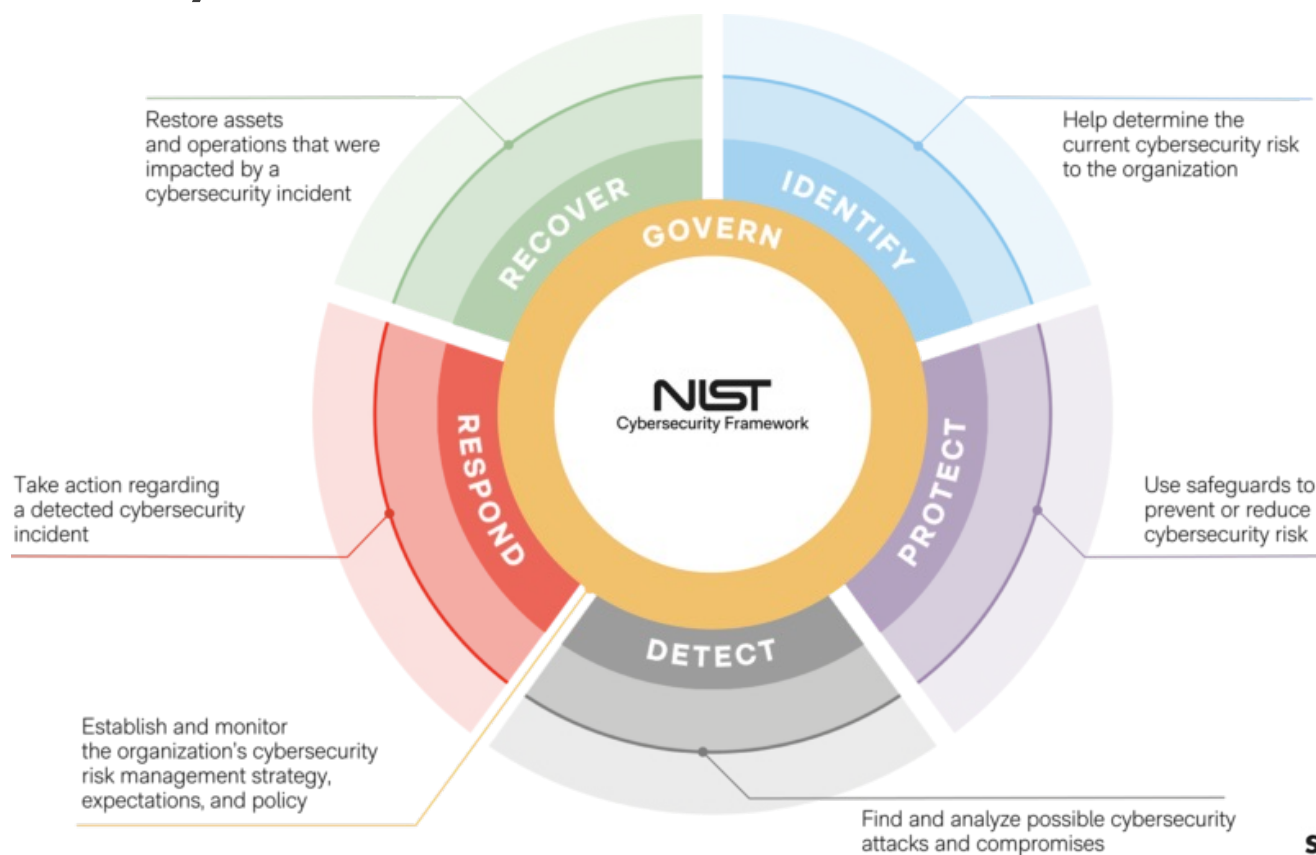


01:20-03:05

https://youtu.be/n7tnEo_22Do?si=6bjfSlEt-G87eJ98&t=79

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

NIST Cybersecurity Framework (2.0)





שיעור 4

תורת ההגנה בסייבר 2.0 של מערך הסייבר הישראלי.
עיונים במסגור אבטחת הסייבר של ENISA.